DISPOSITIONS RELATIVES À LA CLASSIFICATION, À L'HABILITATION ET À LA PROTECTION DU SECRET DE SÉCURITÉ NATIONALE

Annexe à l'arrêté ministériel n° 2021-827 du 23 décembre 2021 modifiant l'arrêté n° 2016-723 du 12 décembre 2016 portant application de l'article 18 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale et fixant les niveaux de classification des informations, modifié

ANNEXE AU « JOURNAL DE MONACO » N° 8.571

DU 31 DÉCEMBRE 2021

TABLE DES MATIÈRES

Table des matières

INTRODUCTION

Certaines informations présentent, en cas de divulgation, un risque tel d'atteinte à la sécurité nationale que seules certaines personnes sont autorisées à y accéder. Considérer qu'une information présente ce risque conduit le Gouvernement Princier à la classifier, c'est-à-dire à lui conférer le caractère de secret de sécurité nationale et à la faire bénéficier d'une protection juridique et matérielle strictes.

La présente annexe décrit l'organisation générale et les modalités de la protection du secret de sécurité nationale. En s'efforçant de clarifier les obligations légales, règlementaires et matérielles inhérentes à cette protection, elle précise les conditions dans lesquelles le Ministre d'État et les Conseillers de Gouvernement-Ministres, pour chaque service de l'État, mettent en œuvre l'application de ces dispositions, en veillant à limiter le nombre et le niveau des habilitations et la production de documents classifiés à ce qui est strictement nécessaire, afin de garantir la plus grande efficacité du dispositif. Elle définit également les procédures d'habilitation et de contrôle des personnes physiques et morales pouvant avoir accès au secret de sécurité nationale, les conditions d'émission, de traitement, d'échange, de conservation ou de transport des documents classifiés et veille aux modalités de leur protection que ce soit sur le support papier ou informatique.

La présente annexe détermine en outre les critères, les niveaux et les conditions de classification des informations et supports concernés ainsi que les règles d'accès aux lieux abritant de telles informations.

Elle prend également en compte l'accroissement constaté des échanges d'informations classifiées, au niveau national ou au niveau international. Dès lors que tous les États protègent leurs informations classifiées, la Principauté de Monaco, au titre des accords de sécurité conclus, est tenue de garantir, à charge de réciprocité, la protection des informations classifiées qui lui sont transmises par les États parties.

Il s'avère enfin que la protection du secret de sécurité nationale ne se limite pas aux documents classifiés sur support papier mais s'étend également aux moyens informatiques et électroniques servant à leur élaboration, leur traitement, leur stockage et leur transmission. La menace constante d'une attaque informatique multiforme et la possibilité, à tout moment, de compromission à l'insu même de l'utilisateur exigent, en réponse, des règles de sécurité des systèmes d'information adaptées à l'évolution rapide des techniques et une expertise fortement développée auprès de tous les acteurs publics ou privés.

Dans la suite du document, les termes « Secret de Sécurité Nationale », avec majuscules, font référence au niveau de classification. Les termes « secret de sécurité nationale », avec minuscules, font référence à la notion de secret de sécurité nationale créée par l'article 18 de la loi n° 1.430 du 13 juillet 2016, portant diverses mesures relatives à la préservation de la sécurité nationale.

TITRE I - PRINCIPES GÉNÉRAUX

1. Fondements de la protection

Décider de classifier une information ou un support est un acte important, tant par les mesures de protection contraignantes qui en découlent, que par les conséquences judiciaires que cette décision peut entraîner.

La décision de classification est ainsi à manier au plus juste :
- utilisée de façon abusive, la classification nuit, de par les mesures de protection qu'elle impose, à l'exigence de réactivité et d'agilité de l'action publique. Elle se traduit par une dévaluation du secret de sécurité nationale et une érosion progressive du respect des règles associées ;
- sous-employée, elle facilite l'accès des services de renseignement étrangers, des groupements hostiles ou des individus cherchant à déstabiliser l'État ou la société, à des informations et supports dont la divulgation est de nature à nuire aux intérêts fondamentaux de la Principauté.

La sur-classification, comme la sous-classification, sont ainsi porteuses de risques pour la sécurité de la Principauté.

Peuvent faire l'objet de ces classifications les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers dont la divulgation est de nature à nuire à la sécurité nationale ou pourrait conduire à la découverte d'un secret de sécurité nationale.

La politique de protection du secret de sécurité nationale vise à rendre responsable, pénalement et administrativement, toute personne ayant accès à des informations ou supports classifiés.

Une information classifiée est compromise lorsqu'elle est portée à la connaissance du public ou d'une personne non habilitée ou n'ayant pas le besoin d'en connaître. L'évaluation des risques de compromission des informations ou supports classifiés et des vulnérabilités des personnes ou des systèmes les traitant, au regard de la protection des intérêts fondamentaux de la Principauté, est essentielle afin de garantir la protection du secret de sécurité nationale. La stricte application des mesures de sécurité définies dans la présente annexe, complétée par la diffusion de règles et la sensibilisation des personnels, contribue à l'efficacité du dispositif et permet de lutter contre des actions malveillantes, souvent facilitées par l'ignorance, l'imprudence, l'inattention ou la négligence.

La protection du secret de sécurité nationale, qu'il s'agisse d'une information ou d'un support, doit être assurée par les personnes, physiques ou morales, de droit public ou de droit privé, y accédant. En cas de manquement, même involontaire, ces personnes se rendent coupables de compromission et encourent les sanctions prévues à l'article 19 de la loi n° 1.430 du 13 juillet 2016, précitée.

2. Définitions

Comme indiqué à l'article 2 de l'arrêté auquel est rattachée cette annexe :

Le niveau « Très Secret de Sécurité Nationale » est réservé aux informations et supports qui concernent les priorités gouvernementales en matière de sécurité nationale et dont la divulgation est de nature à nuire très gravement à la protection des intérêts fondamentaux de la Principauté ;

Le niveau « Secret de Sécurité Nationale » est réservé aux informations et supports dont la divulgation est de nature à nuire gravement à la protection des intérêts fondamentaux de la Principauté ou pourrait conduire à la découverte d'un secret de sécurité nationale classifié au niveau « Très Secret de Sécurité Nationale ».

Au sens de la présente annexe, il faut entendre par :

« contrat classifié » : tout contrat, toute convention, tout projet, tout marché quel que soit son régime juridique ou sa dénomination, dans lequel un candidat ou un cocontractant, public ou privé, est amené à l'occasion de la passation du contrat ou de son exécution à connaître et éventuellement à produire, manipuler ou détenir dans ses locaux des informations ou des supports classifiés ;

« habilitation » : décision explicite, prise et délivrée à l'issue d'une procédure spécifique définie dans la présente annexe, permettant à une personne, en fonction de son besoin d'en connaître, d'avoir accès aux informations ou supports classifiés au niveau précisé dans la décision ainsi qu'au(x) niveau(x) inférieur(s) ;

« informations ou supports classifiés » : procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers présentant un caractère de secret de sécurité nationale ;

« systèmes d'information » : tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données informatiques ainsi que les données informatiques stockées, traitées, récupérées ou transmises par ce dispositif ou cet ensemble de dispositifs en vue du fonctionnement, de l'utilisation, de la protection et de la maintenance de celui-ci.

« zone protégée » : lieu (local, établissement ou terrain clos délimité) intéressant la sécurité nationale, bénéficiant d'une protection juridique au sens de l'article 19 de la loi n° 1.430 du 13 juillet 2016 où la libre circulation est interdite et l'accès soumis à autorisation.

3. Champ d'application

Les dispositions de la présente annexe sont applicables à l'ensemble des services placés sous l'autorité directe du Ministre d'État et des Conseillers de Gouvernement-Ministres, aux entités placées sous leur tutelle ainsi que, de manière générale, aux opérateurs d'importance vitale dans la limite du besoin d'en connaître en raison de leur désignation en tant qu'opérateurs d'importance vitale, aux autres entités, publiques ou privées, concernées par le secret de sécurité nationale, ainsi qu'à toute personne dépositaire, même à titre provisoire, d'un tel secret, y compris dans le cadre de la passation et de l'exécution d'un contrat.

Les informations ou supports classifiés confiés aux entités publiques ou privées de la Principauté de Monaco, en application d'un accord de sécurité, bénéficient des mesures de protection du secret de sécurité nationale en fonction des concordances définies par ledit accord, dès lors qu'elles portent une mention de classification équivalente à l'un des deux niveaux définis.

4. La classification

La décision de classifier au titre du secret de sécurité nationale une information ou un support a pour conséquence de le placer sous la protection de dispositions spécifiques de la loi. L'apposition du marquage de classification constitue le seul moyen de lui conférer cette protection particulière.

Une information, n'ayant pas fait l'objet d'une décision de classification à l'un des deux niveaux définis, n'est pas protégée pénalement au titre du secret de sécurité nationale. Ainsi, le fait d'omettre de procéder à la classification d'une information dont la divulgation est de nature à nuire au secret de sécurité nationale, caractérise une faute, qu'il revient à l'autorité hiérarchique d'apprécier et, le cas échéant, de sanctionner conformément au régime disciplinaire applicable.

5. Mentions particulières de confidentialité

Certaines informations qu'il n'y a pas lieu de classifier peuvent cependant recevoir, de la part de leur émetteur, une marque de confidentialité destinée à restreindre leur diffusion à un domaine spécifique (précisé par une mention particulière[1]) ou à garantir leur protection.

---

[1] Par exemple : « Diffusion Restreinte », « *Confidentiel Personnel* », « *Confidentiel Médical* », « *Confidentiel Technologie* », « *Confidentiel Industrie* », « *Confidentiel Commercial* », « *Confidentiel Concours* », information non classifiée soumise à un contrôle, ou encore « *Spécial Monaco* ».

Ces mentions, qui ne traduisent pas une classification, ne suffisent pas à conférer aux informations concernées la protection pénale propre au secret de sécurité nationale. Leur seul objectif est de sensibiliser l'utilisateur à la nécessaire discrétion dont il doit faire preuve dans la manipulation des informations couvertes par ces mentions.

L'auteur de la divulgation, qu'il relève de la sphère publique ou de la sphère privée, s'expose à des sanctions disciplinaires et professionnelles[2], sans préjudice de l'application éventuelle des dispositions spécifiques aux traitements d'informations nominatives contenues dans la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée.

6. L'accès aux secrets de sécurité nationale

Seules des personnes habilitées et ayant besoin d'en connaître peuvent accéder aux secrets de sécurité nationale.

Une personne habilitée, sous réserve du besoin d'en connaître, peut avoir accès aux informations ou supports classifiés au niveau précisé dans la décision d'habilitation ainsi qu'au niveau inférieur.

La décision d'habilitation est une autorisation explicite, délivrée à l'issue d'une procédure spécifique définie au chapitre 2 de l'arrêté auquel est rattachée cette annexe, permettant à une personne, sous réserve du besoin d'en connaître, d'avoir accès aux informations ou supports classifiés au niveau précisé dans la décision ainsi qu'au niveau inférieur. La décision d'habilitation est assortie d'un engagement de respecter, après en avoir dûment pris connaissance, les obligations et les responsabilités liées à la protection des informations ou supports classifiés.

7. Les lieux abritant des informations classifiées

Les lieux abritant des éléments couverts par le secret de sécurité nationale sont les locaux dans lesquels sont détenus des informations ou supports classifiés, quel qu'en soit le niveau, par des personnes par ailleurs habilitées au niveau requis. Ils doivent être classés en zones protégées conformément à l'article 15 de l'arrêté auquel est rattachée la présente annexe.

8. Contrôles et inspections

Des contrôles et des inspections sont assurés périodiquement par les officiers de sécurité, mentionnés à l'article 10 de l'arrêté auquel est rattachée la présente annexe pour vérifier, l'application et le respect, par l'ensemble des services exécutifs de l'État, des établissements publics ou des entreprises de droit privé, émettant, recevant, traitant ou conservant des informations ou supports classifiés, et relevant de leur périmètre, des règles et des directives relatives à la protection du secret de sécurité nationale.

En cas d'anomalies constatées, l'officier de sécurité établit un rapport de synthèse incluant les mesures préconisées pour rectifier les déficiences constatées et leur planification. Ce rapport est transmis, selon le cas, au Ministre d'État, au Conseiller de Gouvernement-Ministre concerné, au Secrétaire Général du Gouvernement ou à l'autorité responsable de l'entité publique ou privée concernée. La Direction de la Sûreté Publique et/ou l'Agence Monégasque de Sécurité Numérique proposent toutes mesures propres à améliorer les conditions générales de sécurité.

[2] Loi n° 975 du 12 juillet 1975 portant statut des fonctionnaires de l'État.

TITRE II - L'OFFICIER DE SÉCURITÉ DANS L'ENTREPRISE

Le chapitre 1 de l'arrêté auquel est rattachée la présente annexe définit l'organisation de la protection du secret de sécurité nationale. Ce chapitre est complété par le paragraphe suivant.

Un officier de sécurité du contractant est proposé par le chef de l'entreprise contractante. Il doit faire l'objet d'un agrément par l'autorité d'habilitation. Pour être agréé, l'officier de sécurité doit être préalablement habilité et formé. Cet agrément peut être délivré pour une période probatoire de douze mois au plus. À l'issue de cette période probatoire, sauf décision explicite contraire, l'agrément est réputé confirmé. L'agrément peut être retiré à tout moment par l'autorité d'habilitation, notamment lorsque son titulaire cesse d'être habilité. Dans ce cas, le chef de l'entreprise titulaire du contrat concerné doit proposer un nouveau titulaire dans les mêmes conditions et dans les plus brefs délais.

Sous l'autorité du chef de l'entreprise, l'officier de sécurité est chargé de l'organisation générale de la sécurité de l'établissement et notamment des relations, au titre de sa fonction, avec le Directeur de la Sûreté Publique, les autorités d'habilitation et les autorités contractantes.

À ce titre, il est amené à s'assurer notamment :

- de l'application des règles de sécurité énoncées dans les différents textes au sein de l'établissement ;
- de la gestion des dossiers d'habilitation du personnel de l'établissement en fonction du besoin d'en connaître ; il est également chargé des demandes d'habilitation de sous-traitants éventuels ; il est tenu de signaler au Directeur de la Sûreté Publique les éléments de vulnérabilité portés à sa connaissance apparaissant après la décision d'habilitation, et de signaler à l'autorité d'habilitation tout changement dans les statuts de la personne morale ;
- de la tenue à jour d'un registre des membres du personnel titulaires d'une habilitation et auxquels l'accès est autorisé, dans le cadre du contrat et d'éventuels contrats de sous-traitance ; ce registre indique les dates de délivrance et de fin de validité ainsi que le niveau de ces habilitations ;
- de fournir, à la demande du Directeur de la Sûreté Publique, des renseignements sur toutes les personnes qui seront appelées à avoir accès à des informations classifiées ;
- de la sensibilisation et de la formation du personnel ;
- de signaler les compromissions du secret de sécurité nationale avérées ou supposées, dans les conditions définies à l'article 9 de l'Arrêté Ministériel 2016-723, modifié ;
- de la gestion et de la mise à jour des annexes de sécurité des contrats de droit public ou de droit privé ;
- de la mise à jour du dossier de sécurité.

Dans le cadre des contrats impliquant la détention d'informations ou de supports classifiés, il est en outre chargé :

- du contrôle permanent de la gestion et de la protection des informations ou supports classifiés ;
- de la gestion et du suivi des articles contrôlés de la sécurité des systèmes d'information (ACSSI) ;
- de la gestion des demandes d'autorisation d'accès au périmètre d'accès restreint et de la gestion des contrôles élémentaires pour l'accès des personnels extérieurs à l'établissement ;
- de l'application des règles internationales en matière de visites de ressortissants étrangers se rendant dans l'établissement dont il a la charge ;
- de l'application des règles internationales en matière de visites à l'étranger des personnels de son établissement ;
- de la sensibilisation aux prescriptions de sécurité à respecter dans l'établissement par les différents intervenants ;
- du respect des dispositions réglementaires en matière d'accès, de manipulation, de conservation, de reproduction et de destruction des informations classifiées.

TITRE III - MESURES DE SÉCURITÉ RELATIVES AUX PERSONNES

Le chapitre 2 de l'arrêté auquel est rattachée la présente annexe définit les conditions d'accès au secret de sécurité nationale. Ce chapitre est complété par les paragraphes suivants.

1. Information des candidats à l'habilitation

Lors de leur demande d'habilitation, les candidats sont informés, par les mentions portées sur la notice individuelle qui leur est remise, des obligations induites par l'habilitation ainsi que des dispositions relatives à leur responsabilité pénale en cas de compromission[3].

La notification d'une décision d'habilitation favorable par l'officier de sécurité est complétée par une séance de sensibilisation aux risques de compromission puis, par la suite, par des rappels périodiques de la réglementation en vigueur.

Une sensibilisation aux menaces d'investigations ou d'approches par des individus ou des organisations étrangères est faite aux personnes devant se rendre hors du territoire national, que l'État de destination soit ou non lié à Monaco par un accord de sécurité. Avant leur départ, des règles de prudence élémentaire leur sont rappelées.

2. Objet de l'habilitation

L'autorité hiérarchique doit veiller à l'habilitation du personnel placé sous sa responsabilité et, à ce titre, initier, par la constitution d'un dossier, la procédure d'habilitation au niveau requis par le catalogue des emplois.

La demande d'habilitation déclenche une procédure destinée à vérifier qu'une personne peut, sans risque pour la sécurité nationale ou pour sa propre sécurité, connaître des informations ou supports classifiés dans l'exercice de ses fonctions. La procédure comprend une enquête de sécurité permettant à l'autorité d'habilitation de prendre sa décision en toute connaissance de cause.

Toute personne visant ou occupant un poste pour lequel le besoin d'une habilitation est avéré et qui refuserait de se soumettre à la procédure d'habilitation devra être écartée du poste considéré.

3. Procédure d'habilitation des personnes physiques

Seuls les emplois figurant au catalogue des emplois doivent faire l'objet d'une habilitation. Aussi, lorsqu'un poste à pourvoir exige une habilitation, la procédure n'est engagée qu'au seul profit de la personne effectivement nommée dans l'emploi, sauf cas particulier.

Anticiper la prise de poste en engageant la procédure d'habilitation sans attendre la prise effective de fonction peut être une mesure de bonne gestion, qui permet à la personne nouvellement affectée de prendre connaissance des informations classifiées sans perdre de temps.

Il convient toutefois d'éviter toute surcharge inutile du service chargé de cette mission en limitant autant que possible le nombre de demandes d'habilitation.

3.1. Procédures d'habilitation

Le responsable de l'organisme sollicitant l'habilitation, par le biais de son officier de sécurité, décide de la procédure d'habilitation à mettre en œuvre.

Trois procédures d'habilitation sont applicables :

[3] Article 19 de la loi n° 1.430 du 13 juillet 2016 relative à la préservation de la sécurité nationale.

3.1.1. Procédure d'habilitation de droit commun

Cette procédure concerne toutes les personnes appelées à occuper un poste pour lequel le besoin d'habilitation au niveau Secret de Sécurité Nationale ou Très Secret de Sécurité Nationale, y compris pour les classifications spéciales de ce dernier niveau, est avéré.

L'autorité d'habilitation peut également décider d'accorder une décision d'habilitation temporaire à un agent de l'État ou d'un de ses établissements publics lorsque l'intéressé fait l'objet d'une habilitation au niveau Secret de Sécurité Nationale pour lequel il est inscrit au catalogue des emplois et qu'il a besoin, de façon ponctuelle, d'accéder à des informations et supports classifiés au niveau Très Secret de Sécurité Nationale, hors classification spéciale. Cette décision, non renouvelable, est valable pour une durée maximale de trois mois.

3.1.2. Procédure d'habilitation en urgence

Cette procédure exceptionnelle, applicable quel que soit le niveau de l'habilitation, Secret de Sécurité Nationale ou Très Secret de Sécurité Nationale, permet de délivrer une habilitation à une personne dans des délais très brefs selon les modalités détaillées ci-après afin que cette dernière puisse avoir accès à des informations et supports classifiés dès sa prise de fonction.

La procédure d'urgence s'applique aux seuls cas exceptionnels de personnes affectées dans des conditions ne permettant pas le respect des délais de la procédure de droit commun et exerçant des fonctions exigeant un accès immédiat à des informations et supports classifiés.

La procédure d'urgence n'est pas applicable aux agents de la Division du Renseignement Intérieur.

Le dossier d'habilitation est identique à celui prévu pour la procédure de droit commun. Il est constitué selon la procédure de droit commun, à la différence près que l'autorité compétente doit, dans la demande, préciser et motiver l'urgence de l'habilitation et l'impossibilité de procéder autrement. Pour les classifications spéciales, seul le Ministre d'État peut, en sa qualité d'Autorité Nationale de Sécurité, engager une telle procédure au regard des éléments transmis par l'autorité d'emploi.

Dans les quinze jours ouvrables suivant sa saisine, la Direction de la Sûreté Publique émet un avis de sécurité provisoire. Un avis de sécurité s'entend au sens du présent arrêté d'une conclusion émise par le Directeur de la Sûreté Publique à l'issue d'investigations se rapportant à une personne et visant à détecter et à évaluer les vulnérabilités de cette personne.

La procédure de droit commun se poursuit après l'émission de l'avis de sécurité provisoire. Au vu de ce dernier, l'autorité d'habilitation peut prendre une décision d'habilitation provisoire qui expire :

- *soit lorsqu'à réception de l'avis de sécurité définitif, la décision d'habilitation ou de refus d'habilitation est prise ;*
- *soit au plus tard six mois après sa date d'émission.*

3.1.3. Procédure d'habilitation simplifiée

Cette procédure, uniquement applicable aux demandes d'habilitation au niveau Secret de Sécurité Nationale et réservée aux seuls agents publics (fonctionnaires ou agents non-titulaires, civils ou militaires), permet de délivrer une décision d'habilitation sur le fondement d'une enquête administrative réalisée au moment du recrutement, de la nomination ou de l'affectation, sous réserve, pour le candidat à l'habilitation, de remplir une notice individuelle de sécurité comportant une attestation sur l'honneur de l'exactitude des informations mentionnées.

La décision d'habilitation délivrée dans le cadre d'une procédure simplifiée est valide pour une durée limitée ne dépassant pas la durée maximale prévue pour une habilitation au niveau Secret de Sécurité Nationale.

L'autorité ayant sollicité l'habilitation par procédure simplifiée peut, à tout moment, solliciter une enquête administrative auprès de la Direction de la Sûreté Publique conformément à la procédure de droit commun.

La procédure simplifiée n'est pas applicable aux agents de la Direction de la Sûreté Publique ou de l'Agence Monégasque de Sécurité Numérique.

3.2. Constitution du dossier :

Le dossier d'habilitation a pour objet de réunir les éléments nécessaires à la conduite de l'enquête administrative. Il est constitué de :

- la demande d'habilitation formulée par l'autorité compétente attestant le besoin de connaître des informations et supports classifiés à un niveau donné, pour une personne nommément désignée à un poste donné ;
- la notice individuelle de sécurité, intégralement renseignée et signée par le candidat et vérifiée par l'officier de sécurité de l'organisme dont il relève ;
- l'officier de sécurité adresse le dossier d'habilitation à l'autorité d'habilitation et en conserve une copie datée et signée au plus tard jusqu'à un an après la durée de l'avis de sécurité en cours de validité. La transmission du dossier par voie électronique est privilégiée à condition que le système d'information employé garantisse l'identification et l'authentification de l'émetteur comme du destinataire, assure la confidentialité et l'intégrité des données et permette de tracer les actions effectuées. Dans le cas contraire, le dossier d'habilitation est transmis, accompagné d'une photographie d'identité originale ;
- le dossier d'habilitation constitué de la notice individuelle, de la demande d'habilitation du service employeur et d'une photo d'identité, est adressé à l'autorité d'habilitation, qui vérifie qu'il est complet et le transmet pour instruction à la Direction de la Sûreté Publique sous couvert de l'officier de sécurité du Département de l'Intérieur.

3.3. Instruction du dossier :

L'enquête de sécurité menée dans le cadre de la procédure d'habilitation est une enquête administrative permettant de déceler chez le candidat ou son entourage d'éventuelles vulnérabilités.

Elle est diligentée par la Direction de la Sûreté Publique.

L'enquête administrative est fondée sur des critères objectifs permettant de déterminer si l'intéressé, par son comportement ou par son environnement proche, présente une vulnérabilité, soit parce qu'il constitue lui-même une menace pour le secret de sécurité nationale, soit parce qu'il se trouve exposé à un risque de chantage ou de pressions pouvant mettre en péril les intérêts de l'État.

La durée de l'enquête administrative est en principe de six mois pour un dossier d'habilitation au niveau Secret de Sécurité Nationale et neuf mois au niveau Très Secret de Sécurité Nationale, à compter de sa réception par le service chargé de la réaliser. Dans le cadre d'une procédure d'urgence, ce dernier peut délivrer, sur demande de l'autorité compétente, un avis de sécurité provisoire qui ne prolonge pas la durée de l'enquête. Cet avis de sécurité provisoire est valable jusqu'à réception de l'avis de sécurité définitif ou, au plus tard, six mois après sa date d'émission.

Les enquêtes administratives relatives aux agents de la Direction de la Sûreté Publique et de l'Agence Monégasque de Sécurité Numérique sont diligentées en priorité.

Afin de s'assurer que le comportement de la personne habilitée n'est pas devenu incompatible avec les exigences relatives à la protection du secret de sécurité nationale, l'autorité d'habilitation peut, d'elle-même ou après signalement d'un changement de comportement ou de situation par l'officier de sécurité ou l'autorité d'emploi dont la personne habilitée relève, diligenter une nouvelle enquête administrative.

Si des vulnérabilités sont apparues, l'autorité d'habilitation peut décider d'abroger la décision d'habilitation.

3.4. Clôture de l'instruction et avis de sécurité :

L'enquête administrative menée par la Direction de la Sûreté Publique dans le cadre de l'habilitation s'achève par l'émission d'un avis de sécurité, par lequel le Directeur de la Sûreté Publique fait connaître ses conclusions techniques à l'autorité compétente pour prendre la décision d'habilitation.

Cet avis comporte une évaluation des vulnérabilités éventuellement détectées lors de l'enquête et formule une conclusion de nature à permettre à l'autorité d'habilitation d'apprécier l'opportunité de l'habilitation[4] de l'intéressé, au regard des éléments communiqués et des garanties qu'il présente pour le niveau d'habilitation requis.

Les conclusions de l'avis de sécurité sont de trois types :

- *« avis sans objection », lorsque l'instruction n'a révélé aucun élément de vulnérabilité de nature à constituer un risque pour la sécurité des informations ou supports classifiés ni pour celle de l'intéressé ;*

- *« avis restrictif », lorsque l'intéressé présente certaines vulnérabilités constituant des risques directs ou indirects pour la sécurité des informations ou supports classifiés auxquels il aurait accès, mais que des mesures de sécurité spécifiques prises par l'officier de sécurité permettraient de maîtriser ;*

- *« avis défavorable », lorsque des informations précises font apparaître que l'intéressé présente des vulnérabilités faisant peser sur le secret de sécurité nationale des risques tels qu'aucune mesure de sécurité ne semble suffisante à les neutraliser.*

Les avis restrictifs ou défavorables peuvent être classifiés selon l'appréciation du Directeur de la Sûreté Publique et sont assortis d'une fiche confidentielle ne pouvant être reproduite, indiquant les motifs de l'avis.

Ladite fiche est retournée après prise de connaissance par l'autorité d'habilitation, sans délai, à la Direction de la Sûreté Publique qui l'a émise, aux fins de conservation.

La durée de validité de l'avis de sécurité est fonction du niveau d'habilitation demandé. Elle ne peut excéder :

- *cinq ans pour le niveau « Très Secret de Sécurité Nationale » ;*

- *sept ans pour le niveau « Secret de Sécurité Nationale » ;*

L'avis de sécurité ne constitue en soi ni une autorisation ni un refus et ne lie pas l'autorité d'habilitation, qui prend sa décision après avoir apprécié les différents éléments recueillis pendant l'instruction du dossier.

4. La décision d'habilitation des personnes physiques

L'autorité d'habilitation peut décider, lorsque l'enquête a mis en valeur des éléments de vulnérabilité, de n'accorder l'habilitation qu'après avoir pris des précautions particulières. Ainsi, afin de garantir le plus efficacement possible la protection des informations ou supports classifiés, l'attention de l'employeur, par une procédure de mise en garde, ou celle de l'intéressé lui-même, par une procédure de mise en éveil, est attirée sur les risques auxquels l'un ou l'autre se trouve exposé.

Les procédures de mise en garde et de mise en éveil peuvent être cumulées.

[4] Titre I, Chapitre II, section 1, paragraphe 9 et paragraphe 10.

4.1. La mise en garde :

Cette procédure permet à l'autorité d'habilitation de mettre en œuvre des mesures de sécurité ou de prendre des précautions particulières à l'égard de l'intéressé, si nécessaire avec le conseil du Directeur de la Sûreté Publique.

À l'issue de l'entretien de mise en garde, une attestation particulière est signée par l'officier de sécurité. La décision d'habilitation n'est rendue qu'à l'issue de la procédure. L'attestation est conservée par l'autorité d'habilitation.

Au niveau « Très Secret de Sécurité Nationale », la procédure de mise en garde est menée sous couvert du Ministre d'État, qui conserve l'attestation.

4.2. La mise en éveil :

Lorsque l'autorité d'habilitation ou son représentant décide d'accorder l'habilitation sur la base d'un avis de sécurité restrictif ou en dépit d'un avis de sécurité défavorable, elle peut choisir de demander la mise en éveil de l'intéressé, qui consiste à sensibiliser ce dernier sur les éléments communicables de vulnérabilité révélés par l'enquête. La mise en éveil est menée par l'officier de sécurité concerné. L'autorité d'habilitation définit les modalités de la mise en éveil en liaison avec le Directeur de la Sûreté Publique et peut, au cas par cas, solliciter sa présence ou celle de son représentant lors de l'entretien avec l'intéressé.

Le cas échéant, l'officier de sécurité étudie avec la Direction de la Sûreté Publique les mesures de sécurité complémentaires à mettre en œuvre au regard de la situation.

À l'issue de l'entretien de mise en éveil, une attestation particulière est signée par l'autorité d'habilitation, ou son représentant, par l'officier de sécurité et par l'intéressé.

La décision d'habilitation n'est prise qu'à l'issue de la procédure. L'attestation est conservée par l'autorité d'habilitation.

Au niveau « Très Secret de Sécurité Nationale », la mise en éveil est menée sous couvert du Ministre d'État, qui conserve l'attestation.

4.3. Le refus d'habilitation :

L'intéressé est informé de la décision défavorable prise à son endroit. Un refus d'habilitation n'a pas à être motivé conformément aux dispositions de l'article 5 de la loi n° 1.312 du 29 juin 2016 relative à la motivation des actes administratifs.

La décision par laquelle l'autorité d'habilitation refuse d'habiliter une personne au titre de la protection du secret de sécurité nationale, est notifiée à l'intéressé par l'officier de sécurité.

Lors de cet entretien, l'officier de sécurité remet à l'intéressé la décision de refus d'habilitation ainsi qu'un récépissé de notification de décision de refus d'habilitation qui comporte la mention des voies et délais de recours et dont un exemplaire, daté et signé par l'intéressé, est conservé par l'autorité d'habilitation.

4.4. Décision favorable et engagement de responsabilité :

La décision d'habilitation est notifiée par l'officier de sécurité compétent à l'intéressé, qui signe le premier volet de l'engagement de responsabilité. Par cet acte, le titulaire de l'habilitation reconnaît avoir eu connaissance des obligations particulières imposées par l'accès à une information ou à un support classifié ainsi que des sanctions prévues par la loi en cas d'inobservation, délibérée ou non, de la réglementation protégeant le secret de sécurité nationale.

Il est également notifié à l'intéressé qu'il est tenu d'informer au plus vite, pendant toute la durée de son habilitation, l'officier de sécurité dont il relève de tout changement affectant sa vie personnelle (mariage, divorce, établissement ou rupture d'une vie commune, etc.), professionnelle ou son lieu de résidence. Il lui est signifié qu'il devra l'informer de toute relation suivie et fréquente dépassant le strict

cadre professionnel avec un ou plusieurs ressortissants étrangers. L'officier de sécurité devra alors lui faire remplir, afin de mettre à jour les informations, une notice individuelle et la transmettre à l'autorité d'habilitation (sous forme électronique lorsque la procédure est dématérialisée).

Ce changement de situation pourra justifier un réexamen du dossier d'habilitation et, le cas échéant, la saisine de la Direction de la Sûreté Publique sous couvert de l'officier de sécurité du Département de l'Intérieur en vue de l'émission d'un nouvel avis.

Le second volet de cet engagement est signé par l'intéressé à la cessation de ses fonctions ou au retrait de l'habilitation, et précise que les obligations relatives à la protection des informations classifiées auxquelles il a pu être donné accès perdurent au-delà du terme mis à ses fonctions ou à son habilitation. Une fois signé, ce second volet est retourné à l'autorité d'habilitation.

Une personne titulaire d'une décision d'habilitation ne peut en faire état ni révéler son niveau d'habilitation sauf si la communication de ces informations est nécessaire à l'exercice de ses fonctions ou à l'accomplissement d'une mission pour laquelle elle a été habilitée.

5. Habilitation : durée de validité, changement d'affectation et abrogation

Lorsqu'une personne habilitée change d'affectation, son habilitation pour le poste initial prend fin et une autre décision peut être prise, si la nouvelle affectation l'exige, sur la base de l'avis de sécurité en cours.

La décision d'habilitation cesse de produire ses effets :

- soit à la fin de validité figurant sur la décision qui peut être au plus égale à celle de l'avis de sécurité ;
- soit lorsque la fonction ou la mission l'ayant justifiée disparaît, y compris si la date de fin de validité figurant sur la décision est postérieure.

La décision d'habilitation est implicitement abrogée au terme de la durée de validité de la décision ou lorsque la fonction ou la mission cesse, quand bien même la date de fin de validité inscrite sur la décision d'habilitation n'est pas échue.

Une décision d'habilitation peut être abrogée à tout moment ou ne pas être renouvelée si l'intéressé ne remplit plus les conditions nécessaires à sa délivrance.

L'abrogation fait l'objet d'une décision explicite, notifiée à l'intéressé. Lors de la notification, l'intéressé signe le second volet de l'engagement de responsabilité. L'autorité d'habilitation informe la Direction de la Sûreté Publique sous couvert de l'officier de sécurité du Département de l'Intérieur de la décision d'abrogation.

6. Renouvellement

Afin d'éviter une interruption inopportune des conditions d'emploi, dans l'exercice de la fonction ou l'accomplissement de la mission du titulaire d'une décision d'habilitation lorsque la durée d'habilitation, qui ne peut excéder celle de l'avis de sécurité, est inférieure à celle de la fonction ou de la mission la justifiant, la validité de la décision initiale est tacitement prorogée d'une durée maximale de douze mois après la fin de validité de la décision initiale sous réserve qu'une demande de renouvellement, pour la même fonction ou la même mission, soit engagée dans un délai d'un an minimum et, au plus tard, trois mois avant la date d'expiration de l'habilitation en cours.

Cette demande de renouvellement s'accompagne d'un nouveau dossier de demande d'habilitation.

Si la procédure de renouvellement n'est pas engagée dans les délais impartis, aucune prorogation tacite n'est, en revanche, possible. Le titulaire doit quitter sans délai les fonctions ou cesser la mission ayant justifié son habilitation à expiration de la décision initiale.

7. Conservation des décisions

Pendant leur durée de validité, les décisions d'habilitation sont conservées par l'officier de sécurité. Ces documents, qui portent une mention de protection, ne sont en aucun cas remis aux intéressés ni reproduits.

En cas de nécessité, il peut être remis aux intéressés, par l'autorité d'habilitation, un certificat de sécurité délivré pour une mission déterminée et une période limitée. La délivrance de ces certificats peut être déléguée à l'officier de sécurité. Il est de la responsabilité de l'intéressé de procéder ou de faire procéder à la destruction de ce certificat dès le retour de mission.

Les éléments relatifs à l'habilitation des personnels sont conservés cinq ans à compter de la date de péremption de l'habilitation.

8. Répertoire des habilitations

Les officiers de sécurité tiennent pour chacun des deux niveaux de classification, un répertoire :

- des dossiers d'habilitation en cours d'instruction ;
- des habilitations en cours de validité.

Les officiers de sécurité désignés par le Ministre d'État tiennent à jour le répertoire central des habilitations au niveau « Très Secret de Sécurité Nationale » avec classifications spéciales, y compris dans le domaine international.

9. Portée de la décision d'habilitation en matière internationale

Toute décision d'habilitation aux informations ou supports classifiés du domaine national peut, à défaut d'une habilitation spécifique et sous réserve du besoin d'en connaître, donner accès aux informations ou supports classifiés du niveau correspondant et des niveaux inférieurs des domaines internationaux ou confiés aux entités publiques ou privées de la Principauté de Monaco en application d'accords de sécurité conclus à cet effet avec d'autres états.

Une décision d'habilitation aux informations ou supports classifiés du domaine international ne donne pas accès aux informations ou supports classifiés du domaine national.

10. Mise à jour du catalogue des emplois

Un catalogue des emplois est établi pour chaque niveau de classification. Il identifie, via l'octroi d'un numéro de poste, chaque fonction ou mission impliquant nécessairement l'accès à des information et supports classifiés au niveau de classification considéré, ainsi que les noms et prénoms des personnes physiques occupant les postes inscrits au catalogue des emplois. Chaque catalogue des emplois est mis à jour par l'officier de sécurité qui en est le titulaire.

Dès l'ouverture d'un catalogue des emplois, l'officier de sécurité en adresse une copie au Ministre d'État ou Conseillers de Gouvernement-Ministres concernés.

L'officier de sécurité adresse chaque année le catalogue des emplois au Ministre d'État ou Conseillers de Gouvernement-Ministres concernés. A cette occasion, il inscrit les postes qui requièrent un accès au secret de sécurité nationale et réévalue le niveau d'habilitation requis par les fonctions ou missions.

Dans le cas où elles ne nécessitent plus d'accéder au secret de sécurité nationale, l'officier de sécurité en lien avec l'autorité d'habilitation les supprime du catalogue des emplois, notifie aux titulaires des emplois concernés que leur décision d'habilitation est abrogée et leur fait signer le second volet de l'engagement de responsabilité.

Les demandes d'habilitation sont établies en référence au catalogue des emplois et précisent le numéro de poste du catalogue des emplois auquel correspond la demande.

Lorsqu'une demande d'habilitation porte sur une fonction ou une mission nouvelle, ou sur une fonction ou une mission non préalablement inscrite sur un catalogue des emplois, et que la fonction ou la

mission considérée nécessite sans conteste que son titulaire accède à des informations et supports classifiés, l'officier de sécurité met à jour le catalogue des emplois en concertation avec l'autorité d'habilitation.

TITRE IV - MESURES DE SÉCURITÉ APPLICABLES AUX PERSONNES MORALES

Toute personne morale peut être qualifiée pour accéder à des informations et supports couverts par le secret de sécurité nationale si son besoin d'en connaître est reconnu par l'État.

Les exigences à remplir par la personne morale pour être alors considérée comme qualifiée varient selon la nature juridique de la personne morale considérée et selon les finalités justifiant cet accès.

Ces exigences sont détaillées au sein du présent chapitre et synthétisées en Appendice 12.

1. Établissement public de l'État

Tout établissement public sous tutelle de l'État peut accéder à des informations et supports classifiés sous réserve :

- de disposer d'un besoin d'en connaître reconnu par le Ministre d'État ou le Conseiller de Gouvernement - Ministre dont il relève ;
- du respect des mesures définies par le présent arrêté, et, le cas échéant, des directives techniques particulières applicables à son secteur d'activité.

Le responsable de l'établissement est, en sa qualité de responsable d'organisme, responsable du respect des règles de la protection du secret de sécurité nationale en son sein et par son personnel, sous le contrôle du Ministre d'État ou du Conseiller de Gouvernement - Ministre de tutelle.

À ce titre, notamment, le responsable de l'établissement s'assure de l'aptitude de ses locaux à abriter des éléments couverts par le secret de sécurité nationale au regard du présent arrêté, complété, le cas échéant, des directives techniques particulières applicables à son secteur d'activité. En cas d'utilisation d'un système d'information, il s'assure par une homologation du système avec l'Agence Monégasque de Sécurité Numérique, qui est membre de droit de la commission, que ce système est apte à traiter et protéger les informations et supports classifiés qu'il héberge.

Lorsqu'un établissement public candidate à un appel d'offres ou un appel à projet international nécessitant l'accès à des informations et supports classifiés, il se conforme aux exigences de l'autorité contractante étrangère et suit, le cas échéant, la procédure décrite ci-dessous.

2. Opérateurs d'importance vitale

Les opérateurs d'importance vitale ayant besoin d'accéder, en cette qualité, à des informations et supports classifiés n'ont cependant pas à faire l'objet d'une habilitation « personne morale » mais se conforment aux dispositions du présent arrêté, complétée des directives techniques particulières, le cas échéant, applicables, ainsi qu'aux dispositions spécifiques détaillées dans le plan particulier de protection.

En dehors des activités liées à sa désignation en tant qu'opérateur d'importance vitale, un tel opérateur ne peut accéder au secret de sécurité nationale sauf s'il est partie à une convention ou un contrat nécessitant l'accès au secret de sécurité nationale, conformément aux dispositions ci-dessous.

3. Contrat de la commande publique, contrat de sous-traitance ou sous-contrat à la commande publique ou contrat de subvention

Les dispositions de la présente partie s'appliquent, selon les modalités définies ci-après, aux personnes morales, candidates ou parties à un contrat de la commande publique, à un contrat de sous-traitance, à un sous-contrat à un contrat de la commande publique, à un contrat de subvention, ci-après désigné sous le terme générique de « contrat », ou à un contrat exécuté au profit d'une entité étrangère impliquant l'accès du contractant à des informations et supports classifiés (cf. Appendice 14).

L'État doit pouvoir, y compris dans l'exercice de ses missions en matière de sécurité nationale, s'appuyer sur des compétences extérieures, en particulier dans les domaines technique, technologique, industriel ou pour l'optimisation des fonctions de soutien. Il doit alors être en mesure d'échanger en toute

confiance avec ses cocontractants et leurs sous-traitants, y compris des informations et supports couverts par le secret de sécurité nationale.

Ainsi, la procédure d'habilitation propre à la personne morale vise un double objectif :

- à travers les vérifications effectuées dans son cadre sur l'actionnariat de la personne morale, son équipe dirigeante, ses modes de financement, sa stratégie, ses relations contractuelles, elle permet à l'État de prendre des garanties sur la fiabilité de ses co-contractants et leur chaîne de sous-traitance, indépendamment de celle qu'offre la procédure d'habilitation du représentant légal de la personne morale et de ses seuls préposés susceptibles d'accéder à des informations et supports classifiés ;
- à travers les vérifications faites sur l'organisation de la chaîne de sécurité mise en place par la personne morale (cf. paragraphe 3.1.2 ci-après), elle permet de s'assurer que la personne morale dispose de la structure de sécurité nécessaire à la protection des informations et supports classifiés auxquels elle est susceptible d'avoir accès et d'engager pénalement son représentant légal en cas de défaillance de cette structure de sécurité.

L'habilitation de la personne morale impose des exigences plus ou moins étendues, selon qu'elle autorise :

- uniquement l'accès de la personne morale à des informations et supports classifiés, sans détention de ces informations et supports par la personne morale dans ses locaux ou au sein d'un système d'information qu'elle détient ;
- l'accès de la personne morale à des informations et supports classifiés avec détention physique de tout ou partie de ces informations et supports au sein d'au moins l'un de ses établissements ;
- la détention par la personne morale d'informations et supports classifiés au sein d'un système d'information qu'elle détient.

3.1. Avant signature du contrat

3.1.1. Obligation d'information par l'autorité publique contractante :

a) Information relative à l'obligation d'habilitation

Le responsable légal est informé, dans la mesure du possible dès la pré-information et au plus tard dès l'avis d'appel public à la concurrence ou, à défaut de mise en concurrence, dès le début de la procédure de passation, de son obligation d'obtenir, pour lui-même et pour la personne morale qu'il représente, des habilitations de même niveau, préalablement à la signature du contrat, voire dès le dépôt de leur candidature[5].

L'autorité publique contractante l'informe des délais impartis pour fournir les éléments constitutifs des dossiers de demande d'habilitation. Elle lui adresse les formulaires nécessaires ou, à défaut, lui indique les modalités pour se les procurer ainsi que, le cas échéant, le service compétent pour traiter le dossier. Dans le cadre d'un contrat de sous-traitance ou d'un sous-contrat à un contrat de la commande publique impliquant également l'accès à des informations ou supports classifiés, le primo-contractant[6] est tenu à la même obligation d'information à l'égard de ses sous-traitants et sous-contractants.

[5] l'autorité contractante peut en effet exiger des candidats qu'ils soient habilités au moment du dépôt de leur candidature, c'est-à-dire qu'ils soient en mesure de présenter une attestation d'habilitation et, dans le cadre d'un contrat impliquant la détention d'informations et supports classifiés, qu'ils produisent un avis technique d'aptitude physique délivré par la Direction de la Sûreté Publique justifiant de leur capacité à traiter, conserver et transmettre ces informations et supports classifiés au niveau de protection nécessaire.

[6] Primo-contractant : est ainsi dénommé celui qui, dans le cadre d'un marché public, a conclu le contrat avec la personne publique, en qualité de maître d'ouvrage, et qui confie, sous sa responsabilité, tout ou partie de l'exécution de ce contrat à un ou plusieurs sous-traitants ou sous-contractants.

b) Informations relatives à l'obligation de mise en conformité physique en cas de détention d'informations ou supports classifiés

Lorsque le contrat ou sa procédure de passation ou de conclusion impliquent la détention au sein d'un ou plusieurs établissements de la personne morale d'informations et supports classifiés, l'autorité publique contractante informe la personne morale des normes physiques que cette détention implique et dont la conformité aux exigences du présent arrêté est sanctionnée par l'obtention d'un avis d'aptitude physique délivré par la Direction de la Sûreté Publique.

c) Informations relatives à l'obligation d'homologation des systèmes d'information appelés à traiter des informations classifiées et aux procédures de sécurité à mettre en place pour la gestion des articles contrôlés de la sécurité des systèmes d'information

Si l'utilisation d'un système d'information classifié est requise pour l'exécution du contrat, voire dans le cadre de sa passation ou de sa conclusion, l'autorité publique contractante précise que ce système doit faire l'objet, préalablement à son emploi, d'une décision d'homologation avec l'Agence Monégasque de Sécurité Numérique comme membre de droit de la commission d'homologation, et que la mise en œuvre ou l'accès à des articles contrôlés de la sécurité des systèmes d'information (ACSSI) impliquent le respect des mesures de sécurité requises par le présent arrêté.

3.1.2. Préfiguration de la chaîne de sécurité de la personne morale

Pour toutes les démarches engagées avant la signature du contrat, le représentant légal de la personne morale désigne, parmi son personnel, la personne qui exercera la fonction d'officier de sécurité (cf. Appendice 15) pour être le correspondant de l'autorité publique contractante et de l'autorité d'habilitation.

3.1.3. Communication d'informations et supports classifiés en phase précontractuelle

Sauf si l'autorité publique contractante exige l'habilitation dès la candidature, à moins que l'autorité publique contractante lui permette de disposer d'un accès aux informations et supports classifiés dans ses propres locaux. Lorsqu'en phase précontractuelle d'un contrat de la commande publique ou d'un contrat de subvention, l'accès à des informations et supports classifiés par les candidats admis est nécessaire, l'habilitation des personnes physiques employées par la personne morale candidate est possible sans que la personne morale qui les emploie ne soit elle-même habilitée, à condition que la procédure d'habilitation la concernant ait été engagée et que les lieux destinés à abriter les informations et supports classifiés soient aptes à les conserver conformément aux dispositions mentionnées TITRE V Sécurité des lieux.

Le candidat désigne parmi son personnel, au plus tard lorsque sa candidature a été retenue pour établir une offre, les personnes qui accèderont aux informations et supports classifiés dans le strict besoin de l'élaboration de l'offre. Si les personnes désignées ne sont pas titulaires d'une habilitation ou si la décision d'habilitation les concernant n'est pas appropriée aux besoins du contrat, le candidat dépose simultanément une demande d'habilitation pour chacune d'elles. Cette demande est instruite en procédure d'urgence (cf. Titre III §3.1.2). La délivrance d'une décision d'habilitation provisoire des personnes qui accèderont aux informations et supports classifiés dans le strict besoin de l'élaboration de l'offre ne préjuge pas de l'habilitation de la personne morale pour exécuter ledit contrat.

Le candidat dont l'offre n'est pas retenue détenant des informations et supports classifiés est tenu de les restituer à l'autorité contractante dès la notification du rejet de son offre et selon les modalités définies par l'autorité publique contractante. Il remet à l'autorité publique contractante une attestation par laquelle il certifie ne conserver aucune information ni support classifié. Dans le cas où des informations ou supports classifiés ont été transmis sous forme dématérialisée, il fournit une attestation précisant que les documents ont été effacés conformément aux dispositions du présent arrêté. Si les systèmes d'information classifiés et les articles contrôlés de la sécurité des systèmes d'information utilisés pour consulter les informations dématérialisées ne sont plus utilisés dans le cadre d'autres conventions ou contrats, ils sont détruits selon les dispositions du présent arrêté.

3.1.4. Procédure d'habilitation de la personne morale

À l'exception des établissements publics de l'État pour les contrats conclus avec une autorité publique contractante, les personnes morales souhaitant conclure un contrat nécessitant pour son exécution l'accès à des informations et supports classifiés doivent être habilitées. La personne morale doit pouvoir justifier de son habilitation, ainsi que de celle de son responsable légal dès la candidature si l'autorité publique contractante l'exige ou au plus tard au moment de la signature du contrat.

a) Constitution du dossier d'habilitation

Afin d'enclencher la procédure d'habilitation, la personne morale constitue un dossier d'habilitation (cf. Appendice 16). Ce dossier comprend également les éléments nécessaires au lancement de la procédure d'habilitation de son responsable légal.

Si la personne morale a déjà fait l'objet d'une décision d'habilitation à l'occasion d'un précédent contrat, elle est tenue de présenter :

- une attestation d'avis de sécurité (cf. Appendice 17) produite par l'autorité d'habilitation mentionnant la fin de validité de l'avis de sécurité délivré par la Direction de la Sûreté Publique ou, dans le cas où l'autorité d'habilitation est identique à celle ayant délivré la précédente habilitation, une attestation d'habilitation (cf. Appendice 18) ;
- une attestation précisant qu'aucun changement dans la direction ou les statuts de la personne morale n'est intervenu depuis la délivrance de la précédente habilitation.

b) Envoi du dossier d'habilitation

Le dossier d'habilitation est transmis par l'officier de sécurité de la personne morale à l'autorité publique contractante.

Dans le cadre d'un contrat de sous-traitance ou de sous-contrat à un contrat de la commande publique ou à un contrat de subvention, le dossier constitué par le sous-traitant ou le sous-contractant est transmis soit par l'officier de sécurité du primo-contractant à l'autorité publique contractante, après vérification par ce dernier, de la complétude du dossier, soit directement à l'autorité publique contractante. Cette transmission est assortie d'une justification par le primo-contractant du besoin d'habilitation de son sous-traitant ou sous-contractant et d'une copie du plan contractuel de sécurité du contrat que le primo-contractant prévoit de conclure avec le sous-traitant ou le sous-contractant, afin que l'autorité publique contractante puisse apprécier sa conformité avec la réglementation applicable et le plan contractuel de sécurité du contrat principal.

L'envoi du dossier d'habilitation par voie dématérialisée est privilégié.

c) Instruction du dossier d'habilitation

L'autorité publique contractante vérifie la complétude des dossiers d'habilitation. Lorsque le dossier est incomplet, elle informe la personne morale des pièces manquantes et du délai imparti pour les fournir. À expiration de ce délai, la personne morale n'ayant pas fourni les documents nécessaires à la complétude de son dossier est réputée avoir renoncé au contrat.

Le dossier d'habilitation est ensuite vérifié :

- dans le cadre d'un contrat de la commande publique ou d'un appel à projet, par l'autorité publique contractante. Seuls les dossiers des candidats retenus sont ensuite transmis à l'autorité d'habilitation. L'autorité publique contractante informe l'autorité d'habilitation des candidats écartés aux différents stades de la compétition. Elle lui transmet le projet de plan contractuel de sécurité. Seuls les candidats retenus se voient délivrer une décision d'habilitation ;
- dans le cadre d'un contrat de sous-traitance ou d'un sous-contrat, par l'autorité d'habilitation du primo-contractant.

Après cette première phase d'instruction, l'autorité d'habilitation transmet les dossiers d'habilitation à la Direction de la Sûreté Publique sous couvert de l'officier de sécurité du Département de l'Intérieur.

La Direction de la Sûreté Publique mène les investigations nécessaires sur chaque personne morale pour évaluer l'absence de vulnérabilité pour la sécurité nationale.

La Direction de la Sûreté Publique émet un avis de sécurité qui est ensuite transmis à l'autorité d'habilitation. Sauf changement dans la situation de fait ou de droit de la personne morale, la durée de validité de l'avis de sécurité émis est fixée conformément au paragraphe 3.3 du Titre III).

d) Délivrance de la décision d'habilitation

La décision d'habilitation de la personne morale est une décision explicite délivrée par l'autorité d'habilitation (cf. Appendice19), notamment sur le fondement de l'avis de sécurité émis par la Direction de la Sûreté Publique. L'autorité d'habilitation n'est pas liée par cet avis, qui n'est qu'un des éléments parmi les actes préparatoires à sa décision.
La décision d'habilitation comporte une durée de validité fixée par l'autorité d'habilitation ainsi que, s'il y a lieu, un domaine de validité. Cette durée ne peut excéder la durée de validité de l'avis de sécurité émis conformément au paragraphe 3.3 du Titre III).

Dans le cas où la Direction de la Sûreté Publique n'a pas encore rendu son avis, en cas d'urgence justifiée et après saisine de la Direction de la Sûreté Publique, l'autorité d'habilitation, peut exceptionnellement prendre sa décision au vu d'autres éléments utiles en sa possession. L'habilitation ainsi délivrée est provisoire.

Tout changement de fait ou de droit dans la situation de la personne morale de droit privé intervenant après la décision doit être signalé à l'autorité d'habilitation afin de lui permettre, le cas échéant, de reconsidérer sa décision.

La décision de refus d'habilitation (cf. Appendice 20) est notifiée au représentant légal de la personne morale (cf. Appendice 21) dans les conditions prévues au 4.3 du Titre III.

Une décision de refus ne préjuge pas de la conclusion de conventions ou de contrats de toute nature n'impliquant pas la mise en œuvre de mesures de protection du secret de sécurité nationale ou impliquant l'accès au secret de sécurité nationale pour un besoin autre que celui résultant du contrat pour lequel l'habilitation est refusée.

e) Principe de reconnaissance de la décision d'habilitation d'une personne morale

Dans le cas où une personne morale a déjà fait l'objet d'une habilitation à l'occasion d'une convention ou d'un contrat, cette habilitation demeure valable, pour toute autre convention ou contrat passé, dans les limites de date et de domaine de validité de l'habilitation initiale et sauf changement dans la situation de fait ou de droit de la personne morale.

f) Cas particulier des personnes morales de droit étranger soumissionnant à un contrat de droit monégasque nécessitant l'accès à des informations ou supports classifiés

Seule une personne morale établie sur le territoire d'un État avec lequel la Principauté dispose d'un accord général ou spécifique de sécurité (cf. paragraphe 2.1.3 du Titre VII) peut être habilitée dans le cadre d'un contrat de droit monégasque prévoyant l'accès à des informations ou supports classifiés.

La personne morale, de droit étranger souhaitant conclure un tel contrat, est alors tenue, à l'appui de sa candidature, de produire une attestation justifiant de son habilitation, délivrée par l'autorité compétente de l'État dont elle relève. Si la personne morale de droit étranger n'est pas habilitée, le Ministre d'État, en sa qualité d'autorité nationale de sécurité, sollicite l'autorité compétente de l'État, sous la juridiction de laquelle la personne morale de droit étranger se trouve, afin qu'elle procède à son habilitation.

Aucune personne morale de droit étranger ne peut candidater ou présenter une offre lorsque l'exécution du contrat implique la détention au sein d'un établissement de la personne morale d'un système d'information, d'informations ou supports portant la mention *Spécial Monaco*.

g) Cas des personnes morales de droit monégasque soumissionnant dans un cadre international

Lorsqu'une personne morale de droit monégasque, non préalablement habilitée, candidate à un marché ou à un appel à projet au profit d'une autorité contractante de droit étranger, en vue d'un contrat nécessitant l'accès à des informations ou supports classifiés étrangers, elle adresse un dossier d'habilitation au Ministre d'État, en sa qualité d'autorité nationale de sécurité.

Le Ministre d'État transmet le dossier d'habilitation au Conseiller de Gouvernement - Ministre de l'Intérieur en vue de la délivrance d'une décision d'habilitation conformément à la procédure décrite au sein du présent « paragraphe ». Lorsque la procédure d'habilitation permet la délivrance d'une décision d'habilitation, l'officier de sécurité concerné, désigné par le Conseiller de Gouvernement - Ministre de l'Intérieur adresse une attestation d'habilitation (cf. Appendice 18) à l'officier de sécurité de la personne morale candidate à l'habilitation.

Une personne morale déjà habilitée et disposant d'un avis de sécurité en cours de validité s'adresse au Conseiller de Gouvernement - Ministre de l'Intérieur, en tant qu'autorité d'habilitation, pour une extension éventuelle de son domaine d'habilitation. L'officier de sécurité adresse une attestation d'habilitation à l'officier de sécurité de la personne morale candidate.

3.1.5. Lancement de la procédure d'aptitude physique

a) Cas où la personne morale ne dispose pas d'avis technique d'aptitude des locaux et des systèmes d'information contribuant à la sécurité des locaux

Lorsque le contrat implique la détention par la personne morale d'informations et supports classifiés, la personne morale dépose, parallèlement au dossier d'habilitation et le cas échéant d'homologation du ou des systèmes d'information classifiés qui ont vocation à être utilisés pour l'exécution du contrat, un dossier d'aptitude pour chacun des établissements situés sur le territoire de la Principauté dans lesquels elle envisage de conserver des informations et supports classifiés. Ce dossier est destiné à évaluer l'aptitude desdits établissements à assurer la protection des éléments couverts par le secret de sécurité nationale.

Un contrôle initial d'aptitude portant sur les mesures prises par la personne morale pour assurer la sécurité des informations et supports classifiés et, le cas échéant, du système d'information chargé du contrôle d'accès, est effectué par la Direction de la Sûreté Publique et si nécessaire avec l'Agence Monégasque de Sécurité Numérique pour le système d'information, dans le ou les établissement(s) concerné(s), préalablement à la signature de la convention ou du contrat.

À l'issue du contrôle initial, l'avis technique d'aptitude physique délivré par la Direction de la Sûreté Publique est transmis à l'autorité publique contractante et à l'autorité d'habilitation et notifié à la personne morale :

- si l'avis est sans réserve : le responsable légal de la personne morale établit une attestation de conformité physique certifiant la conformité aux normes des locaux du ou des établissements concernés (cf. Appendice 22) ;
- si l'avis fait état de carences dans le dispositif de sécurité mis en œuvre au sein de la personne morale : son responsable légal s'engage à mettre en œuvre toutes les mesures nécessaires à la mise en conformité de son établissement et des systèmes d'information contribuant à la sécurité des locaux, dans un délai défini en liaison avec la Direction de la Sûreté Publique et l'autorité publique contractante et compatible avec la date de début des prestations du contrat nécessitant la détention d'informations et de supports classifiés.

À l'issue des travaux de mise aux normes et, au plus tard, à la date d'échéance du délai défini en liaison avec la Direction de la Sûreté Publique, le responsable légal de la personne morale transmet le certificat de mise aux normes de sécurité physique (cf. Appendice 23) à l'autorité publique contractante et à l'autorité d'habilitation. Cette dernière en informe la Direction de la Sûreté Publique et peut, en lien avec l'autorité publique contractante, la solliciter pour diligenter un contrôle.

b) Cas où un avis technique d'aptitude des locaux et des systèmes d'information contribuant à la sécurité des locaux est déjà en cours de validité

Si les locaux où seront abrités les informations et supports classifiés dans le cadre de la convention ou du contrat considéré disposent d'un avis technique d'aptitude physique en cours de validité et qu'aucun changement des conditions qui ont présidé à sa délivrance n'est intervenu, cet avis suffit. Le responsable d'organisme le communique alors à l'autorité publique contractante et à l'autorité d'habilitation, accompagné d'une attestation de non-changement des conditions qui ont présidé à sa délivrance.

Il en va de même pour le système d'information chargé du contrôle d'accès.

3.1.6. Lancement de la démarche d'homologation

Lorsque l'exécution de la convention ou du contrat prévoit l'utilisation d'un système d'information classifié, la personne morale engage parallèlement à la procédure d'habilitation et à la démarche d'aptitude physique, une démarche d'homologation conformément aux modalités précisées au paragraphe 1 du Titre VI.

Si la personne morale dispose déjà d'un système d'information classifié homologué au niveau requis, la décision d'homologation demeure valide. La personne morale adresse alors une copie de la décision d'homologation à l'autorité publique contractante, ainsi qu'à l'autorité d'habilitation.

3.2. Exécution du contrat

3.2.1. Décisions administratives préalables au lancement de l'exécution des prestations du contrat nécessitant l'accès à des informations ou supports classifiés

a) Finalisation du dossier d'aptitude physique

Si les attestations d'aptitude physique ne sont pas parvenues dans le délai prédéfini ou si des carences sont constatées lors des contrôles effectués par la Direction de la Sûreté Publique conformément au paragraphe 3.1.5 a) du Titre IV, une mise en demeure de se conformer aux prescriptions du présent arrêté est effectuée par l'autorité publique contractante. Le défaut d'exécution des travaux de mise en conformité fait obstacle à l'exécution du contrat et engage la responsabilité du représentant légal de la personne morale.

b) Finalisation de la démarche d'homologation des systèmes d'information classifiés

Dans le cas où la procédure d'homologation du système d'information classifié devant être utilisé pour l'exécution du contrat n'a pas été finalisée avant la signature du contrat, l'homologation du système doit intervenir au plus tard avant le début des prestations du contrat nécessitant son utilisation selon un calendrier établi en liaison avec l'autorité publique contractante et l'Agence Monégasque de Sécurité Numérique.

L'autorité publique contractante peut, en parallèle de la démarche d'homologation ou de confirmation de l'existence d'une décision d'homologation en cours de validité, solliciter auprès de l'Agence Monégasque de Sécurité Numérique ou d'un Prestataire d'Audit de la Sécurité des Systèmes d'Information (PASSI), un contrôle d'aptitude visant à vérifier la capacité du système d'information à traiter des informations et supports classifiés au niveau requis conformément aux exigences du présent arrêté.

c) Habilitation des personnes physiques participant à l'exécution du contrat prévoyant l'accès à des informations ou supports classifiés

Sont seules autorisées à connaître des informations et supports classifiés pour le compte d'une personne morale habilitée les personnes rattachées à cette dernière qui ont fait l'objet d'une décision d'habilitation délivrée à l'issue de l'une des procédures d'habilitation définies au paragraphe 3 du Titre III.

Cette décision doit intervenir avant le début d'exécution par la personne physique considérée de ses missions nécessitant l'accès à des informations ou supports classifiés.

Afin d'éviter tout retard dans le lancement de l'exécution des prestations du contrat nécessitant l'accès à des informations ou supports classifiés, les procédures d'habilitation des personnes non encore habilitées sont lancées dès la signature du contrat, ou en amont de celle-ci, si la conclusion du contrat avec la personne morale considérée est certaine.

Sauf exception relative aux administrateurs et auditeurs des systèmes d'information classifiés et internes à la personne morale (cf. procédure d'habilitation de droit commun), le niveau et la durée de validité de cette habilitation ne peuvent excéder ceux de l'habilitation de la personne morale.

Un catalogue des emplois, tenu par l'officier de sécurité de la personne morale, est établi et mis à jour selon les modalités définies au paragraphe 8 du Titre III, complétées le cas échéant des directives techniques particulières applicables et des stipulations du plan contractuel de sécurité. Ce catalogue des emplois tient lieu de répertoire des postes nécessitant l'accès à des informations ou supports classifiés. Il indique le niveau, les dates de délivrance et de fin de validité des décisions d'habilitation du personnel. Une mise à jour annuelle est réalisée et, à cette occasion, le représentant légal de la personne morale vérifie que les personnes habilitées ont effectivement eu accès à des informations et supports classifiés pour le niveau concerné et supprime, le cas échéant, les fonctions et missions ne nécessitant plus d'accéder au secret de sécurité nationale.

Dès lors qu'une personne physique est susceptible, dans l'exécution de son contrat de travail, de connaître ou de détenir des informations et supports classifiés, son contrat de travail comporte, dans la mesure du possible, une clause de protection du secret de sécurité nationale conforme à la clause-type figurant à l'Appendice 13. En cas de changement d'affectation amenant le salarié à travailler dans les conditions définies au premier alinéa, le contrat de travail fait l'objet d'un avenant écrit conforme aux présentes dispositions. Les parties au contrat de travail peuvent compléter ou adapter la clause-type selon les spécificités dudit contrat sans lui être contraire.

3.2.2. Obligations du titulaire

a) Devoir de discrétion de la personne morale habilitée

La personne morale et son personnel titulaire d'une décision d'habilitation ne peut publiquement en faire état ni s'en prévaloir. Elle ne peut communiquer à des tiers cette décision, ni aucune information résultant des informations et supports auxquels elle a accès pour l'exécution des prestations du contrat nécessitant l'accès à des informations et supports classifiés, sauf autorisation expresse de l'autorité publique contractante ou en réponse à des procédures contractuelles qui l'exigeraient.

b) Obligations du responsable légal

En sa qualité de responsable d'organisme, le responsable légal de la personne morale s'engage, sous sa responsabilité pénale et contractuelle et celle de la personne morale, à assurer la protection des informations et supports classifiés dont son organisme et son personnel ont à connaître et le plan contractuel de sécurité qu'il a conclu avec l'autorité publique contractante.

À ce titre, il approuve la politique de sécurité des systèmes d'information et la politique de protection du secret de sécurité nationale de son organisme et met en place, sous sa responsabilité, la chaîne de sécurité animée par l'officier de sécurité.

La chaîne fonctionnelle de protection du secret est organisée de façon à veiller à la mise en œuvre de l'ensemble des dispositions relatives à la protection du secret de sécurité nationale au sein de l'organisme. Elle est structurée de façon à :

- veiller à la bonne mise en œuvre des mesures de sécurité applicables aux personnes physiques et morales ;

- garantir la protection physique et logique des informations et supports classifiés, y compris les systèmes d'information classifiés conformément aux Titres V et VI ;
- assurer la gestion des informations et supports classifiés conformément au Titre VII ;
- être en capacité de détecter dans les meilleurs délais toute compromission avérée ou suspectée du secret sécurité nationale.

Chaque responsable d'organisme ayant accès au secret de sécurité nationale élabore une politique de protection du secret en déclinaison de l'arrêté ministériel 2016-723, modifié, et, le cas échéant, des directives techniques particulières applicables à son organisme. S'agissant de la sécurité des systèmes d'information classifiés, cette politique se conforme aux recommandations de l'Agence Monégasque de Sécurité Numérique.

Cette politique peut être plus restrictive que la réglementation sous réserve qu'elle ne s'y oppose pas. Elle :

- précise la déclinaison au sein de l'organisme de la chaîne fonctionnelle de protection du secret, et, le cas échéant, des chaînes de la sécurité des systèmes d'information classifiés et de la sécurité des articles contrôlés de la sécurité des systèmes d'information ;
- définit les exigences en ce qui concerne l'habilitation, ainsi que la formation et la sensibilisation à la protection du secret et la sécurité des systèmes d'information et des articles contrôlés de la sécurité des systèmes d'information ;
- précise les mesures de protection et de gestion des informations et supports classifiés, des systèmes d'information classifiés, des articles contrôlés de la sécurité des systèmes d'information et des lieux abritant des éléments couverts par le secret de sécurité nationale. À ce titre, la politique de protection du secret comprend les mesures de contrôle nécessaires pour limiter l'accès des personnes non qualifiées aux emprises de l'organisme abritant des informations et supports classifiés et comprend, pour les organismes utilisant des systèmes d'information classifiés, les exigences relatives à leur sécurité. Ces exigences sont élaborées par l'officier de sécurité ;
- fixe les obligations en matière de contrôle et de suivi de l'activité liée aux habilitations, aux lieux abritant des éléments couverts par le secret de sécurité nationale, aux informations et supports classifiés, aux systèmes d'information classifiés et aux articles contrôlés de la sécurité des systèmes d'information ;
- établit les procédures de remontée de l'information et les mesures de protection à mettre en œuvre en cas de compromission avérée ou supposée du secret de sécurité nationale ou d'articles contrôlés de la sécurité des systèmes d'information.

Pour les opérateurs d'importance vitale, cette politique est conforme aux engagements pris dans le cadre du plan particulier de protection.

Pour les organismes accédant à des informations et supports classifiés au titre d'une convention ou d'un contrat selon les modalités définies aux paragraphe 3 et 4 du Titre IV, cette politique est conforme aux stipulations du ou des plans contractuels de sécurité applicables à l'organisme.

La politique de protection du secret fait l'objet d'une révision à intervalles réguliers ou en cas de nécessité afin de garantir la pertinence, l'efficacité et l'adéquation des mesures. En particulier, elle est revue lorsqu'un incident de sécurité a abouti à divulguer ou rendre possible la divulgation d'un secret de sécurité nationale.

c) Obligations spécifiques des primo-contractants

En cas de recours à des sous-traitants ou sous-contractants pour l'exécution de son contrat qui ont besoin, à cet effet, d'accéder à des informations et supports classifiés, le primo-contractant en informe l'autorité publique contractante au moment de la signature du contrat, sauf impossibilité caractérisée, et justifie leur besoin d'en connaître pour exécuter le contrat.

Lorsque l'autorité publique contractante reconnaît ou identifie le besoin du sous-traitant ou du sous-contractant d'accéder à des informations et supports classifiés, le primo-contractant informe le sous-traitant ou le sous-contractant pressenti.

Le sous-traitant ou le sous-contractant pressenti constitue alors un dossier de demande d'habilitation de la personne morale et le transmet à l'autorité d'habilitation selon les modalités décrites au paragraphe 3.1.4 du Titre IV

L'accès à des informations et supports classifiés par un sous-traitant ou un sous-contractant ne peut se faire que sous couvert d'un contrat comportant un plan contractuel de sécurité approuvé par l'autorité publique contractante de référence et sous réserve de l'habilitation préalable du sous-traitant ou du sous-contractant et de ses employés appelés à en connaître. Cet accès est strictement limité au besoin d'en connaître de sous-traitants ou sous-contractants, eu égard aux prestations définies par le sous-traité ou le sous-contrat.

Dans le cas où l'autorité publique contractante reconnaît ou identifie le besoin du sous-traitant ou du sous-contractant d'accéder à des informations et supports classifiés, le primo-contractant informe le sous-traitant ou le sous-contractant pressenti.

3.2.3. Mesures de sécurité liées à la détention d'informations et supports classifiés

Durant l'exécution du contrat, le titulaire est tenu de mettre en œuvre les mesures de sécurité requises pour assurer la protection des informations et supports classifiés. Ces mesures sont détaillées dans un plan contractuel de sécurité partie intégrante au contrat.

a) Plan contractuel de sécurité

Toute convention ou tout contrat nécessitant l'accès à des informations ou supports classifiés comporte un plan contractuel de sécurité qui énumère les exigences de sécurité relatives à la convention ou au contrat et détermine le besoin d'en connaître. Il stipule que des inspections, contrôles ou audits peuvent être organisés dans les établissements de la personne morale abritant des informations et supports classifiés aux fins de s'assurer de leur condition de protection.

Le plan contractuel de sécurité répond aux exigences mentionnées à l'Appendice 24. Celles-ci peuvent être adaptées par l'autorité publique contractante en liaison avec le titulaire sans pouvoir leur être contraires. Il doit mentionner, entre autres, la classification suivant le niveau retenu (*Secret de sécurité Nationale, Très Secret de Sécurité Nationale*) et la nature (Spécial Monaco, Spécial Monaco-*pays tiers*, autres) des informations et supports classifiés.

Lorsque son contenu le justifie, le plan contractuel de sécurité est classifié en tout ou partie. Il peut être modifié en cours d'exécution de la convention ou du contrat à l'initiative de l'autorité publique contractante ou sur proposition de la personne morale.

L'autorité publique contractante valide le plan contractuel de sécurité des éventuels sous-traités et des sous-contrats au contrat principal.

Le plan contractuel de sécurité du primo-contrat intègre la liste des sous-traités et des sous-contrats concernés identifiés lors de la rédaction du plan contractuel de sécurité, les travaux réalisés, leurs dates prévisionnelles de début et de fin d'exécution ainsi que les informations et supports classifiés dont la connaissance est nécessaire à leur réalisation.

Le suivi des plans contractuels de sécurité des sous-traités ou des sous-contrats est effectué par le contractant principal sous la responsabilité et le contrôle de l'autorité publique contractante de référence. Les modalités de ce contrôle peuvent être définies dans des clauses particulières ou dans le plan contractuel de sécurité du contrat principal.

b) Inspections, contrôles et audits

Conformément aux stipulations du plan contractuel de sécurité, la personne morale se soumet à des inspections, contrôles et audits périodiques de l'autorité publique contractante ou de la Direction de la Sûreté Publique, tout au long de l'exécution du contrat et après son exécution si elle continue à détenir des informations et supports classifiés.

Des contrôles d'aptitude sont diligentés périodiquement dans ses locaux pour vérifier le respect de la protection du secret de sécurité nationale pour l'exécution de chaque convention et contrat.

Ces inspections, contrôles et audits incluent les systèmes d'information s'ils traitent d'informations classifiées ou s'ils contribuent à la sécurité des locaux abritant des éléments couverts par le secret de sécurité nationale.

Lorsqu'une inspection, un contrôle ou un audit fait apparaître que les locaux ou les systèmes d'information de la personne morale ne sont plus conformes à la réglementation et aux normes fixées par le(s) plan(s) contractuel(s) de sécurité actif(s), la Direction de la Sûreté Publique informe la personne morale, l'autorité publique contractante et l'officier de sécurité désigné par le Conseiller de Gouvernement - Ministre de l'Intérieur de la non-conformité de ces locaux. Le responsable légal de la personne morale fait procéder à leur mise en conformité et prend toutes les mesures nécessaires pour assurer la sécurité des informations et supports classifiés pendant les travaux de réaménagement.

Après chaque mise en conformité, un contrôle donnant lieu à un nouvel avis d'aptitude des locaux concernés est effectué par la Direction de la Sûreté Publique. Lorsqu'il apparaît que des informations et supports classifiés sont conservés dans des lieux qui ne sont pas de nature à garantir leur protection, la Direction de la Sûreté Publique en informe l'autorité d'habilitation ainsi que l'autorité publique contractante. Cette dernière peut mettre en demeure la personne morale d'effectuer les travaux nécessaires à leur mise en sécurité dans un délai de trois mois à compter de la notification de la mise en demeure. À l'issue d'une mise en demeure infructueuse, l'autorité d'habilitation peut abroger la décision d'habilitation de la personne morale. Tout refus de mise en conformité ou tout retard pour se mettre en conformité peut être considéré comme un non-respect des engagements conventionnels ou contractuels en matière de protection du secret de sécurité nationale et entraîner le prononcé des sanctions prévues par la convention ou le contrat, sans préjudice d'éventuelles sanctions pénales.

3.3. Résiliation et terme du contrat

3.3.1. Fin de l'habilitation de la personne morale

Si la décision d'habilitation arrive à expiration au cours de l'exécution d'un contrat visé par les présentes dispositions, une demande de renouvellement est déposée auprès de l'autorité d'habilitation dans l'année et, au plus tard, six mois avant cette date d'expiration. La durée de validité de la décision est alors prorogée dans les conditions définies au paragraphe 6 du Titre III.

L'habilitation peut être abrogée en cours de validité ou peut ne pas être renouvelée si la personne morale de droit privé ne remplit plus les conditions nécessaires à sa délivrance.

L'abrogation de la décision d'habilitation (cf. Appendice 20) est notifiée au représentant légal de la personne morale dans les mêmes formes que le refus d'habilitation (cf. paragraphe 4.3 Titre III).

L'abrogation de la décision d'habilitation n'entraîne pas nécessairement la résiliation du contrat, en particulier si l'accès aux informations et supports classifiés n'est plus nécessaire à son exécution. Les conséquences d'une telle décision doivent ainsi être examinées au cas par cas.

3.3.2. Mesures particulières en fin d'exécution du contrat

Lorsque les prestations du contrat nécessitant l'accès à des informations et supports classifiés ont été réalisées, la personne morale en informe dans le délai d'un mois l'autorité publique contractante qui lui précise la destination à donner aux informations et supports classifiés qu'elle détenait jusqu'alors. À cet effet, les modalités de destruction, d'archivage ou de restitution des informations et supports classifiés ainsi que celles portant sur le démantèlement des systèmes d'information classifiés sont définies par l'autorité

publique contractante en liaison avec les services concernés dans une fiche de clôture du plan contractuel de sécurité. Le plan contractuel de sécurité du contrat est clôturé sauf s'il a donné lieu à un ou plusieurs sous-traités ou sous-contrats. Dans ce cas, il ne peut être clôturé qu'après la clôture des plans contractuels de sécurité de chaque sous-contrat.

Si la personne morale conserve des informations et supports classifiés après la clôture du plan contractuel de sécurité, elle est tenue de :

- maintenir la protection du secret sécurité nationale ;
- disposer d'une décision d'habilitation pour elle-même, valide et cohérente avec les informations et supports classifiés conservés ;
- maintenir les habilitations de son personnel ayant le besoin d'en connaître ;
- entretenir les aptitudes physiques des locaux abritant des informations et supports classifiés ;
- tenir à jour les dossiers d'homologation des systèmes d'information classifiés et maintenir l'homologation de ces systèmes.

Un suivi de ces obligations est assuré par la Direction de la Sûreté Publique et l'Agence Monégasque de Sécurité Numérique, chacun en ce qui le concerne.

4. Mesures de sécurité applicables en cas de cessation d'activité ou de dissolution de la personne morale

Le plan contractuel de sécurité précise les modalités de destruction, d'archivage ou de restitution des informations et supports classifiés détenus par la personne morale, en cas de cessation d'activité ou de dissolution de cette dernière.

TITRE V - SÉCURITÉ DES LIEUX

1. Principe de défense en profondeur et analyse de risques

La protection du secret de sécurité nationale appelle la mise en place de mesures de sécurité plus ou moins élevées selon qu'il s'agit de :

- lieux dit « abritants », c'est-à-dire de lieux ayant vocation à conserver des informations et supports classifiés, quel qu'en soient le niveau et le volume ;
- ou de lieux, telles que les salles de réunion, où des informations et supports classifiés sont communiqués, échangés ou manipulés mais où ces informations et supports n'ont pas vocation à être conservés.

La liste des lieux visés abritants est établie de façon précise et limitative par arrêté du Ministre d'État. Cet arrêté est actualisé chaque année.

Les réseaux informatiques et données informatisées qui ont fait l'objet de mesures de classification destinées à restreindre leur diffusion ou leur accès présentent un caractère de secret de sécurité nationale. Il en découle que les lieux dans lesquels sont conservés ces réseaux informatiques et données informatisées sont des lieux abritants.

Dans les deux cas, le système de protection déployé est destiné à protéger les informations et supports classifiés contre toute menace, interne ou externe, qui pourrait mettre en cause leur disponibilité, leur intégrité, leur confidentialité et leur traçabilité et à empêcher qu'une personne non qualifiée puisse y accéder. Il s'appuie sur une analyse de risques et s'inscrit dans une logique de défense en profondeur qui repose sur des barrières successives répondant aux critères suivants :

- être multifonctions, c'est-à-dire comporter plusieurs dispositifs successifs, complémentaires, de nature différente, associés ou combinés à un ou plusieurs dispositifs de détection-alarme reposant eux-mêmes sur des principes différents ;
- être homogènes, c'est-à-dire garantir la même efficacité en tous points, l'atteinte aux informations et supports classifiés se mesurant toujours dans la zone de moindre résistance et la valeur d'un système équivalant à celle de son élément le plus faible ;
- être dissuasives, c'est-à-dire contribuer à réduire le risque d'une tentative d'atteinte aux informations et supports classifiés ;
- être contrôlées, c'est-à-dire être testées fréquemment afin de vérifier qu'il est en état opérationnel ;
- être traçables, c'est-à-dire fournir tout moyen pouvant apporter un historique du fonctionnement des différents composants.

La sécurité des lieux résulte de l'articulation des différentes mesures de protection définies à l'Appendice 25. La sécurité des lieux abritants repose sur une articulation de l'ensemble de ces mesures, conforme au niveau de classification des informations et supports qu'ils conservent. Les lieux où des informations et supports classifiés sont communiqués ou manipulés sans y être conservés garantissent *a minima* le respect des règles relatives à la classe du bâtiment et/ ou de l'emprise, ainsi qu'à la classe du local (cf. 2. a) et b) de l'Appendice 26). Il est à noter qu'un lieu où est installé ou conservé un système d'information classifié est considéré comme un lieu abritant.

2. Protection physique

2.1. Règles générales

Conformément au principe de défense en profondeur, la sécurité des informations et supports classifiés est assurée par un ensemble de mesures destinées à garantir l'intégrité des bâtiments, des lieux qui abritent les meubles dans lesquels ils sont conservés ou dans lesquels un système d'information classifié est déployé, ainsi que par la fiabilité des meubles dans lesquels ils sont conservés. Ces mesures ont pour

objet d'éviter toute dégradation, compromission ou risque de compromission des informations et supports classifiés.

Le degré de sécurité physique à appliquer pour assurer la protection des lieux abritants dépend des niveaux de classification et, le cas échéant, de protection logique des informations et supports classifiés qu'ils abritent et des menaces auxquelles ils sont exposés.
Le dispositif global de protection et la solution technique retenue reposent sur les conclusions rendues par l'autorité compétente qui s'appuient sur l'évaluation des menaces et des contraintes inhérentes à l'environnement du site, ainsi que sur les méthodes de travail et de gestion des informations et supports classifiés concernés (par exemple, en fonction de la circulation de ces informations et supports dans le site et du nombre de personnes y ayant accès).
La sécurisation physique des accès d'énergie, des locaux techniques et des moyens de communication participe également de la protection physique des informations et supports classifiés.
Les informations et supports classifiés qui ne sont plus sous la surveillance de l'utilisateur font l'objet, selon les risques liés à leur environnement, de mesures de protection adaptées, déterminées par l'autorité compétente.

2.2. Dispositif global de protection

Le dispositif de protection physique des informations, supports et systèmes d'information classifiés est constitué de plusieurs barrières successives, que sont :
- l'emprise du bâtiment et/ou le bâtiment lui-même ;
- les locaux qui contiennent le meuble ou les éléments du système d'information ;
- le meuble dans lequel sont conservés les informations et supports classifiés ;
- et, pour les systèmes d'information, la sécurité logique à l'égard des utilisateurs du système et éventuellement, à l'égard des ressources du système d'information.

Le degré de protection de l'ensemble du dispositif est fonction du niveau de protection assuré par les mesures appliquées à chacune de ces barrières. Les types de mesures de sécurité physique, leur articulation selon le type de barrière et les mesures spécifiques aux niveaux supérieurs de classification sont détaillés de l'Appendice 25 à 28.

Compte tenu de leur environnement particulier, les lieux dans lesquels sont conservés des informations et supports classifiés et, le cas échéant, des systèmes d'information classifiés, peuvent faire l'objet de dispositions de sécurité adaptées.

Sur un territoire étranger et compte tenu de leur environnement particulier, les organismes détenteurs d'informations et supports classifiés relevant administrativement ou contractuellement de la juridiction de la Principauté, doivent, sauf urgence ou contrainte majeure (opérationnelle, etc.), appliquer les mesures de protection décrites dans la présente instruction.

Lorsque les circonstances imposent la détention et la production d'informations et supports classifiés mais ne permettent pas la mise en place des moyens adéquats de sécurité physique, des mesures compensatoires sont prises afin de conserver le même niveau de protection. Ces mesures de substitution procèdent d'une analyse précise des risques, réalisée par le responsable du site concerné. Elles sont évaluées par la Direction de la Sûreté Publique. Le Conseiller de Gouvernement - Ministre de l'Intérieur est destinataire de l'analyse de risques et de l'avis la Direction de la Sûreté Publique. Le niveau de protection doit, en toute hypothèse, être suffisant pour permettre la prise en compte du délai réel d'intervention avant la compromission.

3. Contrôle d'accès

3.1. Contrôle physique des accès

Le contrôle d'accès s'intègre dans un système de management de la sûreté qui comprend aussi bien des moyens de détection que de surveillance. Il combine des moyens techniques, organisationnels et humains et a pour objectif :

- de filtrer les flux de circulation, les individus et les véhicules qui souhaitent entrer ou sortir d'un site, d'un bâtiment ou d'un local. L'accès à un local technique d'un système d'information classifié fait l'objet de mesures de protection physique supplémentaires ;
- d'empêcher ou de limiter les déplacements de personnes non autorisées.

Il peut s'appuyer sur la création de zones protégées et réservées.

3.1.1. Zones protégées

La création d'une zone protégée est obligatoire pour les lieux abritant des informations et supports classifiés au niveau *Secret de Sécurité Nationale* et au niveau *Très Secret de Sécurité Nationale*.

Une zone protégée est un local ou un terrain clos rattaché à une entreprise, un service, un établissement, public ou privé, intéressant la sécurité nationale, auquel l'accès est soumis à autorisation afin de protéger les installations, les matériels, le secret des recherches, des études ou des fabrications ou les informations et supports classifiés qui s'y trouvent.

Elle est créée par arrêté ministériel et permet d'assurer aux lieux abritant des informations et supports protégés par le secret de sécurité nationale une protection juridique, et notamment pénale, contre les intrusions, que ces lieux soient rattachés à un service de l'État, à un établissement public ou à toute personne physique ou morale, publique ou privée, intéressant la sécurité nationale.

L'ensemble des accès est contrôlé en permanence afin d'éviter toute pénétration intentionnelle ou fortuite dans la zone protégée. Ce contrôle inclut des mécanismes d'authentification garantissant l'accès aux seules personnes autorisées, au moyen d'un système d'information homologué.

Les limites de la zone protégée et les mesures d'interdiction d'accès dont elle fait l'objet sont rendues apparentes afin de ne pas être franchies par inadvertance. À cet effet, des panneaux sont disposés en nombre suffisant aux endroits appropriés.

Par principe, l'autorisation de pénétrer dans une zone protégée est donnée par le chef du service, de l'établissement ou de l'entreprise, selon les directives et sous le contrôle du Ministre d'État ou du Conseiller de Gouvernement-Ministre ayant déterminé le besoin de protection.

Le Ministre d'État peut diligenter une enquête administrative afin de s'assurer que le comportement de la personne, physique ou morale, n'est pas incompatible avec l'accès à cette zone ou ne l'est pas devenu.

L'officier de sécurité du site saisit alors la Direction de la Sûreté Publique sous couvert de l'officier de sécurité du Département de l'Intérieur d'une demande d'enquête administrative (cf. Appendice 2) avant d'autoriser l'accès à la zone protégée. Après instruction du dossier et sur la base des éléments qu'il a pu réunir, la Direction de la Sûreté Publique émet un avis qu'il adresse au demandeur. Cet avis peut être favorable, défavorable ou réservé. La durée de validité de cet avis est de 5 ans au niveau « *Très Secret de Sécurité Nationale* » et 7 ans au niveau « *Secret de Sécurité Nationale* ».

L'autorisation d'accéder à une zone protégée est délivrée par écrit et peut être retirée à tout moment dans les mêmes formes.

Sans préjudice des sanctions disciplinaires, toute personne non autorisée s'introduisant ou tentant de s'introduire dans une zone protégée encourt la peine prévue à l'article 19 de la loi n° 1.430 du 13 juillet 2016 suscitée.

3.1.2. Zones réservées

La création d'une zone réservée, par définition incluse dans une zone protégée et pouvant même lui correspondre, vise à apporter une protection complémentaire. Elle est obligatoire pour les lieux abritant des informations et supports classifiés au niveau « *Très Secret de Sécurité Nationale* ».

Les zones réservées sont créées par décision du responsable d'organisme. Chaque Conseiller de Gouvernement- Ministre veille à ce que des zones réservées soient créées dans tous les organismes qui, de

manière habituelle, élaborent, traitent, reçoivent ou détiennent des informations et supports classifiés au niveau *Très Secret de Sécurité Nationale.*

Les mesures de sécurité propres aux zones réservées sont définies en Appendice 28.

Lorsqu'un organisme est amené à traiter ou détenir de tels informations et supports au niveau *Très Secret* pour des raisons opérationnelles et de manière temporaire, le responsable d'organisme crée une zone réservée temporaire soumise aux mesures de sécurité détaillées en Appendice 28, y compris lorsque les conditions de création d'une zone protégée ne sont pas réunies.

3.2. Accès des personnes non habilitées dans le cadre de l'exécution d'un contrat « sensible »

3.2.1. Mesures de sécurité relatives au contrat sensible

Un contrat « sensible » est un contrat, quel que soit son régime juridique ou sa dénomination, qui n'implique pas l'accès à des informations ou supports classifiés mais dont l'exécution nécessite l'accès à un lieu abritant des éléments couverts par le secret de sécurité nationale.

Il s'agit notamment des contrats de gardiennage, d'entretien ou de maintenance de lieux abritant des éléments couverts par le secret de sécurité nationale.

Sauf si un accord de sécurité impose, au cas d'espèce, des règles plus strictes, il n'y a pas lieu de procéder à l'habilitation de la personne morale ni à celle de son personnel. En revanche, l'autorité publique contractante ou le primo-contractant dans le cadre d'un contrat sensible en sous-traitance ou sous-contrat à un contrat classifié (cf. paragraphe 3 Titre IV) ou sensible fait figurer au contrat les stipulations nécessaires pour garantir que ses conditions d'exécution ne portent pas atteinte au secret de sécurité nationale. Ces stipulations prennent la forme d'une clause de protection du secret sur le modèle de clause-type présenté en Appendice 29, complétée ou adaptée, le cas échéant, selon les spécificités du contrat considéré, sans toutefois être contraire ou moins disante que le modèle.

3.2.2. Mesures de sécurité relatives à la personne morale exécutant un contrat sensible

L'autorité contractante peut solliciter de la Direction de la Sûreté Publique que soit diligentée une enquête administrative à l'encontre d'une personne morale, ainsi que de ses éventuels sous-contractants et leur personnel, sur la base des éléments fournis à l'occasion de la procédure de passation du marché ou lors de la demande d'acceptation du sous-contractant.

La Direction de la Sûreté Publique adresse son avis, consigné sur une fiche navette (cf. Appendice 30), à l'autorité contractante et à l'officier de sécurité concerné.

Lorsque l'avis révèle un fait pouvant constituer un motif d'exclusion, l'autorité publique contractante peut écarter la candidature de la personne morale concernée, sauf si des raisons impérieuses imposent le recours à ladite personne morale, que le marché en cause ne peut être confié qu'à ce seul opérateur économique et qu'un jugement définitif de la Principauté ou d'une juridiction d'un État membre de l'Union européenne n'exclut pas expressément l'opérateur concerné des marchés.

3.2.3. Mesures de sécurité relatives au personnel de la personne morale exécutant un contrat sensible

Le personnel de la personne morale chargé d'exécuter la prestation prévue par le contrat sensible peut préalablement faire l'objet d'une enquête administrative par la Direction de la Sûreté Publique.

Il est recommandé d'insérer une clause de protection du secret (cf. Appendice 13, point 5) dans les contrats de travail des personnes exécutant un contrat sensible. Lorsqu'un salarié exécutant un contrat de travail ordinaire se trouve soumis aux conditions applicables aux contrats sensibles, un avenant conforme aux présentes dispositions peut être introduit dans son contrat de travail.

Les parties contractantes peuvent compléter ou adapter la clause du contrat de travail mentionnée précédemment selon les spécificités dudit contrat sensible sans jamais lui être contraires.

3.2.4. Accès des personnes non habilitées à des lieux abritant des éléments couverts par le secret de sécurité nationale, dans le cadre de la législation du travail

Les règles de protection du secret de sécurité nationale s'appliquent à toute inspection ou à tout contrôle prévu par des dispositions législatives ou réglementaires.

En matière de législation sociale, les personnes morales de droit privé liées par un contrat prévoyant l'accès à des informations et supports classifiés (cf. Titre IV) doivent concilier l'impératif de protection du secret de sécurité nationale avec la nécessité d'appliquer les règles propres au droit du travail, relatives aux contrôles et inspections (par exemple les médecins ou les inspecteurs du travail, les ingénieurs de prévention, les instances représentatives du personnel). Lorsque la personne morale de droit privé détient des éléments couverts par le secret de sécurité nationale conformément aux dispositions précédentes, seule l'autorité responsable du site auquel le lieu abritant est rattaché, après contrôle de la qualité et vérification de l'identité des contrôleurs ou inspecteurs, les autorise à pénétrer accompagnées dans les zones où sont abrités des informations et supports classifiés.

Bien que les contrôleurs ou inspecteurs s'engagent à ne rien révéler des secrets de fabrication ou procédés d'exploitation qui pourraient leur être révélés à cette occasion, sous peine d'encourir des poursuites sur le fondement de la violation du secret professionnel, ils ne sont nullement autorisés, sauf à être dûment habilités et à justifier du besoin d'en connaître pour l'exercice de leur fonction ou l'accomplissement de leur mission, à accéder ou à prendre connaissance d'informations et supports classifiés, cet accès restant subordonné au respect des règles énoncées par le présent arrêté.

Si, dans des circonstances exceptionnelles, l'un d'eux accède fortuitement à un secret de sécurité nationale, il s'expose, en cas de divulgation, aux peines prévues à l'article 19 de la loi n° 1.430 du 13 juillet 2016, suscitée.

3.2.5. Exception en cas de secours, de sécurité ou d'incendie

Le personnel d'intervention en matière de secours, de sécurité ou d'incendie, agissant dans des cas d'urgence avérée, est autorisé à procéder aux opérations requises par la situation sans être soumis aux formalités ordinaires

Si, dans des circonstances exceptionnelles, l'une de ces personnes accède fortuitement à un secret de sécurité nationale, elle s'expose, en cas de divulgation, aux peines prévues à l'article 19 de la loi n° 1.430 du 13 juillet 2016, suscitée.

3.3. Vérification de la protection physique par la Direction de la Sûreté Publique

3.3.1. Règles générales

Les lieux abritant des informations et supports classifiés font l'objet d'un avis technique d'aptitude physique à un niveau au moins égal au niveau de classification des informations et supports qu'ils ont vocation à abriter.

Cet avis obligatoire est délivré par la Direction de la Sûreté Publique.

3.3.2. Evaluation de la sécurité physique

La Direction de la Sûreté Publique et l'Agence Monégasque de Sécurité Numérique pour la partie informatique s'assurent de la cohérence de l'analyse de risques et des moyens mis en œuvre pour contrer une atteinte aux informations et supports classifiés, notamment que les mesures de protection physique des locaux et de protection logique des systèmes d'information chargés de la sûreté permettent de détecter une intrusion suffisamment tôt et de la freiner le temps nécessaire à une intervention (cf. Appendice 26). Cette

évaluation figure dans l'avis technique d'aptitude physique. En raison de la diversité des dispositifs de protection disponibles sur le marché et de l'évolution constante des techniques utilisées, le responsable d'organisme peut, en cas de besoin, consulter la Direction de la Sûreté Publique et l'Agence Monégasque de Sécurité Numérique, sur les normes que doivent respecter les matériels et les systèmes de protection qu'ils désirent mettre en place.

Lorsque les moyens techniques et, le cas échéant, logiques ne permettent pas de contrer une atteinte à la protection des informations et supports classifiés, la Direction de la Sûreté Publique émet un avis technique d'inaptitude physique. Elle peut également émettre un avis technique avec réserve si la mise aux normes est envisageable sous réserve de la réalisation de travaux de sécurité physique dans un délai défini en liaison avec l'officier de sécurité de l'organisme concerné.

L'avis technique d'aptitude physique précise le niveau de classification des informations et supports classifiés qui peuvent être traités et conservés dans le local.

En cas de changement affectant l'aptitude physique du lieu abritant pour lequel un avis technique d'aptitude physique a été délivré ou à l'occasion d'une inspection, d'un contrôle ou d'un audit réalisé par la Direction de la Sûreté Publique ou par l'autorité administrative, une demande de réévaluation est formulée par l'officier de sécurité dans les plus brefs délais et avant l'échéance de l'avis, auprès de la Direction de la Sûreté Publique.

Les éléments de vulnérabilité décelés à l'occasion d'une évaluation technique sollicitée par l'officier de sécurité, lors d'une demande de renouvellement ou à l'occasion d'une inspection, d'un contrôle ou d'un audit peuvent entraîner une réévaluation des avis techniques précédemment émis par la Direction de la Sûreté Publique.

4. Sécurisation des salles, bureaux, et équipements

4.1. Principe d'identification

Les informations et supports classifiés sont traités dans des locaux qui sont à l'abri des captations, réémissions ou enregistrements non autorisés de sons, d'images et d'informations.

Le niveau de classification des informations et supports qui peuvent être traités dans le local est indiqué à l'intérieur de celui-ci. Le contrôle du local est effectué de manière régulière sous la responsabilité de l'officier de sécurité.

4.2. Politique du bureau propre et de l'écran vide

En dehors des heures de travail ou lorsqu'une personne pénètre dans son espace de travail, tout détenteur d'information ou support classifié s'assure qu'aucune information ou support classifié n'est susceptible d'être accessible par une personne non qualifiée au sens du présent arrêté.

4.3. Organisation des réunions

La tenue d'une réunion de travail, d'une conférence, d'un exercice ou la présentation de matériels impliquant l'accès de ses participants à des informations et supports classifiés exige la mise en œuvre de mesures de sécurité. L'autorité organisatrice veille à la protection des informations et supports classifiés échangés au cours ou dans la suite d'une réunion de travail, d'une conférence, d'un exercice ou d'une présentation de matériels et s'assure notamment que :

- le local où se tient la réunion présente les garanties de sécurité prévues par la présente annexe ;

- les participants à la réunion sont habilités au niveau requis par la réunion et ont le besoin d'en connaître ;

- les informations et supports classifiés communiqués aux participants lors de la réunion sont traités et gérés conformément à la réglementation applicable.

Les mesures de sécurité devant être mises en œuvre, avant, pendant et après la réunion, sont détaillées en Appendice 31.

5. Protection contre les menaces extérieures et environnementales

Selon le besoin en disponibilité des systèmes d'information classifiés et le résultat de l'analyse de risques, le responsable d'organisme détermine les mesures de protection physique contre les menaces extérieures et environnementales adéquates. Lorsque le site abrite des systèmes d'information classifiés, ces mesures figurent dans le dossier d'homologation (cf. paragraphe1.4 Titre VI).

Ces mesures concernent notamment les dispositifs contre les incendies, les dégâts des eaux, les risques liés à l'alimentation électrique et tout autre risque environnemental identifié.

TITRE VI - SÉCURITÉ DES SYSTÈMES D'INFORMATION CLASSIFIÉS

Comme pour les lieux abritant des éléments couverts par le secret de sécurité nationale, les mesures de sécurité applicables aux systèmes d'information classifiés visent à prévenir toute menace, interne ou externe, qui pourrait mettre en cause la disponibilité, l'intégrité, la confidentialité et la traçabilité des informations et supports classifiés qu'ils contiennent, ainsi qu'à empêcher qu'une personne non autorisée puisse y accéder.

La sécurité d'un système d'information classifié repose avant tout sur une analyse de risques, à partir de laquelle un ensemble de mesures organisationnelles, physiques, logiques et environnementales sont mises en place. Une logique de défense en profondeur articulée autour de cinq axes en découle :

- prévenir : éviter la présence ou l'apparition de failles de sécurité ;
- bloquer : empêcher les attaques ;
- contenir : limiter les conséquences d'une attaque ;
- détecter : pouvoir identifier, en vue d'y réagir, les incidents et les attaques survenant sur le système d'information ;
- réparer : disposer de moyens pour remettre le système en fonctionnement et en conditions de sécurité à la suite d'un incident ou d'une attaque.

La sécurité d'un système d'information classifié repose sur deux grands types de barrières de sécurité : les mesures de sécurité physiques et environnementales et les mesures de sécurité logiques inhérentes au système lui-même.

L'ensemble de ces mesures sont prises en compte dans la démarche d'homologation préalable à la mise en service de tout système d'information classifié.

1. Homologation du système d'information classifié

1.1. Démarche d'homologation

Conformément à l'arrêté ministériel n° 2017-56 du 1er février 2017, tout système d'information classifié doit faire l'objet d'une décision d'homologation préalablement à son emploi.

La démarche d'homologation vise à s'assurer que l'ensemble des risques pesant sur le système a été identifié et a fait l'objet d'un traitement approprié afin de réduire la vraisemblance d'une attaque informatique, et en particulier, au titre de la protection du secret, d'une compromission des informations classifiées qu'il aura à traiter.

Cette démarche repose sur une analyse de risques globale et prend ainsi en compte tous les éléments, y compris environnementaux, indispensables au fonctionnement et à la sécurité du système. Le dossier d'homologation inclut ainsi les éléments fonctionnels, organisationnels et techniques mis en œuvre pour garantir la disponibilité, l'intégrité, la confidentialité et la traçabilité des informations classifiées que le système d'information classifié est appelé à traiter, ainsi que le périmètre géographique et physique dans lequel le système est déployé.

La décision d'homologation, aboutissement de cette démarche, est une décision prise par l'autorité d'homologation. Elle atteste que les risques pesant sur la sécurité de ce système et sur les informations classifiées qu'il aura à traiter ont été identifiés et que les mesures nécessaires pour le protéger sont mises en œuvre. Le traitement d'informations dont le niveau de classification est supérieur au niveau de classification prévu par la décision d'homologation du système d'information est interdit.

Le périmètre d'homologation d'un système d'information classifié inclut les éventuels supports amovibles mis à disposition par l'autorité d'emploi pour ce système d'information, que ceux-ci soient destinés à être utilisés exclusivement au sein du système d'information classifié (cf. Titre VI, paragraphe 8.1) ou qu'ils soient destinés à réaliser des échanges avec d'autres systèmes d'information (cf. Titre VI,

paragraphe 8.2). Par la décision d'homologation, l'autorité d'homologation accepte les risques résiduels de sécurité, en pleine connaissance de cause.

En particulier, une grande attention est prêtée à :

- l'interconnexion avec d'autres systèmes ;
- l'usage de supports amovibles ;
- l'accès à distance par des utilisateurs en mobilité ;
- les moyens de visualisation et d'hébergement des informations classifiées ;
- les opérations de maintenance ou d'exploitation du système ou d'administration, en particulier lorsqu'elles sont effectuées par des prestataires externes.

1.2. Autorité d'homologation

L'autorité d'homologation est le Ministre d'État pour les systèmes d'information traitant d'informations classifiées.

1.3. Commission d'homologation

L'autorité d'homologation met en place une commission d'homologation chargée de l'assister et de préparer la décision d'homologation. Cette commission comprend :

- *L'Autorité d'homologation ou son représentant ;*
- *Le Conseiller de Gouvernement-Ministre de l'Intérieur ou son représentant, autorité cliente et président de la commission d'homologation;*
- *Le Directeur de l'Agence Monégasque de Sécurité Numérique ou son représentant ;*
- *Le Responsable Sécurité des Systèmes d'Information de l'autorité cliente ;*
- *L'Autorité d'exploitation ;*
- *Le Responsable fonctionnel ;*
- *Le Responsable technique du système ;*
- *L'Officier de sécurité de l'autorité d'exploitation, responsable de la sécurité du projet.*

Des représentants de la Direction de la Sûreté Publique peuvent être conviés à la commission et sont obligatoirement présents lorsque l'homologation est au profit d'une personne morale de droit privé.

Dans le cadre de l'utilisation d'un système d'information classifié en exécution d'un contrat au sens du Titre IV, l'autorité contractante participe également à la commission.

1.4. Dossier d'homologation

Le dossier d'homologation est établi selon les recommandations de l'Agence Monégasque de Sécurité Numérique. Le dossier d'homologation, initié dès la conception du système, est par la suite tenu à jour tout au long du cycle de vie du système d'information classifié.

La stratégie d'homologation précise, à partir de l'analyse de risques pesant sur le système d'information classifié et conformément à la politique de sécurité des systèmes d'information applicable, la constitution du dossier d'homologation.

La nécessité de verser au dossier d'homologation les documents listés ci-après est ainsi évaluée et justifiée au regard de l'analyse de risques et de la stratégie d'homologation. Si un document n'est pas versé au dossier d'homologation, la justification associée y figure.

Doivent être versés au dossier d'homologation les documents suivants :

- la politique de sécurité du système d'information applicable ;
- les procédures d'exploitation sécurisée du système, y compris la documentation à destination des utilisateurs et des administrateurs ;

- les modalités de gestion des risques résiduels ;
- le plan d'amélioration continue de la sécurité ;
- les résultats des tests et des audits menés pour vérifier l'état de sécurité du système ;
- la documentation relative à la gestion des éléments cryptographiques mis en œuvre dans le système d'information ;
- la cartographie complète du système d'information qui comprend notamment la liste des équipements externes pouvant être connectés au système d'information (matériel de maintenance, d'audit, etc.) ;
- les schémas détaillés de l'architecture du système d'information ;
- les agréments des dispositifs de sécurité ;
- l'analyse de risques et les mesures de mitigation envisagées, lorsque, par dérogation, il est envisagé de recourir à des dispositifs de sécurité non agréés (cf. Titre VI § 5.1).

Une fois le système d'information classifié déployé, les documents relatifs aux lieux d'installation, et notamment les mesures de protection physique et les avis techniques d'aptitude physique, sont versés au dossier d'homologation.

Le dossier d'homologation est tenu à disposition de l'Agence Monégasque de Sécurité Numérique.

1.5. Durée de la décision d'homologation

La décision d'homologation est prononcée pour une durée maximale de trois ans pour un système d'information au niveau Secret de Sécurité Nationale.

L'Agence Monégasque de Sécurité Numérique est destinataire de toute décision d'homologation portant sur les systèmes d'information classifiés et peut demander le dossier d'homologation correspondant. La Direction de la Sûreté Publique est également destinataire de la décision d'homologation.

1.6. Contrôle et renouvellement de l'homologation

L'autorité d'homologation fixe les conditions du maintien de l'homologation de sécurité tout au long du cycle de vie du système d'information. La commission d'homologation se réunit a minima une fois par an jusqu'à la fin de vie du système d'information classifié pour assurer un contrôle régulier du bon fonctionnement du système d'information selon les conditions qu'elle a approuvées.

L'autorité d'homologation procède au renouvellement de l'homologation avant le terme prévu. Elle s'assure de la complétude du dossier d'homologation et vérifie que les pièces nécessaires à son actualisation y figurent.

Une nouvelle décision d'homologation est nécessaire lorsque :

- les conditions d'emploi et d'exploitation du système ont été significativement modifiées ;
- de nouvelles fonctionnalités ou applications ont été installées ;
- le système a été interconnecté à de nouveaux systèmes ;
- des problèmes d'application des mesures de sécurité ou des conditions de maintien de l'homologation ont été révélés, par exemple lors d'un audit de sécurité ;
- les menaces sur le système ont significativement évolué ;
- de nouvelles vulnérabilités non corrigées ont été identifiées ;
- le système a fait l'objet d'un incident de sécurité significatif au regard de l'analyse de risques.

Si le système d'information classifié n'a pas connu de changements significatifs, une procédure simplifiée d'homologation est mise en œuvre.

1.7. Procédure dérogatoire en cas d'urgence opérationnelle

La décision d'homologation intervient avant la mise en service opérationnelle du système. Cependant, de façon exceptionnelle, lorsque l'urgence opérationnelle le requiert, il peut être procédé à une mise en service provisoire, sans attendre l'homologation du système, en tenant compte de l'avancement de

la procédure d'homologation et des risques résiduels de sécurité. Dans ce cas, l'autorité d'homologation délivre une autorisation provisoire d'emploi (APE) pour une durée courte et associée à un plan de mise en conformité.

2. Homologation des interconnexions d'un système d'information classifié

2.1. Interconnexion entre deux systèmes d'information classifiés de même niveau

Toute interconnexion entre systèmes d'information classifiés de même niveau doit être justifiée et faire l'objet d'une homologation spécifique à ce même niveau. L'ajout d'une interconnexion constitue, en effet, un changement structurel nécessitant une nouvelle homologation des systèmes d'information interconnectés.

L'autorité d'homologation est le Ministre d'État, ou toute autorité à qui il en délègue la responsabilité, dans les cas suivants :

- pour les transferts d'informations entre des systèmes d'information classifiés de même niveau, dont l'un n'est pas sous maîtrise nationale ;
- lorsque l'utilisation de dispositifs de sécurité agréés est obligatoire mais impossible, notamment lorsqu'il n'en existe pas ou lorsqu'ils ne sont pas agréés au bon niveau.

L'interconnexion est obligatoirement réalisée à l'aide de dispositifs de sécurité agréés lorsqu'ils sont utilisés comme moyens essentiels de protection contre les accès non autorisés aux informations classifiées ou au système, pour les transferts d'informations entre des systèmes d'information classifiés de même niveau ou de niveaux équivalents, dont l'un n'est pas sous maîtrise nationale.

Ces dispositifs de sécurité agréés sont déployés dans les conditions d'emploi associées aux décisions d'agrément pour cet usage.

2.2. Autres interconnexions

Les interconnexions entre systèmes d'information de niveaux de classification différents ou entre un système d'information classifié et un système d'information non-classifié sont par principe interdites.

Toute interconnexion de ce type dérogeant à l'interdiction de principe doit être justifiée par un besoin opérationnel strictement nécessaire. La justification est versée au dossier d'homologation.

Toute interconnexion d'un système d'information classifié avec un système d'information non classifié ou de niveau de classification différent est homologuée au niveau du système d'information le plus élevé. Cette interconnexion fait l'objet d'une homologation spécifique. L'ajout d'une interconnexion constitue un changement structurel nécessitant une nouvelle homologation des systèmes d'information interconnectés.

L'autorité d'homologation est par défaut l'autorité d'homologation du système d'information du niveau le plus élevé, mais elle peut être aussi désignée après concertation entre les autorités d'homologation de chaque système d'information interconnecté.

L'interconnexion est obligatoirement réalisée à l'aide de dispositifs de sécurité agréés lorsqu'ils sont utilisés comme moyens essentiels de protection contre les accès non-autorisés aux informations classifiées ou au système.

Ces dispositifs de sécurité agréés sont déployés dans les conditions d'emploi associées aux décisions d'agrément pour cet usage.

3. Mesures de sécurité applicables en cas de sous-traitance du développement ou de la maintenance d'un système d'information classifié

Le développement ou le maintien en conditions opérationnelles et de sécurité d'un système d'information classifié respecte les règles définies dans le présent arrêté. Aucun sous-traitant ne peut accéder à un système d'information classifié s'il ne fait pas l'objet d'une décision d'habilitation.

Toute information spécifique liée au développement ou à la configuration d'un logiciel ou d'un système d'information classifié et dont la divulgation est susceptible de porter atteinte à la sécurité du système d'information classifié ou des informations classifiées qu'il contient est classifiée à un niveau équivalent ou supérieur à celui du système d'information classifié lui-même.

Lorsqu'ils sont considérés comme des documents administratifs, compte tenu du risque d'atteinte au secret de sécurité nationale et à la sécurité des systèmes d'information susceptible de résulter de leur divulgation, les codes source et les éléments de configuration d'un système d'information classifié ne sont pas librement communicables et peuvent être classifiés en fonction de leur sensibilité.

Les besoins de protection du code source et des éléments de configuration d'un système d'information classifié sont définis dans le plan contractuel de sécurité du contrat correspondant.

4. Mesures de sécurités physiques

4.1. Lieu abritant le système d'information classifié

Comme tout lieu abritant des informations et supports classifiés, les lieux abritant des systèmes d'information classifiés doivent satisfaire aux règles énoncées au Titre V.

4.2. Matériel classifié laissé sans surveillance par son détenteur

La démarche d'homologation tient compte des risques liés à la protection physique des matériels classifiés, y compris lorsque des matériels classifiés peuvent être laissés sans surveillance par leur détenteur. À cette fin, différentes mesures de défense en profondeur sont combinées conformément aux dispositions de l'Appendice 26. Des mesures spécifiques sont également prises pour protéger l'accès aux éléments physiques des systèmes d'information classifiés hors équipements de mobilité. Le cas échéant, l'homologation du système d'information classifié prévoit des mesures de protection adaptées.

5. Mesures de sécurité inhérentes au système d'information classifié

Tout équipement constitutif d'un système d'information classifié est équipé de moyens de protection et doté d'une configuration durcie.

5.1. Dispositifs de sécurité

Les dispositifs de sécurité sont des moyens matériels ou logiciels destinés à protéger les informations traitées par le système ou à protéger le système lui-même. Ces dispositifs proposés par le responsable de la sécurité des systèmes d'information peuvent être développés pour un usage général ou pour un système particulier. Ils mettent en œuvre différents types de fonctions et de mécanismes de sécurité, comme :

- des fonctions cryptographiques permettant la protection en confidentialité ou en intégrité, l'authentification ou la signature des informations stockées sur des supports ou transmises sur des réseaux ;
- des fonctions ou des mécanismes destinés à protéger le dispositif lui-même, comme le contrôle, l'enregistrement et l'imputabilité des accès au dispositif, à empêcher ou à détecter les intrusions physiques ou logiques non autorisées, à garantir la protection, ou l'effacement le cas échéant, des données sensibles stockées, et plus généralement toute fonction ou tout mécanisme destiné à garantir l'intégrité et la disponibilité du dispositif ;
- des fonctions d'administration et de gestion sécurisée du dispositif ;
- des fonctions ou des mécanismes limitant les émissions de signaux compromettants.

5.2. Recours à des dispositifs de sécurité agréés

Un dispositif de sécurité mis en place dans un système d'information qui traite d'informations classifiées est agréé par l'agence nationale de la sécurité des systèmes d'information lorsqu'il est utilisé, en complément de mesures organisationnelles de sécurité, comme un moyen essentiel de protection contre les accès non autorisés aux informations classifiées ou au système.

À titre exceptionnel, et sur le fondement d'une analyse de risques réalisée par le responsable de la sécurité du système d'information dans le cadre de l'homologation, l'autorité d'homologation peut autoriser le recours à des matériels et logiciels agréés à un niveau inférieur, voire non agréés lorsqu'il n'existe pas de dispositif de sécurité agréé au bon niveau. La justification de cette autorisation est motivée dans le dossier d'homologation du système.

6. Conception et exploitation du système d'information

6.1. Administration des systèmes d'information classifiés

Les actions d'administration permettent de maintenir le système d'information classifié en condition de sécurité et en condition opérationnelle. Qu'il s'agisse d'actions liées à des évolutions du système d'information ou à l'exploitation courante, celles-ci nécessitent des privilèges. Elles constituent à ce titre une activité critique.

De manière générale, les principes suivants doivent être appliqués :

- les actions d'administration sont menées par du personnel spécialement formé et sensibilisé ;
- le système d'information d'administration est classifié au même niveau que le système d'information administré ;
- l'administration d'un système d'information classifié au niveau Secret de Sécurité Nationale est faite dans une zone protégée et au niveau Très Secret de Sécurité Nationale dans une zone réservée.

Les pratiques d'administration, en particulier pour la gestion des comptes privilégiés et la protection de leurs mécanismes d'authentification, sont établies suivant les recommandations de l'Agence Monégasque de Sécurité Numérique. Toute non-conformité est justifiée et intégrée dans les risques résiduels présentés lors de la commission d'homologation. Au niveau *Très Secret de Sécurité Nationale*, les non-conformités sont également déclarées à l'Agence Monégasque de Sécurité Numérique, au plus tard lors de la commission d'homologation.

L'autorité d'emploi d'un système d'information classifié applique les règles suivantes au système d'information d'administration et aux flux correspondants :

- les ressources matérielles, les ressources logicielles et les informations d'authentification sont strictement séparées selon leur usage. Ainsi, toute action d'administration est réalisée exclusivement par un administrateur depuis un compte administrateur individuel et dédié à cet usage. En outre, les actions d'administration sont conduites depuis des ressources d'administration dédiées (postes de travail, serveurs, ou autres équipements spécifiques). Les ressources d'administration, matérielles et logicielles, en particulier les postes d'administration, sont utilisées exclusivement pour les actions d'administration. Ces ressources sont gérées et configurées par l'autorité responsable de l'administration du système d'information classifié ou par le prestataire qu'elle a mandaté pour réaliser les actions d'administration ;
- les flux d'administration sont cloisonnés à l'égard des flux métier au niveau des ressources administrées. Les ressources d'administration accèdent aux ressources administrées au moyen d'une interface réseau dédiée à l'administration. Cette interface est physique ou, à défaut, logique. L'interface réseau utilisée pour les actions d'administration n'est accessible qu'aux seules ressources d'administration. En l'absence de mesure d'isolation physique de cette interface, un filtrage logique assure cette

restriction d'accès. Quand des raisons techniques ou opérationnelles ne permettent pas l'administration des ressources administrées par des interfaces réseau dédiées, les actions d'administration sont faites par l'unique interface réseau de la ressource administrée. Ce cas de figure est justifié dans le dossier d'homologation ;

- les flux réseau entre les ressources administrées et les ressources d'administration sont filtrés. Afin de réduire le risque de compromission des ressources d'administration depuis les ressources administrées, les ressources d'administration sont déployées sur un réseau dédié à cet usage. Ce réseau portant les ressources d'administration est un réseau physiquement cloisonné de préférence ou, à défaut, un réseau logiquement cloisonné à l'aide de mécanismes de chiffrement et d'authentification réseau. Un filtrage strict des flux réseau entre les ressources administrées et les ressources d'administration est mis en place. Pour minimiser les possibilités de rebonds entre ressources administrées en cas de compromission de l'une d'entre-elles, un mécanisme de filtrage restreint les possibilités de communication sur ce réseau d'administration.

6.2. Maîtrise des logiciels en exploitation

L'autorité d'emploi du système d'information installe, sur un système d'information classifié, les seuls services et fonctionnalités qui sont indispensables au fonctionnement ou à la sécurité du système d'information. Le responsable de la sécurité des systèmes d'information s'assure que les services et les fonctionnalités qui ne sont pas indispensables, notamment ceux installés par défaut, sont désactivés et les fait désinstaller si cela est possible. Lorsque la désinstallation n'est pas possible, cela est mentionné dans le dossier d'homologation du système d'information classifié en précisant les services et fonctionnalités concernés, ainsi que les mesures de réduction du risque mises en œuvre.

L'autorité d'emploi du système prévoit des dispositifs pour empêcher l'installation de services et fonctionnalités hors de ces procédures. En cas d'impossibilité, il y est fait mention dans le dossier d'homologation.

6.3. Contrôle d'accès aux systèmes d'information classifiés

6.3.1. Gestion des droits d'accès sur la base du principe du moindre privilège, corolaire du respect du besoin d'en connaître

Par principe, toute personne habilitée accédant à des informations ou support classifiés depuis un système d'information classifié utilise, à cette fin, un compte utilisateur individuel assorti des droits d'accès correspondant à son profil et à son besoin d'en connaître. Ce compte ne dispose pas de droits d'administration sur le système d'information classifié. Ainsi, l'administrateur d'un système d'information classifié et l'administrateur de sécurité disposent de comptes individuels dédiés pour chacune de ces fonctions, distincts de leur compte utilisateur.

Par défaut, un administrateur est habilité au niveau d'habilitation correspondant au moins au niveau de classification du système d'information classifié administré. Lorsque les droits qui lui sont octroyés sur le système d'information classifié sont étendus, lui permettant notamment d'outrepasser ses droits ou de masquer ses actions sur le système d'information classifié, l'administrateur doit être habilité au niveau *Très Secret de Sécurité Nationale*, sans incidence sur le niveau d'habilitation de la personne morale.

À titre dérogatoire, lorsque des raisons techniques ou opérationnelles ne permettent pas de créer de compte individuel, ni de restreindre les droits d'administration aux seules personnes autorisées, cela est justifié dans le dossier d'homologation et le Ministre d'État en est informé. Le responsable de la sécurité du système d'information met alors en place les mesures nécessaires pour réduire le risque lié à l'utilisation de comptes partagés ou de service et assurer la traçabilité et l'imputabilité de l'utilisation de ces comptes. Ces mesures et les raisons justifiant le recours à des comptes partagés ou de service sont décrites dans le dossier d'homologation du système d'information classifié concerné.

Seule l'Agence Monégasque de Sécurité Numérique peut autoriser cette dérogation pour les systèmes d'information classifiés au niveau *Très Secret de Sécurité Nationale*. L'autorité d'homologation sollicite son autorisation dès la phase de conception du système d'information classifié.

Les utilisateurs d'un système d'information classifié ont uniquement accès aux données, systèmes et services auxquels ils sont autorisés à accéder au regard de leur niveau d'habilitation et de leur besoin d'en connaître. Les éléments constitutifs du système d'information s'authentifient, dans la mesure du possible, auprès des réseaux et des services. Le principe de moindre privilège est pris en compte dans la mesure du possible.

La procédure relative au retrait des droits d'accès est validée par l'autorité d'emploi du système. Elle est précisée dans la politique de sécurité du système d'information de l'État (PSSI-E).

a) Maîtrise de la gestion des accès des utilisateurs

L'autorité d'emploi du système d'information classifié met en place une politique de gestion des éléments d'authentification liés aux comptes utilisateurs et administrateurs suivant les recommandations de l'Agence Monégasque de Sécurité Numérique et s'assure de son respect.

Dans le cas d'un système d'information classifié, le mécanisme de contrôle d'accès permet également de tracer chaque accès (consultation, copie, modification, impression, etc.) à chaque information classifiée.

Le mécanisme de contrôle d'accès repose sur des mécanismes d'authentification forte établis selon le Référentiel Général de Sécurité de la Principauté.

Si la mise en œuvre de tels mécanismes n'est pas possible pour des raisons techniques ou opérationnelles et après en avoir rendu compte au Ministre d'État, des mesures organisationnelles, décrites dans le dossier d'homologation, sont prises pour pallier cette lacune.

b) Revue des droits d'accès des comptes

Pour chaque système d'information classifié et système d'administration des systèmes d'information classifiés, une revue des droits d'accès des comptes est mise en place. La périodicité et les modalités de cette revue sont fixées par l'autorité d'homologation en cohérence avec les besoins opérationnels et ne doit pas excéder un an. Les conditions précises de cette revue sont décrites dans le dossier d'homologation, ainsi que dans les exigences de la PSSI-E.

c) Mesures de sécurité logiques relatives aux mentions complémentaires de protection

Les systèmes d'information susceptibles de traiter des informations portant une mention complémentaire de protection, font l'objet de mesures de sécurité particulières techniques ou organisationnelles pour garantir l'accès aux seules personnes ayant le besoin d'en connaître. Le processus d'homologation tient compte du fait que le système d'information est susceptible de traiter de telles informations.

Dans le cas d'un système devant traiter à la fois des informations portant la mention complémentaire de protection et d'autres ne la portant pas, et accessible à des personnes non autorisées à accéder à des informations portant la mention complémentaire de protection, le système d'information considéré et les mesures organisationnelles afférentes garantissent notamment que :

- pour chaque mention de protection, les informations classifiées en étant marquées sont stockées dans des zones du système d'information clairement identifiées et indiquées dans le dossier d'homologation ;
- les zones du système d'information ainsi identifiées sont cloisonnées du reste du système d'information avec des mesures conformes aux recommandations de l'Agence Monégasque de Sécurité Numérique ;
- le contrôle d'accès du système d'information permet d'assurer la protection du besoin d'en connaître pour les informations classifiées marquées de la mention de protection

considérée. Si nécessaire, un contrôle d'accès dédié est mis en place ;
- lorsque des données portant une mention de protection circulent hors des zones identifiées, elles sont chiffrées avec des moyens conformes aux recommandations de l'Agence Monégasque de Sécurité Numérique ;
- l'accès aux informations portant une mention de protection complémentaire ou aux zones les contenant est tracé et indique explicitement les éventuelles mentions de protection.

6.3.2. Responsabilité des utilisateurs

Chaque utilisateur est responsable de la protection de ses informations d'authentification et du bon usage des outils associés (de type ACSSI, cartes à puce, etc.). L'autorité d'emploi du système d'information met à sa disposition des moyens de conservation sécurisés et adaptés de ces informations.

6.3.3. Articles contrôlés de la sécurité des systèmes d'information classifiés

Certains moyens, tels que les dispositifs de sécurité ou leurs composants, et certaines informations relatives à ces moyens (spécifications algorithmiques, documents de conception, clefs de chiffrement, rapports d'évaluation, etc.) nécessitent la mise en œuvre d'une gestion spécifique visant à assurer leur traçabilité et leur intégrité tout au long de leur cycle de vie. Le traitement de ces moyens et informations, appelés « articles contrôlés de la sécurité des systèmes d'information », est défini par arrêté ministériel.

6.4. Supervision logicielle de la sécurité et traçabilité

6.4.1. Synchronisation des horloges

Pour les besoins en traçabilité, les composantes d'un système d'information classifié sont synchronisées sur une source de temps unique. Lorsque des raisons techniques ou opérationnelles ne le permettent pas, cette impossibilité est mentionnée dans le dossier d'homologation et des mesures palliatives sont mises en place par le responsable de la sécurité des systèmes d'information.

6.4.2. Journalisation des événements

À des fins d'investigation, de suivi *a posteriori* des échanges, de traitement des incidents et d'archivage, une journalisation des événements est mise en place pour tracer et imputer les actions réalisées sur les systèmes d'information classifiés selon les recommandations l'Agence Monégasque de Sécurité Numérique.

Les événements enregistrés par le système de journalisation sont horodatés au moyen de sources de temps synchronisées entre elles. Ils sont, pour chaque système d'information classifié, centralisés et archivés pour une durée d'au moins trois ans pour le niveau *Secret de Sécurité Nationale* et d'au moins cinq ans pour le niveau *Très Secret de Sécurité Nationale*. Le format d'archivage des événements permet de réaliser des recherches automatisées sur ces événements. Si la mise en œuvre de tels mécanismes est impossible pour des raisons techniques ou organisationnelles et, après en avoir rendu compte au Ministre d'État, des mesures palliatives sont prises et décrites dans le dossier d'homologation.

6.4.3. Protection de l'information journalisée

Les journaux des événements ne doivent pas être conçus pour contenir d'informations permettant de retrouver les informations d'authentification (de type mots de passe, codes PIN, clés privées, etc.).

Les journaux d'événements sont sauvegardés et protégés de manière à assurer leur intégrité et leur disponibilité.

6.4.4. Accès aux journaux

Pour chaque système d'information classifié, une procédure portant sur la manipulation des journaux est élaborée par le responsable de la sécurité des systèmes d'information. Elle précise les personnes autorisées à y accéder, leurs modes de traitement ainsi que les moyens techniques et opérationnels mis en œuvre pour assurer le respect du besoin d'en connaître et la traçabilité des accès.

Les données de traçabilité des accès sont archivées sur une durée d'au moins trois ans pour le niveau *Secret de Sécurité Nationale* et cinq ans pour le niveau *Très Secret de Sécurité Nationale*.

6.4.5. Systèmes de détection

Une procédure de détection des incidents de sécurité affectant le système d'information classifié est établie.

Cette procédure prévoit des mesures organisationnelles et techniques destinées à détecter les incidents de sécurité affectant le système d'information classifié. Les mesures organisationnelles comprennent les modalités d'exploitation des dispositifs de détection et décrivent la chaîne de traitement des événements de sécurité identifiés par ces dispositifs. Les mesures techniques précisent la nature et le positionnement des dispositifs de détection.

Des dispositifs de détection capables d'identifier des événements caractéristiques d'un incident de sécurité notamment d'une attaque en cours ou à venir et de permettre la recherche de traces d'incidents antérieurs sont mis en œuvre. À cet effet, ces dispositifs :

- collectent les données représentatives de l'activité du système d'information, issues du réseau, des systèmes et/ou des applications, à partir de capteurs positionnés de manière à optimiser la couverture du dispositif de supervision global ;
- analysent les données issues des capteurs notamment en recherchant des marqueurs techniques d'attaques connus ou des anomalies, dans le but d'identifier les événements de sécurité et de les caractériser ;
- archivent les métadonnées des événements identifiés afin de permettre une recherche *a posteriori* de marqueurs techniques d'attaques ou de compromission sur une durée d'au moins trois ans pour le niveau *Secret de Sécurité Nationale* et d'au moins cinq ans pour le niveau *Très Secret de Sécurité Nationale*.

Les stratégies de collecte et d'analyse sont élaborées par l'Agence Monégasque de Sécurité Numérique.

Le recours à plusieurs sources de données pour détecter des activités malveillantes est encouragé. Un système de corrélation et d'analyse des journaux des événements doit être mis en œuvre et exploité.

L'architecture de déploiement des systèmes de détection ne doit pas remettre en cause la sécurité du système d'information classifié. Dans le cadre de systèmes de détection réseau, des dispositifs de type « TAP » qualifiés, qui concourent à l'atteinte de cet objectif de sécurité, sont utilisés.

Ces systèmes de détection sont exploités en s'appuyant sur les exigences du référentiel en matière de détection des incidents de sécurité.

Les systèmes de détection sont pris en compte dans le périmètre de l'homologation et les risques propres à ces systèmes font l'objet d'une attention particulière. Si les systèmes de détection sont communs à plusieurs systèmes d'information classifiés, ils font l'objet d'une homologation spécifique.

Si la mise en œuvre de tels systèmes de détection est impossible pour des raisons techniques ou organisationnelles et, après en avoir rendu compte au Ministre d'État, des mesures palliatives sont prises et décrites dans le dossier d'homologation.

6.5. Maintenance et maintien en condition opérationnelle et en condition de sécurité

Les opérations de maintenance, qui incluent les opérations de maintien en condition opérationnelle et en condition de sécurité sur un système d'information classifié sont tracées et imputées à leur auteur. Elles sont réalisées par des personnes habilitées.

Le matériel connecté au système d'information classifié pour sa maintenance et son maintien en condition opérationnelle ou de sécurité lui est dédié et est classifié au même niveau que le système d'information. Les équipements sont utilisés conformément aux parties paragraphes 5 et 7.

L'autorité d'emploi du système d'information élabore, tient à jour et met en œuvre une procédure de maintien en condition de sécurité des ressources matérielles et logicielles de ses systèmes d'information classifiés.

Cette procédure prévoit :

- l'installation et la maintenance de toutes les ressources matérielles et logicielles des systèmes d'information classifiés dans des versions supportées par leurs fournisseurs ou leurs fabricants et mises à jour du point de vue de la sécurité, sauf en cas de difficultés techniques ou opérationnelles justifiées ;
- préalablement à l'installation de toute nouvelle version, la vérification de l'origine de cette version et de son intégrité, et l'analyse de l'impact, d'un point de vue technique et opérationnel, de cette version sur le système d'information classifié concerné ;
- une veille sur les vulnérabilités affectant le système d'information classifié afin de pouvoir mettre en œuvre, dès qu'une vulnérabilité est connue, des mesures palliatives en attente de la publication d'une mesure correctrice de sécurité ;
- l'installation sans délai sous le contrôle du responsable de la sécurité du système d'information, de toute mesure correctrice de sécurité concernant l'une de ses ressources, après s'être assuré de l'origine de cette mesure et de son intégrité.

Lorsque des raisons techniques ou opérationnelles le justifient, conformément aux instructions de l'autorité d'homologation, l'autorité d'emploi du système d'information peut décider, pour certaines ressources de ses systèmes d'information classifiés et des systèmes d'administration de systèmes d'information classifiés, de ne pas installer une version supportée par le fournisseur ou le fabricant de la ressource concernée ou de ne pas installer une mesure correctrice de sécurité. Dans ce cas, le responsable de la sécurité du système d'information met en œuvre des mesures techniques ou organisationnelles pour réduire les risques liés à l'utilisation d'une version obsolète ou comportant des vulnérabilités connues. Il documente ces mesures et les intègre au cycle de maintien en condition de sécurité de son système d'information.

6.6. Cloisonnement

Les systèmes d'information classifiés sont séparés physiquement des systèmes d'information de classification différente et des systèmes d'information non-classifiés. À défaut, des moyens agréés sont utilisés pour cloisonner logiquement ces systèmes d'information.
Lorsque sont concernés deux systèmes d'information classifiés au même niveau dont l'un n'est pas sous maîtrise nationale, les mêmes dispositions s'appliquent.

6.7. Mécanismes de filtrage des flux de données

L'autorité d'emploi du système d'information classifié met en place des mécanismes de filtrage des flux de données circulant dans ou entre les systèmes d'information classifiés afin de bloquer la circulation des flux susceptibles de faciliter des attaques informatiques. Ces mécanismes respectent les règles suivantes :

- le responsable de la sécurité des systèmes d'information établit et tient à jour une liste des règles de filtrage mentionnant l'ensemble des règles en vigueur ou supprimées ;
- la circulation des flux de données est limitée autant que possible aux seuls flux nécessaires au fonctionnement et à la sécurité du système d'information classifié ;
- les flux entrants et sortants ainsi que les flux entre sous-systèmes du système d'information classifié sont filtrés au niveau de leurs interconnexions de manière à ne permettre que la circulation des seuls flux strictement nécessaires au fonctionnement et à la sécurité du système d'information. Les flux qui ne sont pas conformes aux règles de filtrage sont bloqués.

6.8. Gestion de la continuité et de la reprise de l'activité

Tout système d'information classifié fait l'objet d'un plan de continuité ou de reprise informatique (PCI/PRI).

Ce plan se conforme au plan de protection des sites, au plan de continuité ou de reprise d'activité (PCA/PRA) de l'organisme ainsi que, le cas échéant, aux exigences du contrat au profit duquel le système d'information classifié est mis en œuvre.

Il est tenu à jour et régulièrement testé à l'occasion d'exercices.

L'absence de plan de continuité ou de reprise informatique est mentionnée et justifiée dans le dossier d'homologation.

7. Sécurité en mobilité

Par principe, les systèmes d'information classifiés sont conçus et paramétrés pour interdire les accès à distance.

Lorsqu'un tel accès est absolument nécessaire pour des raisons opérationnelles, l'autorité d'homologation, s'appuyant sur le responsable de la sécurité du système d'information, protège l'accès à distance à ces systèmes d'information en ayant recours à des équipements mettant en œuvre des dispositifs de sécurité agréés au niveau de classification du système d'information auquel il donne accès.

8. Supports amovibles

La connexion ou l'installation d'équipements personnels à un système d'information classifié est strictement interdite.

La connexion d'un support amovible non classifié à un système d'information classifié est possible sous réserve de la mise en place de mesures techniques de protection telles que, notamment, la détection, la protection contre l'introduction de codes malveillants ou l'exfiltration d'information.

Avant toute utilisation sur un système d'information traitant d'informations classifiées, l'innocuité de tout support est vérifiée.

Si l'utilisation de supports amovibles est autorisée, ceux-ci sont intégrés au périmètre d'homologation du système d'information classifié (cf. paragraphe 1.1) lorsqu'ils sont gérés, administrés et mis à disposition par l'autorité d'emploi du système d'information classifié.

Tout support amovible susceptible de contenir ou d'avoir contenu de l'information classifiée d'un niveau donné est classifié au moins au même niveau et est soumis à ce titre aux obligations décrites au Titre VII. En aucun cas, un support amovible classifié ne peut être connecté à un système d'information non-classifié ou de classification inférieure.

Lorsque des informations classifiées sont transportées à l'aide de supports amovibles, les supports amovibles respectent les exigences en matière de transport d'informations classifiées sur un support amovible (cf. Titre VII § 3.2.2).

L'officier de sécurité sensibilise les utilisateurs aux mesures de sécurité à respecter dans l'emploi des supports amovibles.

8.1. Supports amovibles au sein du système d'information classifié

Seuls les supports amovibles gérés, administrés et mis à disposition par l'autorité d'emploi du système d'information classifié sont autorisés à se connecter à ce système d'information classifié.

Des dispositifs de sécurité permettant de prévenir la connexion ou l'installation de supports amovibles non autorisés sont mis en place.

8.2. Supports amovibles entre un système d'information classifié et d'autres systèmes

Lorsque des supports amovibles sont utilisés pour importer et exporter des informations à partir d'un système d'information classifié, ce transfert d'information est réalisé exclusivement en connectant ces supports amovibles à des points de connexion appartenant au système d'information classifié.

Ces points de connexion des supports amovibles sont dédiés à cet usage et garantissent notamment les exigences de sécurité suivantes :

- contrôle d'autorisation (approbation de la sortie d'information) ;
- rupture protocolaire : (rupture du flux transitant entre le support amovible et le système d'information émetteur ou destinataire) ;
- traçabilité et imputabilité du transfert.

Les exportations d'informations classifiées réalisées à partir de supports amovibles sont tracées par des moyens techniques ou organisationnels qui permettent notamment d'horodater le transfert et de l'imputer à un utilisateur du système d'information classifié.

L'utilisation de supports amovibles entre un système d'information classifié et un système d'information non classifié ou de classification différente est par principe interdite.

Toute dérogation à l'interdiction de principe doit être justifiée par un besoin opérationnel strictement nécessaire. La justification est versée au dossier d'homologation et les mesures de protection minimales suivantes s'appliquent :

- *une analyse de risques est conduite pour identifier les mesures techniques et organisationnelles visant à prévenir tout risque de sortie incontrôlée d'information classifiée lié aux cas d'usage de ces supports amovibles ;*
- *les échanges d'information entre un système d'information classifié et un système d'information non classifié ou de classification différente s'effectuent au moyen de points de connexion des supports amovibles mettant en œuvre des dispositifs de sécurité utilisés comme moyens essentiels de protection contre les accès non-autorisés aux informations classifiées. Ces dispositifs de sécurité sont agréés (cf. Titre VI § 5.2). En absence de dispositifs agréés et après en avoir rendu compte à l'autorité d'homologation et à l'officier de sécurité concernés, des mesures palliatives sont prises et décrites dans le dossier d'homologation.*

9. Audit des systèmes d'information

En complément des tâches de maintien en condition de sécurité, l'autorité d'homologation réalise ou fait réaliser des audits de sécurité périodiques des systèmes d'information classifiés, a minima, avant chaque homologation ou renouvellement d'homologation.

L'autorité d'emploi du système d'information visé précise les conditions du déroulement de l'audit, notamment de l'utilisation et de la restitution des équipements nécessaires à l'audit.

L'autorité d'homologation et l'autorité d'emploi du système d'information formalisent les conditions de réalisation de l'audit, le cas échéant, par une convention d'audit. Ces audits de sécurité doivent, au-delà de la conformité aux règles du présent arrêté, évaluer le niveau de robustesse des systèmes d'information eu égard aux évolutions de la menace informatique. Il s'agit de vérifier l'application de mesures de défense en profondeur, de les éprouver par des techniques et outils à l'état de l'art et de réaliser des tests complémentaires qui peuvent être conduits inopinément en fonction des relevés d'audit initiaux.

Les risques associés à l'utilisation des outils d'audit, des privilèges et de communication des relevés techniques nécessaires à la réalisation de l'audit de sécurité figurent dans le dossier d'homologation du système visé, quel que soit son niveau de classification et sans préjudice des dispositions du présent arrêté. Les rapports d'audit portant sur des systèmes d'information classifiés sont classifiés au moins au niveau *Secret de Sécurité Nationale.* Les relevés techniques d'audit sont classifiés au maximum au même niveau que le rapport.

L'autorité d'homologation et l'officier de sécurité tiennent les rapports d'audit à disposition de l'Agence Monégasque de Sécurité Numérique.

En cas de recours, pour un audit d'un système d'information classifié, à un prestataire privé, la prestation d'audit doit être qualifiée par l'Agence Monégasque de Sécurité Numérique.

Par principe, les auditeurs doivent être habilités au niveau de classification du système d'information classifié audité ou disposer d'un certificat de sécurité de même nature.

TITRE VII - GESTION DES INFORMATIONS ET SUPPORTS CLASSIFIÉS

La décision de classifier une information ou un support au titre du secret de la sécurité nationale a pour objet de restreindre l'accès à cette information ou à ce support aux seules personnes qualifiées au sens de l'article 18 de la loi n° 1.430 du 13 juillet 2016, suscitée.

La classification est matérialisée par l'apposition d'un timbre de classification défini dans le présent arrêté qui permet de caractériser l'infraction pénale en cas de compromission et détermine les mesures de protection à mettre en œuvre pour l'élaboration et la gestion de l'information et du support classifié tout au long de son cycle de vie.

1. Élaboration des informations et des supports classifiés

1.1. Règles de classification

Classifier une information ou un support au titre du secret de la sécurité nationale a pour conséquence de le placer sous la protection des dispositions spécifiques des articles 18 et 19 de la loi n° 1.430 du 13 juillet 2016, suscitée.

L'apposition d'un timbre de classification visible constitue le seul moyen de conférer cette protection particulière. Il est une marque de l'autorité publique permettant de vérifier l'authenticité et l'intégrité du support.

1.1.1. Principes régissant la décision de classification

a) *Auteur d'informations et supports classifiés*

L'auteur d'une information ou d'un support classifié est celui qui prend la décision d'apposer le timbre de classification sur une information ou un support au niveau requis par son contenu, conformément aux modalités de classification arrêtées par l'autorité émettrice.

Avant de décider d'apposer un timbre de classification sur une information ou un support, l'auteur d'informations ou supports classifiés procède à l'analyse de l'importance de l'information au regard de son contexte et des directives de classification applicables.

Il veille ainsi, sous le contrôle de son autorité hiérarchique et de l'autorité émettrice pour laquelle il procède à la classification, à ce que le niveau de classification soit approprié à l'information ou au support concernés, c'est-à-dire à ce qu'il soit à la fois strictement nécessaire et suffisant.

Chaque échelon de la chaîne de responsabilité doit être en mesure de justifier le timbre de classification apposé sur une information ou un support classifié et prévient les classifications abusives, qui génèrent des coûts de gestion, des charges de travail importantes et altèrent la valeur du secret de la sécurité nationale.

Inversement, chaque échelon de la chaine de responsabilité s'assure qu'aucune information ou support justifiant une classification n'échappe à la classification. Ne pas classifier une information ou un support dont la divulgation ou auquel l'accès est de nature à porter atteinte à la sécurité nationale constitue un manquement grave aux règles de la protection du secret de sécurité nationale, dont chaque échelon de la chaîne de responsabilité est comptable. Cela caractérise une faute, qu'il revient à l'autorité compétente, le cas échéant, de sanctionner.

b) Le choix du niveau de classification

Le niveau de classification est déterminé par la nature et le contexte de l'information ou du support classifié. La source de l'information peut également être prise en considération lorsque sa sensibilité justifie une protection. Les cas manifestes de sur-classification ou de sous-classification sont signalés par le(s) destinataire(s) à l'autorité émettrice ou à l'auteur de l'information ou du support classifié qui procède, le cas échéant, à la modification appropriée, en informe l'ensemble des destinataires et prend les mesures nécessaires pour éviter une compromission lorsque l'information change de niveau.

1.1.2. Principes de classification

a) Principe de classification d'un document

Tout ensemble (pages, paraphes, annexes, appendices, pièces jointes) d'un document contenant des informations classifiées à des niveaux différents est classifié lui-même au niveau le plus élevé des informations qu'il contient.

Lorsqu'un document comprend diverses parties, les unes nécessitant une classification, les autres non, il convient de s'efforcer de préciser le niveau de classification en marge face aux parties ou paragraphes qu'il couvre (cf. Appendice 32). La diffusion des paragraphes non classifiés ou des paragraphes d'un niveau de classification inférieur est rendue possible par extraction des éléments non classifiés ou en rendant illisibles, de manière irréversible, les paragraphes classifiés ou classifiés au niveau supérieur.

Par principe, l'objet d'un document est classifié au même niveau que le document lui-même, sauf si son auteur en décide autrement et le précise.

b) Principe de classification d'un matériel et des informations qui lui sont relatives

Le niveau de classification des informations (notices, plans, etc.) concernant un matériel peut être différent du niveau de classification de ce dernier.

c) Principe de classification d'un agrégat

Un ensemble d'informations ou supports, dit « agrégat », peut être classifié si le regroupement des informations ou supports qui le composent le justifie, alors même qu'aucun de ses éléments, pris isolément, n'est classifié. Un agrégat d'informations ou supports classifiés peut également être classifié à un niveau supérieur.

d) Principe de transitivité du niveau de classification d'une information extraite d'une information classifiée

Un extrait d'information classifiée conserve le niveau de classification de l'information elle-même, sauf accord de l'autorité compétente désignée par l'autorité émettrice. En l'absence d'indication contraire, la diffusion séquentielle d'extraits non classifiés par découpage de l'information classifiée est interdite. Lorsque des extraits de documents contenant des informations classifiées sont transférés sur un autre support, si ces extraits sont eux-mêmes classifiés, la mention de classification est reportée sur le nouveau support conformément aux dispositions du présent arrêté.

e) Principe de classification des systèmes d'informations classifiés

Pour les systèmes d'information, la décision d'homologation du système vaut décision de classification.

f) Principe de rémanence du niveau de classification des supports informatiques traitant des informations classifiées

En raison de l'impossibilité technique de faire disparaître de manière fiable et irréversible des informations en principe effacées, un support informatique conserve toujours le niveau de classification le plus élevé qui lui a été attribué au cours de son cycle de vie. Il ne peut être déclassé ou déclassifié qu'à la condition que les informations qu'il contient ou a contenues aient elles-mêmes préalablement fait l'objet d'une telle mesure. Il peut être réaffecté dans les conditions prévues au paragraphe 5.2.

1.1.3. Mentions complémentaires à la marque de classification

a) Spécial Monaco

La mention *Spécial Monaco* n'est pas un timbre de classification. Elle est employée pour les informations et supports classifiés ou pour les informations et supports portant la mention *Diffusion Restreinte*, qui ne sauraient être communiqués, en tout ou partie, à un État étranger ou à l'un de ses ressortissants, à une organisation internationale, une institution, un organisme ou un organe de l'Union européenne, voire à une personne morale de droit étranger, même s'il existe un accord de sécurité entre la Principauté et l'État ou la personne de droit international public considérée. La mention *Spécial Monaco* peut ne concerner que certaines parties d'un document.

Lorsque des informations marquées *Spécial Monaco* sont classifiées, elles doivent, outre satisfaire aux mesures de sécurité appropriées à leur niveau de classification, n'être transmises qu'à des personnes physiques ou morales monégasques ou spécifiquement autorisées.

b) Autres mentions particulières

Les informations et supports classifiés devant faire l'objet de restrictions spécifiques de diffusion en raison de leur contenu portent, en plus de la marque éventuelle de leur niveau de classification, une mention particulière précisant les services, les États ou les organisations internationales, les institutions, organes ou organismes de l'Union européenne pouvant y avoir accès ou la classification spéciale dont ils font l'objet. Les modalités d'emploi de ces mentions peuvent faire l'objet de directives d'application.

Cette mention, apposée par l'auteur d'informations ou supports classifiés sous la responsabilité de l'autorité émettrice, a pour effet de circonscrire expressément le périmètre de diffusion de ces informations et supports ainsi que d'attirer l'attention sur le strict besoin d'en connaître. Les mesures de sécurité du niveau de classification sont appliquées et leur acheminement est réalisé de façon à garantir le respect du périmètre de diffusion ainsi délimité.

1.2. Marquage

1.2.1. Visibilité du marquage

L'accès à une information ou un support classifié par une personne non qualifiée est prohibé par la loi n° 1.430 du 13 juillet 2016, suscitée. Aussi, une information doit pouvoir être identifiée comme étant classifiée avant même d'être consultée. Chaque information et support classifié porte ainsi la marque du niveau de classification des informations qu'il contient. Cette marque est qualifiée de « timbre de classification ».

Le marquage constitue une marque de l'autorité publique dont l'usage est strictement réservé aux seules personnes autorisées dans le cadre du présent arrêté.

Des abréviations indiquant la classification peuvent être utilisées pour préciser le niveau de classification des paragraphes du texte d'une information ou d'un support classifié. Les abréviations employées sont les suivantes :

- *Secret de Sécurité Nationale :* SSN ;
- *Très Secret de Sécurité Nationale :* TSSN.

Ces abréviations ne remplacent pas, lorsque cela est possible, la marque de classification inscrite en toutes lettres sur le support.

En cas de non-respect de ces consignes, la protection pénale qui s'attache aux informations classifiées ne s'applique pas.

1.2.2. Marquage des supports préparatoires

Les supports préparatoires servant à l'élaboration d'une information ou d'un support classifié portent un timbre de classification de niveau requis dès lors qu'ils contiennent des informations justifiant la classification de l'information ou du support final.

Dans le cas, à éviter, où la décision de classification ne peut intervenir qu'au moment de la finalisation de l'information ou du support classifié, les informations ou supports ayant servi à l'élaboration

de l'information ou du support classifié (brouillons, documents de travail, impressions sur papier) qui ne sont pas marqués, sont détruits ou effacés, dans les conditions prévues au paragraphe 5.1, le plus rapidement possible dès qu'ils sont devenus sans objet et, en tout état de cause, au plus tard lorsque l'information et le support classifié est émis.

1.2.3. Marquage d'un support papier

Le marquage comprend à la fois le timbre, l'identification et la pagination.

a) Timbre

Il indique le niveau de classification et permet par sa position, sa taille et sa couleur, d'attirer immédiatement l'attention sur le caractère secret de l'information ou du support.

Il est apposé, avec une encre de couleur rouge, ou, à titre exceptionnel, d'une couleur contrastant avec celle du support, au milieu du haut et du bas de chaque page. Pour les documents reliés, un timbre d'un modèle de dimension supérieure est placé au milieu du bas de la couverture et de la page de garde (cf. Appendice 33). Le timbre, dont la dimension peut être adaptée à celle du support, est définitif et toujours visible.

Si l'information doit être divulguée aux seuls ressortissants monégasques, le timbre *Spécial Monaco*, de couleur bleue, est apposé en haut de chaque page, immédiatement à droite ou au-dessous du timbre de classification de l'information.

b) Identification

Tout document classifié est identifié dès sa première page. En plus des références ordinaires de toute pièce administrative, des mesures particulières sont prises. Ainsi, sur la première page du document, figurent :

- le timbre du niveau de classification (cf. Appendice 33) ;
- l'échéance de la classification. Le cas échéant, la mention de déclassement ou de déclassification est apposée sur cette même page (cf. Appendice 34) ;
- les références de l'autorité émettrice et de l'auteur de l'information ou du support classifié ;
- la date d'émission ;
- le numéro d'enregistrement.

Les paragraphes, alinéas, annexes traitant d'informations classifiées à un niveau inférieur ou non classifiées, sont mis en évidence s'il y a lieu, par la mention dans la marge, de leur propre niveau de classification ou de protection, ou par une mise en page qui les détache sans ambiguïté du contexte général du document.

Au niveau *Très Secret de Sécurité Nationale*, chaque document est individualisé par son numéro d'exemplaire et le nombre total d'exemplaires est porté sur la première page. Chaque page porte également la référence du document.

c) Pagination

Chaque page du document est numérotée. Sur la première page sont précisés le nombre total de pages et les annexes ou plans qui le composent.

Les pages de chaque annexe sont numérotées de la pagination du document lui-même, et portent mention du nombre total de pages de l'annexe sur la première page de celle-ci.

Pour les documents classifiés au niveau *Très Secret de Sécurité Nationale*, les pages vierges et les feuilles intercalaires sont également numérotées. Toute page vierge porte en son centre la mention "PAS DE TEXTE".

1.2.4. Marquage d'un matériel classifié hors support amovible

Le marquage d'un matériel classifié hors support amovible est adapté au type de support, définitif et toujours visible. Il consiste en :

- un timbre de classification, spécifiant le niveau de classification ayant une dimension adaptée à celle du support et comporte la mention de ce niveau en toutes lettres. En cas de difficultés pratiques, les abréviations mentionnées au paragraphe 1.2.1 peuvent y être substituées ;
- la référence de l'élément.

1.2.5. Marquage d'un support immatériel

Le marquage d'un support immatériel d'informations classifiées (message ou fichier électronique, base de données, etc.) est adapté au type de support et est toujours visible. Il consiste en :

- un timbre spécifiant le niveau de classification en toutes lettres et ayant une dimension adaptée à celle du support (abréviations). Il peut contenir la mention *Spécial Monaco* si l'information doit être divulguée aux seuls ressortissants monégasques ou spécifiquement autorisés ;
- la référence et, le cas échéant, le volume de chacune des informations enregistrées.

Dans la mesure du possible, les règles de marquage d'un support immatériel doivent respecter les règles de marquage d'un support papier (cf. § 1.2.3).

S'il est matériellement impossible d'apposer le marquage sur le support classifié ou contenant une information classifiée, il convient de mettre en œuvre les mesures techniques et organisationnelles décrites dans le dossier d'homologation et la documentation utilisateur.

1.2.6. Marquage des éléments constitutifs d'un système d'information classifié

Le marquage des éléments constitutifs d'un système d'information classifié est adapté au type d'élément et toujours visible. Il consiste en :

- un timbre spécifiant le niveau de classification en toutes lettres et ayant une dimension adaptée à celle de l'élément ;
- une identification assurée par l'inscription des références de l'élément.

S'il est matériellement impossible d'apposer le marquage sur l'élément, il convient de mettre en œuvre les mesures techniques et organisationnelles décrites dans le dossier d'homologation et la documentation utilisateur.

Les claviers et autres périphériques d'entrée similaires peuvent être exemptés de marquage. Cette exemption doit être mentionnée dans le dossier d'homologation.

1.2.7. Marquage d'un support amovible

Le marquage d'un support amovible d'informations classifiées est adapté au type d'élément et toujours visible. Il consiste en :

- un timbre spécifiant le niveau de classification en toutes lettres et ayant une dimension adaptée à celle du support. En cas de difficultés pratiques, les abréviations mentionnées au paragraphe 1.2.1 peuvent y être substituées ;
- une identification assurée par l'inscription des références du support.

S'il est matériellement impossible d'apposer le marquage sur le support, il convient de mettre en œuvre les mesures techniques et organisationnelles décrites dans le dossier d'homologation et la documentation utilisateur.

Pour les supports amovibles agréés, le marquage est réalisé dans les conditions prévues par les instructions d'emploi du support, mentionnées dans la décision d'agrément.

2. Traçabilité des informations et supports classifiés au sein de l'organisme demandeur

2.1. Organisation de la gestion des informations et supports classifiés

2.1.1. Recommandation au niveau Secret de Sécurité Nationale

Les personnes en charge de la gestion des informations et supports classifiés au niveau *Secret de Sécurité Nationale* doivent être habilitées au niveau au moins égal à ce niveau et sont fonctionnellement rattachées, pour l'accomplissement de ces missions, à l'officier de sécurité de leur organisme.

Il est par ailleurs recommandé aux responsables d'organisme ayant accès à des informations et supports classifiés au niveau *Secret de Sécurité Nationale* de mettre en place un officier de sécurité chargé de veiller à la bonne application de la réglementation relative à la gestion des informations et supports classifiés à ce niveau. Ces missions ne peuvent pas être externalisées.

2.1.2. Obligation au niveau Très Secret de Sécurité Nationale

L'officier de sécurité désigné par le Ministre d'État assure le traitement, le marquage, la conservation et le suivi des informations et supports classifiés au niveau *Très Secret de Sécurité Nationale* jusqu'à leur destruction ou leur versement à un service d'archives. À ce titre, il est responsable de l'enregistrement, de l'expédition, de la réception et de la circulation des informations et supports classifiés à ce niveau, qui ne peuvent transiter que par son intermédiaire, hormis ceux comportant la mention « ACSSI ». Il dresse un inventaire annuel des informations et supports classifiés qu'il traite.

Pour remplir ses missions, l'officier de sécurité peut mettre en place un système assurant par voie informatique les fonctions suivantes :

- identification du support d'information (numéro d'enregistrement arrivée ou départ, autorité émettrice et auteur de l'information ou du support classifié, date de création, domaine, titre ou objet, nombre de pages, niveau de classification, mode et date prévue de déclassification, nombre d'exemplaires qu'il gère) ;
- traçabilité des événements concernant les exemplaires du support d'information (arrivée, départ, reproduction, archivage, destruction, déclassement/déclassification, numéro de référence de l'événement, date de l'événement, référence individuelle des exemplaires, nom et fonction du détenteur de chaque exemplaire) ;
- recherche sur les supports d'information (détenteurs successifs d'un exemplaire, date de création, service émetteur, etc.) ;
- inventaire des informations et supports classifiés ;
- fourniture d'états relatifs aux actions effectuées sur les supports d'information (historique, fiche d'enregistrement, fiche de suivi, bordereau d'envoi, procès-verbal de destruction, avis de déclassement/déclassification, archivage, reproduction, etc.).

Aucun organisme ne peut élaborer, traiter, conserver, détruire ou acheminer des informations et supports classifiés au niveau *Très Secret de Sécurité Nationale* faisant l'objet d'une classification spéciale sans y avoir été préalablement autorisé par le Ministre d'État.

2.1.3. Organisation des échanges d'informations et de supports classifiés avec des personnes physiques ou morales de droit étranger

Conformément à l'article 18 de la loi n° 1.430 du 13 juillet 2016, suscitée, la Principauté assure la même protection aux informations et supports classifiés étrangers, reçus ou produits en commun en vertu d'un accord de sécurité, général ou spécifique, régulièrement approuvé et publié, qu'aux informations et supports classifiés monégasques de niveau équivalent.

Symétriquement, la communication d'informations ou supports classifiés monégasques à une personne physique ou morale relevant de la juridiction d'un État étranger ou d'une organisation internationale n'est possible qu'en vertu d'un accord intergouvernemental conclu entre la Principauté et

l'État ou l'organisation internationale considéré ou conformément aux règles de sécurité de l'organisation internationale, lorsque ces dernières sont directement applicables.

Les accords intergouvernementaux relatifs à l'échange et à la protection d'informations classifiées peuvent porter soit :

- sur un domaine spécifique (généralement celui de la sécurité nationale) : l'accord est alors qualifié d'accord de sécurité dans le domaine considéré ;
- sur l'ensemble de l'action gouvernementale : l'accord est alors qualifié d'accord général de sécurité.

Plutôt que de définir, avec chaque partenaire, des mesures de protection *ad hoc*, ces accords fonctionnent sur la base d'un modèle-type et organisent la protection des informations et supports échangés sur la base d'un régime d'équivalence entre les niveaux de classification monégasques et ceux du partenaire. Ce régime d'équivalence est établi après analyse de la législation du partenaire et présenté généralement sous la forme d'un tableau d'équivalence.

La mention *Diffusion Restreinte* qui n'est pas, en Principauté, une mention de classification conférant à ces informations la protection pénale propre au secret de sécurité nationale, mais qui peut être un niveau de classification chez certains partenaires fait, par ailleurs, généralement l'objet d'un traitement spécifique au sein de ces accords.

Partant, sauf dispositions contraires dans l'accord ou des règles de sécurité applicables qu'il convient toujours de consulter avant tout échange d'information ou support classifié avec un partenaire étranger, la gestion (enregistrement, conservation, reproduction, diffusion, transport, expédition, réception, inventaire) des informations et supports classifiés étrangers confiés à la Principauté suit des règles au moins aussi strictes que celles applicables aux informations classifiées nationales de niveau équivalent.

De la même façon, la protection des systèmes d'information traitant d'informations classifiées confiées à la Principauté par des états étrangers ou par des organisations internationales voire des institutions est assurée conformément à l'accord ou aux règles de sécurité applicables.

Symétriquement, lorsque des informations classifiées monégasques sont transmises *via* et sur des systèmes d'information relevant de la responsabilité d'états étrangers ou d'organisations internationales voire d'institutions, les mesures de protection sont fixées par l'accord ou les règles de sécurité applicables, qui assure(nt) à ces informations un niveau de protection au moins équivalent à celui prévu dans le présent arrêté.

Les accords et règles de sécurité font, le cas échéant, l'objet d'instructions complémentaires pour leur application en Principauté. Notamment, dans le cadre des échanges avec les organisations internationales, des règles spécifiques peuvent s'ajouter aux règles nationales et imposer une supervision par l'autorité nationale de sécurité (rôle endossé en Principauté par le Ministre d'État) des modalités de gestion des informations et supports classifiés émis dans le cadre de l'organisation internationale, quel que soit le niveau de classification des informations et supports considéré.

Enfin, des règles complémentaires, si nécessaire plus restrictives, peuvent être stipulées dans le plan contractuel de sécurité attaché à des contrats internationaux nécessitant d'échanger ou de produire des informations ou supports classifiés avec un partenaire étranger.

À défaut d'instruction ou de stipulations complémentaires, les dispositions de la présente annexe s'appliquent.

2.2. Enregistrement

Tout support d'information classifiée est enregistré, dans l'ordre chronologique, dans un système d'enregistrement spécifique, manuel ou informatisé, dont l'accès est restreint aux personnes ayant le besoin d'en connaître. Si ce système est classifié, les personnes y ayant accès sont habilitées au niveau requis.

Pour les informations classifiées dématérialisées, les obligations d'enregistrement sont assurées par les fonctions de traçabilité du système d'information classifié les hébergeant.

L'enregistrement établit sans ambiguïté l'attribution du support à un détenteur, personne physique, clairement identifiée. Le détenteur assume alors la responsabilité de la protection du support. Cet enregistrement est la seule référence de cette attribution de responsabilité. Dans la mesure du possible, le numéro d'enregistrement est assorti d'une fiche où sont inscrites les références des informations contenues. Pour chaque support classifié, il est précisé dans le système d'enregistrement l'échéance de classification fixée par l'auteur de l'information. La mention de l'objet du document peut figurer dans le système d'enregistrement s'il porte le même niveau de protection ou de classification précisé par son auteur que le système ou si son auteur a précisé qu'il n'était pas protégé.

2.2.1. Au niveau Secret de Sécurité Nationale

Un système d'enregistrement est mis en place par le responsable d'organisme avec l'appui de l'officier de sécurité. Il est tenu, sous le contrôle de l'officier de sécurité, par les personnes en charge de la gestion des informations et supports classifiés. Ce système peut être relié à une base de gestion du courrier sous réserve que l'accès à la base soit restreint aux seules personnes ayant le besoin d'en connaître et que cette base permette de tracer les documents jusqu'au détenteur final.

2.2.2. Au niveau Très Secret de Sécurité Nationale

L'officier de sécurité assure l'enregistrement des informations et supports classifiés sur un système d'enregistrement classifié au niveau *Très Secret de Sécurité Nationale*.

Chaque support d'informations classifiées au niveau *Très Secret de Sécurité Nationale* fait l'objet d'une double numérotation présentée sous la forme d'une fraction comportant le numéro d'enregistrement de l'auteur sur le numéro d'enregistrement de l'officier de sécurité chargé de leur traitement.

2.3. Conservation

Le responsable d'organisme met en place des moyens de conservation sécurisés et pérennes des informations et supports classifiés. Lorsque l'organisme dispose de plusieurs établissements, chaque établissement détenant des informations ou supports classifiés dispose des moyens sécurisés et pérennes nécessaires à leur conservation.

En dehors des périodes d'utilisation, les supports classifiés sont conservés dans un meuble de sécurité (coffre-fort ou armoire forte) répondant aux exigences énoncées dans le présent arrêté (cf. Appendice 26). Le niveau de classification des documents contenus ne doit pas figurer à l'extérieur du meuble.

Des informations et supports classifiés de diverses origines peuvent être conservés à l'intérieur d'un même meuble de sécurité à condition d'en assurer le cloisonnement en séparant et précisant l'origine des supports et sous réserve que les personnes y ayant accès aient le même besoin d'en connaître. Dans le cas contraire, les informations et supports classifiés sont conservés dans des sous-coffres précisant leur origine.

La combinaison du meuble de sécurité, suffisamment complexe pour être fiable, n'est connue que des seuls utilisateurs. Une copie de cette combinaison est conservée sous enveloppe opaque, fermée, dans le coffre-fort ou l'armoire forte d'une autorité spécialement désignée, la clef de ce meuble, le cas échéant, étant elle-même placée dans un meuble distinct.

La combinaison est changée tous les ans et, à chaque fois, en cas de mutation des utilisateurs, d'identification d'un risque ou de suspicion de compromission.

Les clefs des lieux abritant des informations et supports classifiés sont impérativement mises en sécurité, notamment hors des heures ouvrables, suivant une procédure clairement établie par chaque autorité responsable (dépôt dans un coffre mural, sans clef, à combinaison et à commande unique ou avec ouverture par lecture de badge, garde permanente avec système d'alarme, etc.). Il est formellement interdit d'emporter les clefs de ces lieux et des meubles de sécurité à l'extérieur des locaux de travail.

La responsabilité de la conservation des informations et supports classifiés incombe au détenteur auquel l'information ou le support classifié a été attribué, à l'officier de sécurité ou aux personnes en charge de la gestion des informations et supports classifiés.

Les informations classifiées dématérialisées sont stockées sur un système d'information homologué au même niveau de classification ou au niveau supérieur. Les exigences de sécurité relatives à la sécurité du système d'information de l'organisme prévoient des moyens et des procédures de sauvegarde et de conservation sécurisés et pérennes des informations classifiées contenues au sein des systèmes d'information classifiés utilisés. Ces moyens et procédures respectent le besoin d'en connaître. Le système de sauvegarde est du même niveau de classification que le système d'information traitant les données.

2.4. Reproduction

Le Ministre d'État et le Conseiller de Gouvernement - Ministre de l'Intérieur définissent les consignes pour la reproduction et l'impression de supports classifiés respectivement au niveaux *Très Secret de Sécurité Nationale* et *Secret de Sécurité Nationale.*

Ces consignes :

- désignent les personnes habilitées à autoriser la reproduction ;
- fixent les procédures et les mesures techniques garantissant la traçabilité des impressions, le contrôle du processus par le détenteur, de bout en bout, du lancement de l'impression jusqu'à la récupération de l'information classifiée imprimée.

Le détenteur de l'information ou du support classifié initial est responsable des reproductions et impressions qu'il entreprend jusqu'à leur attribution à un autre détenteur conformément aux modalités du présent arrêté, complétées, le cas échéant, par les consignes évoquées supra, les directives techniques particulières et le plan contractuel de sécurité applicables.

Les matériels utilisés pour la reproduction d'informations classifiées (photocopieuses, télécopieurs, systèmes informatiques, etc.) sont physiquement protégés afin d'en limiter l'emploi aux seules personnes autorisées.

Si ces matériels sont connectés à un système d'information, ils sont intégrés dans le périmètre d'homologation du système d'information. Les opérations de maintenance sur ces matériels sont effectuées dans des conditions permettant de garantir la sécurité des informations classifiées qui ont été reproduites, dans le respect des dispositions de la présente annexe complétée, le cas échéant, par les directives techniques particulières et le plan contractuel de sécurité applicables. Il en est de même pour leur mise au rebut qui doit garantir la destruction des mémoires de ces appareils (cf. § 5.2).

La reproduction numérique d'informations classifiées dématérialisées est autorisée et se fait sous la responsabilité de l'utilisateur, qui est sensibilisé par l'officier de sécurité sur les bonnes pratiques en la matière. Il veille ainsi à limiter la diffusion de ces informations classifiées dématérialisées selon le strict besoin d'en connaître et s'assure que la convention de marquage de ces informations est respectée. Lorsque la reproduction numérique est réalisée sur un support amovible, elle respecte les exigences prévues par le présent arrêté (cf. Titre VI §8 et Titre VII §3.1.1)

2.4.1. Au niveau Secret de Sécurité Nationale

La reproduction totale est effectuée par le détenteur, sous sa responsabilité, à condition de conserver sur un système d'enregistrement détenu par les personnes en charge de la gestion des informations et supports classifiés à ce niveau, les traces du nombre et des destinataires des exemplaires papiers reproduits.

Pour les informations classifiées dématérialisées, ce suivi est assuré par les fonctions de traçabilité du système d'information prévues par le présent arrêté.
La reproduction partielle est possible dans les mêmes conditions que la reproduction totale. Les extraits d'informations classifiées ainsi reproduits sont classifiés au même niveau que le document dont ils sont extraits, sauf si l'autorité émettrice les a expressément classifiés à un niveau inférieur ou ne les a pas classifiés (cf. § 1.2.3 b)).

2.4.2. Au niveau Très Secret de Sécurité Nationale

La reproduction des informations papier et supports classifiés n'est possible qu'avec l'autorisation écrite préalable de l'autorité émettrice.

Le détenteur de l'information papier ou du support classifié qui souhaite en effectuer une reproduction adresse une demande motivée (cf. Appendice 35) à cette autorité, en précisant le nombre d'exemplaires. Si l'autorité émettrice consent à la reproduction (cf. Appendice 36), elle porte mention de cette reproduction sur l'exemplaire en sa possession. L'officier de sécurité désigné par le Ministre d'État assure l'enregistrement de cet(ces) exemplaire(s) et le(s) fait prendre en compte par la (les) personne(s) citée(s) dans la demande.

En cas d'urgence et à titre exceptionnel, le détenteur peut s'affranchir de cette procédure à la condition de prendre les dispositions suivantes :

- limiter au minimum indispensable le nombre de reproductions ;
- procéder au marquage réglementaire en attribuant à chaque exemplaire un numéro individuel composé de deux nombres fractionnaires, en numérateur le numéro d'ordre de la copie dans la série des reproductions et en dénominateur le nombre total de reproductions ;
- porter, sur l'exemplaire reproduit, la destination qui en est faite ou établir une liste séparée des destinataires ;
- rendre compte sans délai à l'autorité émettrice du nombre de reproductions, des numéros de reproduction et de la destination des exemplaires. L'autorité émettrice porte mention de cette reproduction sur l'exemplaire en sa possession.

Pour les informations classifiées dématérialisées, ce suivi est assuré par les fonctions de traçabilité du système d'information prévues par le présent arrêté décrites au Titre VI paragraphe 6.4.

2.5. Gestion des éléments constitutifs d'un système d'information classifié

La sortie d'éléments constitutifs d'un système d'information classifié de la zone dans laquelle ils se trouvent est soumise à une autorisation de l'officier de sécurité identifiant clairement les équipements concernés et désignant nominativement les personnes autorisées à sortir ces éléments. Cette autorisation peut avoir un caractère ponctuel ou permanent.

3. Diffusion des informations et supports classifiés

3.1. Envoi d'informations et supports classifiés

Avant toute diffusion d'informations ou supports classifiés, son auteur établit la liste des destinataires en s'assurant qu'ils sont habilités au niveau de classification requis. Si cette liste est sensible, elle n'est pas jointe aux informations et supports classifiés.

3.1.1. Transmission dématérialisée d'informations classifiées

La transmission d'informations classifiées ne peut être réalisée que depuis ou vers un système d'information classifié. Le transfert d'une information classifiée au travers d'un réseau non classifié ou d'un niveau de classification inférieur s'effectue uniquement à l'aide de moyens de chiffrement agréés.

3.1.2. Expédition d'informations et supports classifiées

Les procédures d'expédition doivent :

- permettre de respecter des délais compatibles avec le degré d'urgence de la transmission ;
- permettre le suivi des informations ou des supports transmis ;
- garantir leur intégrité physique grâce à un conditionnement adapté.

Les autorités d'expédition sont :

- au niveau *Secret de Sécurité Nationale*, les personnes en charge de la gestion des informations et supports classifiés à ce niveau (cf. § 2.1.1) ;
- au niveau *Très Secret de Sécurité Nationale*, l'officier de sécurité (cf.§ 2.1.2).

Au niveau *Très Secret de Sécurité Nationale*, le nombre et le numéro des supports attribués à chaque destinataire ainsi que le numéro des exemplaires conservés par l'émetteur sont précisés dans la liste de diffusion (deux exemplaires au moins, dont un original destiné à terme aux archives).

Après marquage et enregistrement de chaque support, il est procédé aux opérations suivantes :

a) Conditionnement

L'envoi de supports classifiés se fait sous double enveloppe. Chaque enveloppe présente des garanties de solidité suffisantes pour garantir au maximum son intégrité physique :

- l'enveloppe extérieure : renforcée, elle porte l'indication du service expéditeur, l'adresse du destinataire (sans mention trop explicite de nature à attirer l'attention sur le caractère classifié du contenu) et la mention du suivi. Elle ne porte en aucun cas la mention du niveau de classification de l'information ou du support qu'elle contient ;
- l'enveloppe intérieure de sécurité : opaque, toilée ou armée, elle interdit l'ouverture ou la refermeture discrète. Elle porte le timbre du niveau de classification, la référence des supports transmis, le cachet de l'autorité expéditrice, le nom et la fonction du destinataire ainsi que l'indication de l'organisme dans lequel il est affecté.

b) Suivi de l'expédition

Un bordereau d'envoi, sans timbre de classification ni indication de l'objet des informations envoyées, est placé dans l'enveloppe intérieure de sécurité. Il comporte trois feuillets détachables A, B et B' (cf. Appendice 37), signés par le responsable de l'autorité expéditrice ou une personne désignée par lui :

- les feuillets A et B sont placés dans l'enveloppe intérieure et sont adressés au destinataire (cf. § 3.1) qui conserve le premier comme élément de preuve et renvoie le second à titre d'accusé de réception ;
- le feuillet B' est conservé par l'expéditeur jusqu'à réception du feuillet B qui lui est alors substitué.

L'expéditeur s'assure de la date et de l'heure de livraison. Il en avise aussitôt le service destinataire par courrier électronique en indiquant les références du support, à l'exclusion de leur objet et de leur caractère secret. Tout retard anormal doit conduire à suspecter une compromission.

3.2. Transport

3.2.1. Supports classifiés

a) Sur le territoire de la Principauté, à l'intérieur d'un site ou d'une même emprise

Les supports classifiés sont transportés par le détenteur lui-même, par une personne habilitée au niveau requis ou un convoyeur autorisé de l'organisme détenteur ou une personne du service de courrier interne de cet organisme.

La position des supports classifiés doit être suivie sans discontinuité, notamment dans le système d'enregistrement des supports classifiés.

Une fiche de suivi, établie pour chaque support classifié au niveau *Très Secret de Sécurité Nationale*, permet d'en contrôler la position et est émargée par chaque personne qualifiée y ayant accès. La fiche de suivi est conservée par l'officier de sécurité du Ministre d'État dans les mêmes conditions que pour un support classifié au niveau *Très Secret de Sécurité Nationale*.

b) Sur le territoire national, avec changement de site ou d'emprise

Le transport s'opère :

- aux niveaux *Secret* et *Très Secret*, par un porteur, qui est :
  - soit une personne habilitée de l'organisme détenteur ou d'un autre organisme ou d'un organisme lié par contrat (cf. Titre IV § 3) ;
  - soit une personne ayant la qualité de convoyeur autorisé. Le convoyeur autorisé est une personne physique appartenant à l'organisme détenteur, titulaire d'une décision de sécurité

convoyeur (cf. Appendice 38) délivrée par l'autorité d'habilitation après réalisation, par l'autorité compétente, d'une enquête administrative (cf. Appendice 2). Conformément à la demande de l'autorité d'habilitation, cette décision est valide soit pour une mission particulière, soit pour une durée nécessairement inférieure à trois ans. Cette décision peut être renouvelée par une demande qui est nécessairement effectuée avant l'expiration du délai fixé. Cette décision n'autorise en aucun cas à prendre connaissance d'informations et supports classifiés.

Le porteur ne peut se dessaisir des informations et supports classifiés jusqu'à leur remise au destinataire, sauf dérogation exceptionnelle accordée par le Ministre d'État ou le Conseiller de Gouvernement - Ministre dont il dépend.

- au niveau *Secret,* le transport par voie postale est autorisé à la condition impérative de confier le transport à la poste monégasque et par LRAR ;

au niveau *Très Secret*, le transport par voie postale est prohibé.

c) Vers ou depuis l'étranger

Les supports classifiés envoyés à l'étranger ou transitant par des pays étrangers doivent être protégés en permanence pour interdire leur compromission pendant le transport, et notamment lors des escales. Les supports classifiés marqués *Spécial Monaco* ne peuvent sortir du territoire, de manière exceptionnelle, que par lettre de courrier délivrée par le Département des Relations Extérieures et de la Coopération.

Le transport ne peut s'opérer que - par porteur muni d'un certificat de courrier : lorsqu'un accord ou un règlement international de sécurité le prévoit, le transport est possible par porteur, dans les conditions déterminées au point b). Le porteur est alors muni d'un certificat de courrier pour un seul ou plusieurs voyages (cf. Appendice 39 et Appendice 40), délivré par le Ministre d'État, en sa qualité d'autorité nationale de sécurité. Il est rappelé au porteur qu'il s'engage, tout au long du voyage, à garder en sa possession ou sous sa surveillance directe le colis contenant les documents, équipements ou composants classifiés.

Pour les informations échangées dans le cadre d'un accord ou d'un programme international, il convient de se référer aux stipulations de l'accord ou du plan contractuel de sécurité applicable.

3.2.2. Transport d'informations classifiées sur un support amovible

Par principe, les informations classifiées stockées sur un support amovible en vue de leur transport sont chiffrées.

Lorsqu'elles sont chiffrées aux moyens d'un produit ou d'un mécanisme de chiffrement agréé par l'Agence Monégasque de Sécurité Numérique au niveau de classification des informations transportées, le support amovible peut être transporté sans mesure de sécurité complémentaire.

En l'absence de solution agréée au niveau de classification requis ou lorsqu'à titre exceptionnel le chiffrement est impossible, le support amovible est transporté conformément aux dispositions du paragraphe 3.2.1.

3.2.3. Matériels classifiés

La circulation et le transport des matériels classifiés nécessitent des mesures particulières de sécurité : protection contre les vues dans la mesure du possible et garde permanente pendant la durée du transport.

Les itinéraires sont choisis en fonction du degré de sécurité qu'ils présentent. L'autorité en ayant prescrit le mouvement assume la responsabilité des tâches suivantes :

- conditionnement des matériels ;
- choix de l'itinéraire et des lieux d'étape, en accord avec les autorités civiles ou militaires intéressées des pays concernés ;
- organisation du convoyage ou de l'escorte et des dispositions techniques en cas de panne ou d'accident.

Le transport des matériels classifiés est effectué, sauf impossibilité absolue ou opération conjointe, par des moyens monégasques. A défaut, ils sont convoyés et toutes les dispositions sont prises pour que la sécurité soit assurée sans discontinuité pendant toute la durée du transport. Avant tout transport de matériel classifié, un certificat de courrier (cf. Appendice 39 et Appendice 40) est établi pour le porteur. Un plan de transport peut être exigé par le Ministre d'État, en sa qualité d'autorité nationale de sécurité qui le soumet pour avis technique et archivage après validation à l'Agence Monégasque de Sécurité Numérique.

3.3. Réception

La réception est assurée par le destinataire de l'envoi au niveau *Secret de Sécurité Nationale* ou, au niveau *Très Secret de Sécurité Nationale* par l'officier de sécurité désigné par le Ministre d'État, suivant la procédure suivante :

- l'intégrité de l'emballage est vérifiée afin de déceler une éventuelle compromission ;
- le destinataire fait procéder à son enregistrement :
  - au niveau *Secret de Sécurité Nationale*, auprès du service en charge de la gestion des informations et supports classifiés à ce niveau ;
  - au niveau *Très Secret de Sécurité Nationale*, par l'officier de sécurité désigné par le Ministre d'État ;
- pour le support physique, le feuillet B du bordereau d'envoi est complété, daté, signé et renvoyé à titre d'accusé de réception.

Ces règles s'appliquent à la réception, par voie physique, des informations et supports devant faire l'objet d'un enregistrement (cf. § 2.2).

Dans le cas d'une information classifiée dématérialisée, la réception est attestée par les fonctions de traçabilité du système d'information classifié prévues par le présent arrêté.

4. Suivi des supports et informations

4.1. Principes généraux

Tout support classifié, y compris les supports de stockage d'informations classifiées dématérialisées, fait l'objet d'un suivi permanent afin d'assurer sa traçabilité et sa prise en compte par des détenteurs habilités.

À cette fin, un inventaire est réalisé chaque année par chaque détenteur avant le 31 décembre et avant toute prise et fin de fonction, sous le contrôle de l'officier de sécurité.

À l'occasion de l'inventaire, chaque détenteur procède à l'examen rigoureux de la pertinence de la conservation des supports qu'il détient, ainsi que du maintien de la classification des informations et supports dont il est l'auteur. Si le maintien de la classification n'est plus nécessaire, l'auteur prévient les destinataires de leur déclassification ou déclassement dans les conditions prévues au paragraphe 6.4.

L'inventaire des informations classifiées dématérialisées contenues au sein d'un système d'information classifié n'est pas obligatoire, leur suivi étant assuré par la traçabilité interne du système d'information renforcée par les exigences organisationnelles et logiques prévues par le présent arrêté.

4.1.1. Destruction des exemplaires inutiles

Lorsque plusieurs copies d'un même support initial sont détenues :

- si l'original est détenu, seul l'original est conservé ;
- si seules des copies sont détenues, une seule copie est conservée.

Les autres copies sont détruites conformément aux dispositions du paragraphe 5.1.

4.1.2. Réexamen de la pertinence de la classification

La pertinence de la classification d'une information ou d'un support classifié évolue dans le temps.

Chaque détenteur réévalue, à l'occasion de l'inventaire, la pertinence du niveau de classification des informations et supports classifiés dont il est l'auteur et procède, chaque fois que possible, à leur déclassification, ou, à tout le moins, à leur déclassement. Dans les cas, rares, où du fait de circonstances particulières une information ou un support classifié dont il est l'auteur a, depuis sa classification, gagné en sensibilité, le détenteur procède, le cas échéant, à son reclassement, conformément aux directives du Ministre d'État. Il s'assure que les destinataires disposent bien du bon niveau d'habilitation et applique les directives prévues au paragraphe 6.4.

Pour toutes les décisions de déclassification mentionnée au paragraphe 6.3, chaque organisme détenteur vérifie, en outre, au moment de l'inventaire, si les supports qu'il détient ont fait l'objet d'une déclassification et procède, le cas échéant, à leur démarquage conformément à l'Appendice 34.

4.1.3. Appréciation de l'utilité administrative courante

Lors de l'inventaire, chaque détenteur identifie les informations et supports classifiés ne présentant plus d'utilité administrative courante et procède à leur destruction, ou à leur versement aux archives selon les modalités respectivement définies aux paragraphes 5.1, 5.2 et 5.4.

4.1.4. Banalisation d'une période dédiée à l'inventaire

Afin de permettre aux détenteurs d'informations et supports classifiés de procéder à cet examen rigoureux, chaque responsable d'organisme arrête une période ouvrée dédiée à l'inventaire, au cours de laquelle les détenteurs sont déchargés de leurs missions habituelles.

De même, le responsable d'organisme accorde à chaque personne détenant des informations et supports classifiés quittant ses fonctions une période lui permettant de procéder à son inventaire.

L'inventaire précise, pour chaque support classifié, l'échéance de classification fixé par son auteur pour le compte de l'autorité émettrice.

Si l'inventaire fait mention de documents dont l'objet est classifié, il est lui-même classifié au niveau de classification le plus élevé des documents qu'il inventorie.

Les modalités d'inventaire et de suivi des informations et supports classifiés *Secret de Sécurité Nationale* et *Très Secret de Sécurité Nationale*, hors classifications spéciales, détenus par les organismes relevant de son champ d'attribution sont définies respectivement par le Ministre d'État et le Conseiller de Gouvernement - Ministre de l'Intérieur.

4.2. Inventaire au niveau Secret de Sécurité Nationale

Un inventaire annuel est effectué sous la responsabilité de chaque détenteur qui doit être en mesure de le présenter aux éventuelles personnes en charge de la gestion des informations et supports classifiés et, dans tous les cas de figure, à l'officier de sécurité dont il dépend.

Un inventaire est effectué, sous forme contradictoire, à chaque mutation de personnel, l'ancien détenteur et le nouveau apposant tous deux leur signature sur le procès-verbal.

4.3. Inventaire au niveau Très Secret de Sécurité Nationale

Un inventaire annuel est effectué par l'officier de sécurité. Le procès-verbal d'inventaire annuel mentionne les références et l'identification de chaque support classifié *Très Secret de Sécurité Nationale* et est accompagné, le cas échéant, de l'une ou l'autre des pièces administratives suivantes :

- un bordereau de prise en compte ;
- un procès-verbal de destruction (cf. Appendice 41) ;
- une fiche de suivi du support (cf. paragraphe 3.2.1 a)) ;
- un procès-verbal de versement au service des archives compétent.

Un inventaire est effectué, sous forme contradictoire, à chaque mutation de personnel, l'ancien détenteur et le nouveau apposant tous deux leur signature sur le procès-verbal.

5. Fin d'exploitation des informations et supports classifiés

Toute autorité détenant des informations et supports classifiés, produits ou reçus, a pour obligation de faire assurer leur conservation et leur protection conformément aux dispositions législatives et réglementaires en vigueur.

À l'expiration de leur période d'utilisation courante, les informations et supports classifiés font l'objet d'un tri, selon la périodicité prévue par le Ministre d'État ou le Conseiller de Gouvernement - Ministre de l'Intérieur, visant à séparer les supports destinés à être conservés de ceux dépourvus d'utilité administrative ou d'intérêt historique ou scientifique :

- les supports présentant une utilité administrative ou un intérêt historique ou scientifique sont versés au service des archives compétent;
- les autres supports sont détruits selon les principes développés au paragraphe suivant.

5.1. Procédure de destruction

Lorsque des informations et supports classifiés sont périmés ou devenus inutiles, il peut être procédé à leur destruction avec l'accord du Ministre d'État ou des Conseillers de Gouvernement - Ministres. La destruction ne peut être réalisée que par des personnes habilitées ou sous leur surveillance.

La destruction est effectuée de façon à rendre impossible toute reconstitution même partielle des informations contenues sur les supports.

Les techniques de destruction sont adaptées au nombre et au type de supports à détruire. Les principales formes de destruction[7] sont le brûlage, l'incinération, le broyage, le déchiquetage et la surtension électrique.

Les opérations de destruction faisant appel aux techniques de déchiquetage voire de broyage doivent respecter les prescriptions de la norme DIN 66399 en fonction du degré de protection ou de classification de l'information ou du support :

	CLASSE (DIN 66399)	NIVEAU DE SÉCURITÉ (DIN 66399)
TRÈS SECRET DE SÉCURITÉ NATIONALE	3	7
SECRET DE SÉCURITÉ NATIONALE	3	6
DIFFUSION RESTREINTE	2	5

Les informations ou supports classifiés au niveau « Très Secret de Sécurité Nationale » doivent en plus être incinérés.

Lorsque des documents classifiés doivent être transportés afin d'être incinérés, ils doivent impérativement avoir été préalablement déchiquetés et mélangés.

Après l'opération, un procès-verbal de destruction est dressé. Ce procès-verbal de destruction porte la signature du détenteur et, en sus pour les documents *Très Secret de Sécurité Nationale*, celle d'un témoin habilité au niveau *Très Secret de Sécurité Nationale* (cf. Appendice 41).

Au niveau *Très Secret de Sécurité Nationale*, le détenteur du support informe par écrit l'autorité émettrice que, sauf avis contraire de sa part, elle procédera à sa destruction. Sans réponse dans un délai de deux mois, le détenteur procède à la destruction du support et en rend compte à l'autorité émettrice en lui adressant une copie du procès-verbal de destruction. Une copie de ce procès-verbal est également transmise à l'officier de sécurité.

[7] Le brûlage consiste à exposer l'ensemble du support ou de la surface utile à une température de plus de 1 000°C avec un chalumeau ; l'incinération est une combustion complète réduisant le support à l'état de cendre, destinée à empêcher toute dispersion de fragments ; le déchiquetage est une opération qui réduit le support en lambeaux ; le broyage consiste à réduire le support en pulpe.

5.2. Mise au rebut ou réaffectation sécurisée du matériel informatique classifié

Un support classifié ou ayant contenu des informations classifiées ne peut être affecté à un nouvel utilisateur ou à un nouveau besoin qu'après effacement sécurisé de l'ensemble des informations et supports classifiés qu'il contient et reste classifié à un niveau au moins égal au niveau de classification des informations et supports classifiés qu'il a préalablement contenus.

En l'absence d'une telle procédure d'effacement sécurisé, le support classifié n'est pas réaffecté.
Tout support de stockage électronique classifié mis au rebut est préalablement effacé selon les recommandations de l'Agence Monégasque de Sécurité Numérique. À défaut, il est détruit physiquement, selon un procédé conforme aux recommandations de ladite agence, qui rend impossible la reconstitution en tout ou partie de l'information classifiée qu'il a contenue.

5.3. Évacuation et destruction d'urgence

Pour faire face à des circonstances exceptionnelles et en cas de menace immédiate nécessitant l'évacuation des bâtiments par le personnel ou la destruction des informations et supports classifiés, des plans d'évacuation et de destruction d'urgence sont établis par chaque service ou organisme qui détient des informations et supports classifiés. Ces plans prévoient notamment les procédures d'accès, en toute circonstance, aux locaux et aux informations et supports classifiés.

Les modalités d'exécution pratiques de ces plans figurent sur des fiches placées dans chaque coffre par les personnes détenant des éléments couverts par le secret de sécurité nationale. Elles précisent :

- les autorités désignées pour donner l'ordre de destruction ou d'évacuation ;
- la liste des informations et supports classifiés à détruire ou à évacuer ;
- les mesures applicables aux systèmes d'information ;
- la liste et la localisation des moyens de destruction et d'évacuation à utiliser.

La mise en œuvre du dispositif ainsi établi est contrôlée par l'officier de sécurité tous les trois ans.

5.4. Versement aux archives

5.4.1. Préparation du versement par le service versant

a) Examen systématique de la pertinence de la classification par le service versant

i. le service versant est l'auteur de l'information classifiée

Avant tout versement aux archives, le service versant s'assure que la classification demeure pertinente et procède, chaque fois que possible, à sa déclassification selon les modalités prévues au paragraphe 6.4. Lorsqu'après examen, il s'avère que la déclassification n'est pas possible, le support est traité selon les modalités décrites dans les paragraphes suivants.

ii. le service versant n'est pas l'auteur de l'information classifiée

Le support est traité selon les modalités décrites au paragraphe 5.4.2.

Dans le cas où l'information ou le support a fait l'objet d'une décision de déclassification, le service versant appose le timbre de déclassification conformément à l'Appendice 34.

Dans le cas où l'information ou le support n'a pas fait l'objet d'une décision de déclassification, lorsque le service versant est distinct du service ayant procédé à la classification, le support est traité selon les modalités décrites au paragraphe 5.4.2.

b) Identification et regroupement des supports classifiés

Avant chaque versement au service d'archives compétent, chaque support classifié contenu dans un dossier se voit attribuer un numéro d'ordre et fait l'objet d'un inventaire précisant, conformément à l'Appendice 42, la cote d'archives, le nom du service ayant procédé à la classification ou de l'auteur du support classifié, son numéro d'enregistrement, sa date d'émission, son titre ou objet, son niveau de classification et l'échéance de la classification. Ces supports et l'inventaire qui les décrits sont réunis, selon

le niveau de classification et le volume représenté, dans une enveloppe scellée conforme à l'Appendice 42, rangée en tête du dossier auquel ils appartiennent, ou dans des articles clairement séparés des articles non classifiés de manière à faciliter leur protection au sein du service d'archives détenteur.

Le service des archives compétent se charge ensuite de porter sur chaque article matériel (carton, enveloppe ou dossier) sa référence archivistique (« cote »).

5.4.2. Versement et conservation au service d'archives compétents

a) Responsabilité du service d'archives compétent

Lorsque des informations ou supports classifiés sont versés au service d'archives compétent, la responsabilité de leur protection incombe à ce dernier. Le Ministre d'État s'assure de la conformité aux exigences de la présente annexe des conditions de conservation des informations et supports classifiés.

Le service d'archives compétent peut recevoir des informations et supports classifiés jusqu'au niveau *Très Secret de Sécurité Nationale* hors classifications spéciales. Les informations et supports classifiés au niveau *Très Secret de Sécurité Nationale* faisant l'objet d'une classification spéciale ne peuvent être versés aux archives qu'après une procédure, obligatoire et préalable, de déclassement ou de déclassification.

b) Conservation des informations et supports classifiés

Les supports classifiés versés au service d'archives compétent sont conservés dans l'enveloppe scellée rangée en tête du dossier auquel ils appartiennent ou dans des articles clairement séparés et identifiés conservés dans les conditions de sécurité définies au Titre V, et comme prévu au paragraphe 5.4.1 b). L'ensemble est conservé conformément aux exigences détaillées au présent Titre VII.

5.5. Accès aux archives classifiées détenues par le service des archives compétent

Conformément au paragraphe 2.1.1, seule une personne habilitée et qui dispose du besoin d'en connaître pour l'exercice de sa fonction ou l'accomplissement de sa mission peut accéder à des archives classifiées versées au service des archives, compétent. Elle doit, en outre, si d'autres délais de communicabilité sont attachés au document, obtenir préalablement une autorisation de consultation anticipée. Cette autorisation peut être assortie de conditions spécifiques.

Une telle autorisation n'est pas nécessaire pour les représentants de l'autorité émettrice ou les agents du service des archives.

Lorsqu'une personne habilitée mais ne disposant pas du besoin d'en connaître pour l'exercice de sa fonction ou l'accomplissement de sa mission, ou bien lorsqu'une personne non habilitée souhaite accéder à une archive classifiée détenue par le service d'archives, et qui, par conséquent, ne lui est pas librement communicable, sa demande est instruite selon la procédure définie par l'Art. 6 de l'arrêté n° 2016-723, modifié.

6. Expiration de la classification

6.1. Délai de communicabilité

Aucun document classifié, même à l'issue du délai de communicabilité de cinquante ans fixé par le présent arrêté, ne peut être communiqué tant qu'il n'a pas été formellement démarqué par l'apposition d'un timbre de déclassification conforme à l'Appendice 34 sous peine de faire encourir au consultant les peines prévues pour le délit de compromission.

6.2. Mention d'échéance de la classification

La sensibilité d'une information ou d'un support classifié évolue en fonction du temps ou des circonstances.

La protection qui lui est accordée initialement peut ainsi être réévaluée soit dans le sens d'un renforcement (reclassement au niveau supérieur), soit, dans la majorité des cas, dans le sens d'un abaissement prenant la forme d'un déclassement ou d'une déclassification. De même, une information ou un support non protégé peut être classifié postérieurement à son émission si l'évolution de sa sensibilité au regard de la sécurité nationale l'exige.

Afin de garantir le caractère dérogatoire du recours au secret de sécurité nationale et de limiter les lourdeurs liées à la gestion des informations classifiées, l'auteur de l'information classifiée, apprécie, sous la responsabilité de l'autorité émettrice et selon les directives qu'elle a fixées, la durée utile de classification.

Ainsi, l'auteur de l'information procède simultanément à deux opérations juridiques distinctes : la classification, qu'il matérialise par l'apposition d'un timbre de classification, et la déclassification à une date d'entrée en vigueur différée, qu'il matérialise par l'apposition d'une date d'échéance valant timbre de déclassification. Cette date est antérieure à l'échéance du délai de cinquante ans prévu pour sa communicabilité et, pour faciliter l'accès des chercheurs aux archives publiques lui est même largement antérieure dans la très grande majorité des cas.

Pour autant, l'autorité émettrice conserve la possibilité de prolonger à tout moment le délai fixé, sous sa responsabilité, par l'auteur de l'information classifiée, ainsi que la possibilité de déclasser ou reclasser le support.

Lorsqu'à titre exceptionnel aucune date entraînant automatiquement la déclassification du support ne peut être déterminée, l'auteur de l'information classifiée indique la date ou le délai au terme duquel, en sus des réexamens annuels mentionnés au paragraphe 4.1.2, le niveau de classification doit impérativement être réévalué.

Cette date ou ce délai n'excède pas vingt ans à compter de la date de production du support.

Par dérogation aux dispositions précédentes, les informations classifiées, dont la divulgation est susceptible de nuire à la sauvegarde des intérêts fondamentaux de la Principauté ou ne comportent aucune échéance de classification, ne peuvent être déclassifiées.

6.3. Réexamen de la classification des informations et supports classifiés détenus par le service d'archives

Afin de faciliter l'accès aux archives publiques, le Ministre d'État identifie, parmi les ensembles d'archives comportant un volume important de documents classifiés, ceux qui sont fréquemment sollicités ou sont susceptibles de l'être, ou qui présentent un intérêt particulier pour la recherche historique ou scientifique. Il en fait rapport aux autorités émettrices compétentes, afin qu'elles puissent apprécier la pertinence du maintien en classification des documents considérés et que soit, le cas échéant, entreprise une déclassification anticipée et homogène de l'ensemble considéré.

Un point d'étape des déclassifications décidées dans ce cadre est réalisé à chaque réunion de la Commission instituée par l'article 16 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale.

6.4. Procédure de déclassification

Les supports classifiés mentionnent, dans leur timbre, la date à partir de laquelle leur classification devient caduque, sans qu'une décision de déclassification, ni que l'apposition d'un timbre de déclassification, ne soit nécessaire.

Les dispositions qui suivent s'appliquent donc aux seuls informations et supports classifiés qui ne comportent pas une telle mention et qui ne peuvent être déclassifiés qu'après décision de déclassification, matérialisée sur le document par l'apposition d'un timbre de déclassification.

6.4.1. Organisation de la fonction de déclassification

Lorsque le support classifié ne comporte pas dans son timbre de classification de date à partir de laquelle il est automatiquement déclassifié, seule l'autorité émettrice peut décider de reclasser, déclasser ou déclassifier le support (cf. Art. 6 de l'arrêté ministériel n° 2016-723, modifié).

6.4.2. Matérialisation de la décision de classification sur le support classifié

Pour que la décision de déclassification des informations et supports classifiés, qui ne mentionnent pas dans leur timbre de classification de date à partir de laquelle ils sont automatiquement déclassifiés, produise pleinement ses effets et permette leur manipulation sans risque de compromission, elle doit être matérialisée sur le support par l'apposition d'un timbre de déclassification qui précise la date et la référence de la décision de déclassification, conformément au modèle de l'Appendice 34. Cette opération est appelée « démarquage ».

6.4.3. Information des destinataires et consignation des décisions de déclassification

L'autorité ayant procédé à la déclassification informe de sa décision de déclassification les destinataires à qui elle a transmis les informations et supports objet de la décision, afin qu'ils procèdent à leur démarquage.

6.4.4. Déclassification des informations et supports classifiés d'origine étrangère

Pour les informations et supports classifiés d'origine étrangère, seule l'autorité étrangère émettrice peut procéder à leur déclassification ou leur déclassement.

6.4.5. Communicabilité des supports déclassifiés

La déclassification d'un support n'entraîne pas pour autant automatiquement la libre communicabilité de ce support ou des informations qu'il contient.

Ainsi, l'Administration saisie d'une demande de communication d'une information ou d'un support régulièrement déclassifié doit s'assurer qu'aucun autre motif d'incommunicabilité ne trouve à s'appliquer.

GLOSSAIRE

Accord de sécurité : accord intergouvernemental conclu entre au moins deux États ou au sein d'une alliance multinationale et ayant pour objet la protection d'informations ou de supports classifiés. Ces accords comprennent l'identification et la reconnaissance mutuelle des autorités nationales de sécurité, la correspondance des niveaux de classification, la reconnaissance mutuelle des habilitations de personnes, les modalités de transmission et de protection des informations et supports classifiés.

Administrateur de sécurité : personne chargée de la mise en œuvre, du maintien, du contrôle et de l'évolution des mesures de sécurité à appliquer à tout système d'information contenant des informations ou supports classifiés aux niveaux « *Secret de Sécurité Nationale* » ou « *Très Secret de Sécurité Nationale* ».

Administrateur système : personne chargée de la mise au point, de l'exploitation, de la maintenance, du contrôle et des évolutions du système informatique.

Annexe de sécurité : énumération des instructions de sécurité relatives à un contrat classifié.

Archivage : opération consistant à verser à un service d'archives des supports d'information lorsqu'ils ne sont plus d'utilisation habituelle. Les supports faisant encore l'objet d'une classification ne peuvent être archivés que dans certaines conditions et dans des services habilités à les recevoir. Un support classifié au niveau « *Très Secret de Sécurité Nationale* » ne peut en aucun cas être archivé.

Authenticité : propriété d'une information ou d'un traitement qui garantit son identité, son origine et, éventuellement, sa destination.

Autorité d'habilitation : autorité compétente pour solliciter une enquête d'habilitation ou un contrôle élémentaire et émettre la décision.

Autorité Nationale de Sécurité (A.N.S.) : organisme gouvernemental chargé des relations avec les autres États et les structures internationales en matière d'habilitation de personnes et de protection des informations ou supports classifiés. Pour la Principauté de Monaco, l'ANS est le Ministre d'État.

Avis de sécurité : conclusion émise par le Directeur de la Sûreté Publique à l'issue d'investigations se rapportant à une personne et visant à détecter et à évaluer les vulnérabilités de cette personne. L'avis de sécurité est une aide à la décision d'habilitation, mais il ne lie pas l'autorité responsable de la décision.

Besoin d'en connaître : nécessité impérieuse de prendre connaissance d'une information dans le cadre d'une fonction déterminée, pour la bonne exécution d'une mission précise.

Catalogue des emplois : dans un organisme, liste des emplois qui peuvent nécessiter l'accès aux informations ou supports classifiés ou portant la mention particulière « Spécial Monaco ». Le catalogue est dressé sur le seul critère du besoin d'en connaître.

Certificat de sécurité : document prouvant l'habilitation d'une personne au traitement d'informations ou supports classifiés à un niveau précisé.

Classification spéciale : catégorie d'informations ou supports classifiés au niveau « *Très Secret de Sécurité Nationale* » et répondant à la nécessité de cloisonnement. Les classifications spéciales sont organisées en réseaux de sécurité constitués d'antennes d'utilisation. Les habilitations au niveau « *Très Secret de Sécurité Nationale* » sont prononcées au titre d'une ou plusieurs classifications spéciales expressément désignées.

Compromission : prise de connaissance, certaine ou possible, d'une information ou d'un support classifié par une ou plusieurs personnes non qualifiées.

Confidentialité : caractère réservé d'une information ou d'un traitement dont l'accès est limité aux seules personnes admises à la (le) connaître pour les besoins du service, ou aux entités ou processus autorisés.

Convoyeur : personne titulaire d'une « décision de sécurité convoyeur » délivrée par une autorité d'habilitation pour convoyer un document, équipement ou composant classifié.

Décision d'habilitation (au secret de sécurité nationale) : acte administratif autorisant, au terme de la procédure d'habilitation, le titulaire, en fonction de son besoin d'en connaître, à accéder aux informations ou aux supports classifiés d'un niveau déterminé. L'intéressé est informé de la décision d'habilitation, qui ne lui est jamais remise.

Décision de sécurité convoyeur : autorisation accordée pour assurer, durant le transport, la garde des informations ou des supports classifiés.

Déclassement : modification, par abaissement, du niveau de classification d'informations ou supports classifiés.

Déclassification : suppression de la classification d'informations ou supports classifiés à quelque niveau que ce soit.

Disponibilité : propriété d'une information ou d'un traitement d'être utilisable à la demande par une personne ou par un système.

Dossier d'habilitation : dossier constitué en vue de l'habilitation d'une personne. Il comporte la demande d'habilitation établie par l'autorité demanderesse et attestant le besoin d'en connaître, la notice individuelle renseignée par l'intéressé et une photographie d'identité récente.

Donnée : toute représentation d'une information sous une forme conventionnelle destinée à faciliter son traitement.

Engagement de responsabilité : document en deux volets signés par le titulaire de l'habilitation lors de sa prise et de sa cessation de fonction. L'engagement a pour but de rappeler à cette personne la responsabilité pénale qui lui incombe du fait de son habilitation. La signature de l'encart central du formulaire de l'engagement de responsabilité par l'intéressé vaut prise de connaissance de la décision.

Homologation de sécurité : déclaration par l'autorité d'homologation, au vu du dossier d'homologation, que le système d'information considéré est apte à traiter des informations d'un niveau de classification donné conformément aux objectifs de sécurité visés, et que les risques de sécurité résiduels sont acceptés et maîtrisés. L'homologation de sécurité reste valide tant que le système d'information (SI) opère dans les conditions approuvées par l'autorité d'homologation.

Identification : mention figurant sur un support d'information et précisant le numéro de l'exemplaire ainsi que son numéro d'enregistrement.

Imputabilité : capacité à identifier l'auteur d'une action.

Information : tout renseignement ou tout élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, à un enregistrement ou à un traitement.

Information ou support classifié : procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier présentant un caractère de secret de sécurité nationale.

Intégrité : propriété assurant qu'une information ou un traitement n'a pas été modifié ou détruit de façon non autorisée.

Lieux abritant des éléments classifiés : locaux dans lesquels sont détenus des informations ou supports classifiés, quel qu'en soit le niveau.

Marquage : opération consistant à apposer sur un support classifié les mentions précisant son niveau de classification, le numéro d'exemplaire, le numéro d'enregistrement, la pagination pour un document papier et, le cas échéant, la destination exclusivement nationale.

Matériel classifié : objet, équipement, installation, système ou substance présentant un caractère de secret de la sécurité nationale et qui nécessite une protection appropriée au niveau *« Très Secret de Sécurité Nationale »*, *« Secret de Sécurité Nationale »* ou *« Confidentiel de Sécurité Nationale »*.

Mise en éveil : démarche initiée par l'autorité d'habilitation auprès de la personne à habiliter pour la sensibiliser à ses vulnérabilités découvertes au cours de l'enquête administrative.

Mise en garde : démarche initiée par l'autorité d'habilitation visant à sensibiliser l'officier de sécurité du service employeur d'une personne sur l'existence d'éléments pouvant présenter un risque de vulnérabilité de la personne à habiliter.

Non-répudiation : impossibilité de nier la participation au traitement d'une information.

Notice individuelle : formulaire destiné à recueillir les renseignements nécessaires à l'habilitation d'une personne. Elle doit être renseignée par l'intéressé lui-même et constitue un élément majeur du dossier d'habilitation. Elle est exploitée par l'autorité chargée de prononcer la décision et par le Directeur de la Sûreté Publique.

Officier de sécurité : nommé par le responsable du service employeur, il est le correspondant de l'Agence Monégasque de Sécurité Numérique et de la Direction de la Sûreté Publique. Il a pour mission, sous les ordres de son autorité d'emploi et en fonction des modalités propres à chaque structure, de fixer les règles et consignes de sécurité à mettre en œuvre concernant les personnes et les informations ou supports classifiés et d'en contrôler l'application. Il participe à l'instruction et à la sensibilisation du personnel en matière de protection du secret de sécurité nationale. Il est chargé de la gestion des habilitations et, en liaison avec le Directeur de la Sûreté Publique, du contrôle des accès aux zones abritant des éléments du secret de sécurité nationale.

Personne habilitée : est habilitée, au sens de l'article 18 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale, la personne qui, par son état, sa profession, sa fonction ou sa mission, temporaire ou permanente, est habilitée à avoir accès à une information classifiée et a le besoin d'en connaître.

Plan d'urgence : document établi par un organisme détenteur d'informations ou supports classifiés, prévoyant, en cas de circonstances exceptionnelles, les modalités d'évacuation ou de destruction des supports d'information.

Procédure d'habilitation : procédure visant à s'assurer qu'une personne peut, sans risque pour la sécurité nationale ou pour sa propre sécurité, connaître des informations ou supports classifiés dans l'exercice de ses fonctions.

Qualification d'un produit de sécurité : reconnaissance formelle que le produit de sécurité évalué peut protéger des informations jusqu'à un niveau spécifié dans les conditions d'emploi définies.

Reclassement : modification, par relèvement, du niveau de classification d'informations ou de supports classifiés.

Refus d'habilitation : décision prise par l'autorité d'emploi, au vu de l'avis de sécurité ou de tout autre élément recueilli sur une personne, de ne pas habiliter cette personne.

Réseau de sécurité : ensemble des moyens humains, matériels et organisationnels qui permettent l'acheminement en toute sécurité des informations ou supports classifiés à un niveau déterminé (et en deçà), entre un ensemble de correspondants habilités.

Responsable de la classification : autorité émettrice d'informations qui leur attribue, en fonction de leur contenu, un niveau de classification approprié.

Renouvellement d'habilitation : procédure déclenchée à la fin de validité d'un avis de sécurité concernant une personne déjà habilitée en vue d'obtenir un avis actualisé. Ce nouvel avis permettra de prononcer une décision d'habilitation au profit de la personne qui présente encore le besoin d'en connaître.

Retrait d'habilitation : décision prise par l'autorité d'emploi, au vu d'éléments nouveaux de vulnérabilité, de supprimer l'habilitation d'une personne.

Sensibilisation : instruction périodiquement prodiguée aux personnes habilitées ou susceptibles d'être habilitées et destinée à leur faire prendre conscience des enjeux de la protection du secret de sécurité nationale, des sanctions judiciaires et administratives encourues et de la nécessité d'appliquer les mesures de sécurité prescrites.

Support : tout moyen matériel, quelles qu'en soient la forme et les caractéristiques physiques, permettant de recevoir, de conserver ou de restituer des informations ou des données.

Système d'information : ensemble des moyens informatiques ayant pour finalité d'élaborer, de traiter, de stocker, d'acheminer, de présenter ou de détruire des informations.

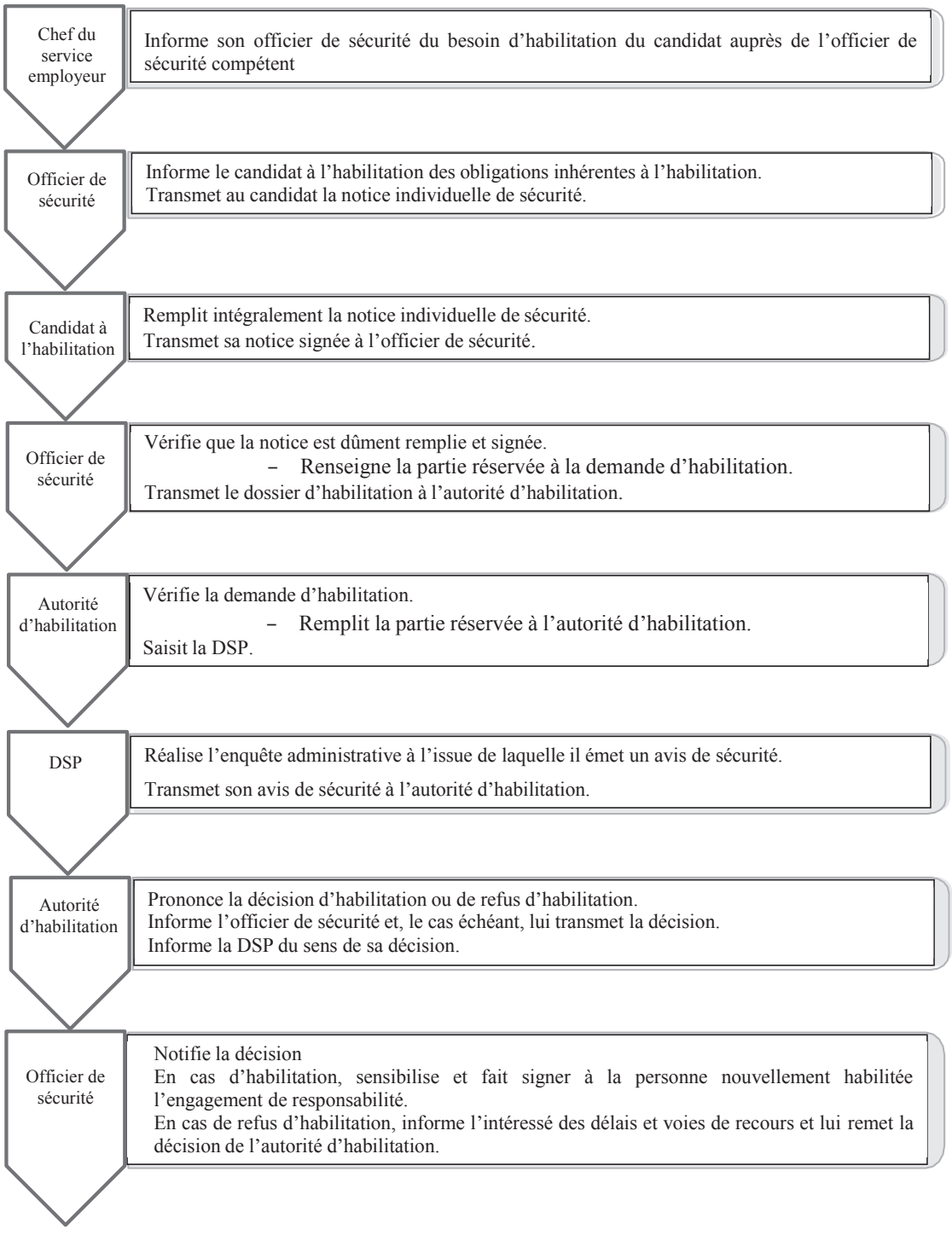
Timbre : mention figurant sur un support d'information précisant son niveau de classification et, le cas échéant, son usage national exclusif. Le timbre possède des caractéristiques définies (dimensions, aspect).

Vulnérabilité : fait relatif à la situation d'une personne et qui amoindrit les garanties qu'elle présente pour la protection des informations ou supports classifiés. Il s'agit d'une fragilité qui peut donner lieu à des pressions de diverses natures et qui doit être prise en compte pour accorder avec ou sans restriction, pour refuser ou pour retirer l'accès aux informations ou supports classifiés.

Zone protégée : lieu (local, établissement ou terrain clos délimité) matérialisé intéressant la sécurité nationale, bénéficiant d'une protection juridique, au sens de l'article 19 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale, où la libre circulation est interdite et l'accès soumis à autorisation.

APPENDICES

Appendice 1 - Schéma présentant la procédure d'habilitation au secret de sécurité nationale à Monaco



Appendice 2 – Modèle de demande d'enquête administrative

Département :

Organisme :

Date et numéro d'enregistrement :

DEMANDE D'ENQUETE ADMINISTRATIVE

Motifs de la demande :

Identité de la personne

Nom :

Prénom :

Date et lieu de naissance :
Nationalité(s) de naissance :
Nationalité(s) actuelle(s) :
Domicile actuel :

Domicile antérieur :

Renseignements

Grade ou titre :

Fonctions ou missions exercées :

Nom, qualité, date, signature de l'autorité
et cachet de l'organisme

Appendice 3 – Modèle de dossier de demande d'habilitation d'une personne physique

1- À remplir par l'autorité d'emploi/administrative du candidat à l'habilitation	
Autorité d'emploi/administrative	
Organisme : N° de la demande :	Date d'enregistrement de la demande :
Procédure d'habilitation engagée	
Type de demande : Procédure d'urgence :	☐ ADMISSION ☐ RENOUVELLEMENT ☐ RÉVISION ☐ Oui, le cas échéant, préciser et motiver la demande :
Habilitation demandée	
Niveau d'habilitation : Nature des informations et supports classifiés :	☐ SECRET DE SECURITE NATIONALE ☐ TRÈS SECRET DE SECURITE NATIONALE, le cas échéant, préciser la classification spéciale : ☐ France ☐ Monaco ☐ Autres, préciser :
Motif de la demande	
Emploi et fonctions exercées (sans acronyme) : Préciser, le cas échéant, le numéro de poste au catalogue des emplois :	
Officier de sécurité en charge du dossier	
Nom – prénom : N° de téléphone : Email :	Date et signature

2- Pour les ressortissants monégasques employés par une personne morale de droit à l'étranger, à remplir par l'autorité étrangère compétente (autorité nationale de sécurité, autorité de sécurité désignée/déléguée étrangère, autre)	
Autorité compétente :	Date et signature

3- À remplir par l'autorité monégasque d'habilitation	
Organisme : Nom - prénom de la personne en charge du dossier :	Date et signature

NOTICE INDIVIDUELLE DE SECURITE

À renseigner intégralement

Identité du candidat à l'habilitation	
Nom de famille *(de naissance, en lettres majuscules) :*	Insérer une photographie d'identité de moins de 3 mois
Nom d'usage *(en lettres majuscules) :*	
Prénoms : *Indiquer en premier le prénom d'usage*	
Sexe : ☐ M ☐ F	
Surnom ou alias éventuels :	
Email(s) personnel(s) actif(s) :	
Comptes de réseaux sociaux :	
Téléphone fixe :	Téléphone portable :
Naissance	
Date :	Pays :
Ville :	Code postal :
Nationalité(s)	
Nationalité(s) actuelle(s) : Si autres nationalités, préciser : - lesquelles : - année d'arrivée à Monaco : - année d'acquisition de la nationalité monégasque :	

Documents administratifs	Numéro	Date de délivrance	Autorité de délivrance
Carte nationale d'identité			
Passeport			
Document étranger			
Autre, préciser :			

Domicile actuel		
N°, rue :		
Ville :	Code postal :	Pays :
Depuis le :		
Identité des personnes résidant au même domicile (autres que celles visées dans « situation de famille actuelle » page 3) :		
Domicile précédent (si changement depuis moins de six mois)		☐ Cocher si sans objet
N°, rue :		
Ville :	Code postal :	Pays :
Période :		

Résidence secondaire ou occasionnelle, y compris à l'étranger ☐ Cocher si sans objet
si nécessaire, utiliser l'espace « renseignements complémentaires » page 7

N°, rue :
Ville : Code postal : Pays :
Depuis le : Téléphone domicile :

Situation professionnelle actuelle

Fonction/profession : ☐ Civil ☐ Militaire
Organisme d'emploi : Depuis le :
Adresse professionnelle :
Téléphone(s) professionnel(s) :
Email(s) professionnel(s) :

Le cas échéant, préciser :
- Département d'origine :
- Département d'emploi :
- grade :
- pour les militaires, précisez Carabinier ou Sapeurs-Pompiers :

Emploi(s) successif(s) durant les cinq dernières années,
si nécessaire, utiliser l'espace « renseignements complémentaires » page 7

Organisme d'emploi et adresse *(n°, rue, code postal, commune, pays si étranger)*	Emploi/fonction	Période	
		du	au

Habilitation déjà détenue ☐ Cocher si sans objet

Niveau d'habilitation : Autorité d'habilitation :
Depuis le :

Niveau d'études et culture générale

Diplômes obtenus ou niveau équivalent	Langues étrangères	
	Langues	Degré de connaissance

Situation de famille actuelle

☐ Célibataire ☐ En instance de mariage ☐ Marié(e) ☐ Veuf(ve) ☐ Séparé(e)
☐ Divorcé(e) ☐ En instance de remariage ☐ Remarié(e) ☐ Concubinage ☐ PACS
☐ Autre situation (avec ou sans cohabitation):

Depuis le : Ville : Pays :

Enfant(s) ne pas mentionner les enfants du conjoint nés d'une précédente union ; s*i nécessaire, utiliser l'espace « renseignements complémentaires » page 7* ☐ Cocher si sans objet

Nom – prénom - sexe	Date, lieu de naissance *(ville et code postal)*	Nationalité(s)	Domicile *(n°, rue, code postal, commune, pays si étranger) si distinct (ex. garde partagée)*

Autre parent des enfants mineurs nés d'une précédente union, *si nécessaire, utiliser l'espace « renseignements complémentaires » page 7* ☐ Cocher si sans objet			
Nom – prénom de l'enfant	Nom – prénom du parent	Date, lieu de naissance du parent *(ville et code postal)*	Nationalité(s) du parent

Parents du candidat (même si décédés)	**Père**	**Mère**
Nom – prénom(s). *Pour la mère : nom de jeune fille suivi du nom d'usage*		
Date, lieu de naissance *(ville, code postal, pays)*		
Nationalité(s) actuelle(s)		
Si autre(s) nationalité(s), *préciser lesquelles, l'année d'arrivée à Monaco ou en France et l'année d'acquisition de la nationalité monégasque ou française*		
N° carte nationale d'identité ou de passeport *(obligatoire pour les ressortissants étrangers)*		
Adresse du domicile actuel ou du dernier domicile avant le décès *(N°, rue, code postal, commune, pays)* Le cas échéant, préciser la date du décès		
Nom et adresse de l'employeur actuel ou du dernier employeur *(pas d'acronyme) (N°, rue, code postal, commune, pays)*		

Fratrie *si nécessaire, utiliser l'espace « renseignements complémentaires » page 7* ☐ Cocher si sans objet				
Nom – prénom - sexe	Date, lieu de naissance *(ville et code postal)*	Nationalité(s)	Profession	Domicile *(n°, rue, code postal, commune, pays)*

Voyages et séjours à l'étranger durant les cinq dernières années en partant du plus récent. *Si nécessaire, utiliser l'espace « renseignements complémentaires » page 7* ☐ Cocher si sans objet		
Pays – adresse *(séjours de plus de six mois)*	Période *(date de début et de fin)*	Motif : professionnel, familial, touristique, etc.

Identité du conjoint du candidat à l'habilitation (personne visée dans le cadre « situation de famille actuelle » page 2)	
Nom de famille *(de naissance, en lettres majuscules) :*	
Nom d'usage *(en lettres majuscules) :*	
Prénoms : *Indiquer en premier le prénom d'usage*	Sexe : ☐ M ☐ F
Surnom ou alias éventuels :	
Email(s) personnel(s) actif(s) :	
Téléphone fixe :	Téléphone portable :
Naissance	
Date :	Pays :
Ville :	Code postal :
Nationalité(s)	
Nationalité(s) actuelle(s) :	
Si autres nationalités, préciser : - lesquelles : - année d'arrivée à Monaco ou en France : - année d'acquisition de la nationalité monégasque ou française :	

Documents administratifs	Numéro	Date de délivrance	Autorité de délivrance
Carte nationale d'identité			
Passeport			
Document étranger			
Autre, préciser :			

Domicile actuel		
N°, rue :		
Ville :	Code postal :	Pays :
Depuis le :		
Identité des personnes résidant au même domicile (autres que celles visées dans « situation de famille actuelle » page 6) :		
Résidence secondaire ou occasionnelle, y compris à l'étranger *si nécessaire, utiliser l'espace « renseignements complémentaires » page 7*		☐ Cocher si sans objet
N°, rue :		
Ville :	Code postal :	Pays :
Depuis le :	Téléphone domicile :	
Situation professionnelle actuelle		
Fonction/profession :	☐ Civil ☐ Militaire (Précisez Carabiniers ou Pompiers) :	
Organisme d'emploi :	Depuis le :	
Adresse professionnelle :		
Téléphone(s) professionnel(s) :		
Email(s) professionnel(s) :		
Le cas échéant, préciser : - Organisme d'origine : - Organisme d'emploi : - grade :		

Niveau d'études et culture générale		
Diplômes obtenus ou niveau équivalent	Langues étrangères	
	Langues	Degré de connaissance

Enfant(s) ne mentionner que les enfants nés d'une précédente union. *Si nécessaire, utiliser l'espace « renseignements complémentaires » page 7* ☐ Cocher si sans objet

Nom – prénom - sexe	Date, lieu de naissance *(ville et code postal)*	Nationalité(s)	Domicile si distinct *(n°, rue, code postal, commune, pays si étranger)*

Parents du candidat (même si décédés)	**Père**	**Mère**
Nom – prénom(s). *Pour la mère : nom de jeune fille suivi du nom d'usage*		
Date, lieu de naissance *(ville, code postal, pays)*		
Nationalité(s) actuelle(s)		
Si autre(s) nationalité(s), préciser lesquelles, l'année d'arrivée en France et l'année d'acquisition de lanationalité française		
N° carte nationale d'identité ou de passeport *(obligatoire pour les ressortissants étrangers)*		
Adresse du domicile actuel ou du dernier domicile avant le décès *(N°, rue, code postal, commune, pays)* Le cas échéant, préciser la date du décès		
Nom et adresse de l'employeur actuel ou du dernier employeur *(pas d'acronyme) (N°, rue, code postal,commune, pays)*		

Fratrie *si nécessaire, utiliser l'espace « renseignements complémentaires » page 7* ☐ Cocher si sans objet

Nom – prénom - sexe	Date, lieu de naissance *(ville et code postal)*	Nationalité(s)	Profession	Domicile *(n°, rue, code postal, commune, pays)*

Voyages et séjours à l'étranger durant les cinq dernières années en partant du plus récent. *Si nécessaire, utiliser l'espace « renseignements complémentaires » page 7* ☐ Cocher si sans objet

Pays – adresse *(séjours de plus de six mois)*	Période *(date de début et de fin)*	Motif : professionnel, familial, touristique, etc.

Si un renseignement n'a pas été apporté, veuillez en expliquer la raison en précisant la rubrique concernée.	☐ Cocher si sans objet

Renseignements complémentaires, préciser la rubrique complétée	☐ Cocher si sans objet

1) Pensez-vous, vous-même ainsi que votre conjoint(e) ou concubin(e)

- avoir été sollicité(e) en dehors de vos attributions professionnelles pour fournir des informations à caractère sensible ? ☐ OUI ☐ NON
- que des pressions ont été exercées sur vous, ou sur des membres de votre famille, à la suite d'un incident survenu sur le territoire étranger ? ☐ OUI ☐ NON
- avoir été l'objet d'approches de la part d'un service de renseignement ou de sécurité étranger ? ☐ OUI ☐ NON

En cas de réponse(s) positive(s), décrire les circonstances :

2) Avez-vous des proches parents résidant à l'étranger ou entretenez-vous des relations autres que professionnelles avec des ressortissants étrangers ? ☐ Cocher si sans objet

Nom et prénom	Date et lieu de naissance	Nationalité	Caractériser le lien *(parenté, amical, etc.)*	Ville et pays de résidence	Employeur

3) Etes-vous en relations professionnelles suivies avec des ressortissants étrangers ou des personnes travaillant pour des administrations étrangères ou des organisations internationales ? Si oui, préciser. ☐ Cocher si sans objet

4) Si vous souhaitez communiquer un point particulier au service chargé de l'instruction de votre dossier, remplissez le champ suivant. ☐ Cocher si sans objet

ATTESTATION DU CANDIDAT A L'HABILITATION

Je soussigné(e) : (nom et prénom)

- *reconnais avoir été informé(e) de l'objet de l'habilitation à laquelle je suis candidat(e) et de sa portée. Ainsi, il m'a été indiqué que la décision d'habilitation, si elle est favorable, m'autorise, en fonction de mon besoin d'en connaître, à accéder à des informations et supports classifiés au(x) niveau(x) précisé(s) dans cette décision. Il m'a également été précisé que la présente demande d'habilitation déclenche une procédure destinée à vérifier qu'il m'est possible, sans risque pour la sécurité nationale ou pour ma propre sécurité, de connaître des informations et supports classifiés dans l'exercice de mes fonctions ou dans le cadre de l'accomplissement de ma mission ;*
- *reconnais être informé(e) :*
- *du caractère obligatoire des réponses qui me sont demandées ;*
- *qu'en l'absence de réponse aux questions posées, aucune décision ne pourra être prise quant à mon éventuelle habilitation ;*
- *que je dispose d'un droit d'accès et de rectification, en application de la loi n°1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée que je pourrais exercer auprès de l'officier de sécurité dont ma procédure d'habilitation dépend ;*
- *que les informations recueillies font l'objet d'un traitement informatique destiné à la gestion des habilitations au secret de sécurité nationale ;*
- *que le destinataire des données de ce traitement est, en fonction de ses attributions et dans la limite du besoin d'en connaître, l'officier de sécurité dont je dépends,*
- *certifie l'exactitude des renseignements que j'ai fournis dans la présente notice et admets avoir été informé(e) que je m'expose, en cas d'altération frauduleuse de la vérité conformément à l'article 90 du Code pénal, aux peines prévues par l'article 98 du Code pénal.*
- *déclare avoir été dûment avisé(e) qu'en vertu des dispositions législatives et réglementaires relatives à la protection du secret de sécurité nationale, l'habilitation à laquelle je me porte candidat(e) engage ma responsabilité et fait naître à ma charge des obligations, parmi lesquelles celles de :*
- *garantir la sécurité des informations et supports classifiés auxquels je peux avoir accès par le strict respect de la réglementation applicable ;*
- *répondre, pénalement et administrativement, de tout acte de malveillance, d'imprudence, de négligence ou d'inattention ayant pour résultat la destruction, le détournement, la soustraction, la reproduction ou la divulgation au public ou à une personne non qualifiée, d'une information ou d'un support classifié (article 19 de la loi n° 1.430 du 13 juillet 2016 suscitée).*

A

Le

Signature du candidat

Appendice 4 – Modèle de décision d'habilitation d'une personne physique

Département :

Organisme :

Date et numéro d'enregistrement :

DECISION D'HABILITATION

Le[8] :

Décide que

Madame/Monsieur[9] :

Date et lieu de naissance :

Grade ou titre :

Fonctions ou missions :

Est habilité(e) jusqu'au[10] **:**

Pour accéder à des informations et supports classifiés au(x) niveau(x)[11] :

- ☐ TRÈS SECRET de SÉCURITÉ NATIONALE
- ☐ TRÈS SECRET de SÉCURITÉ NATIONALE avec Classification spéciale (précisez lesquelles) :
- ☐ SECRET de SÉCURITÉ NATIONALE

A

Le

Signature et cachet de l'autorité d'habilitation

[8] Autorité d'habilitation ou autorité ayant reçu délégation à cet effet
[9] Nom et prénom
[10] Date d'expiration de la décision d'une durée égale ou moindre à celle de l'avis de sécurité
[11] Préciser le(s) niveau(x) de classification auquel (auxquels) il est donné accès

Appendice 5– Modèle d'attestation de mise en garde

Département :

Organisme :

Date et numéro d'enregistrement :

ATTESTATION DE MISE EN GARDE

Je[12] soussigné(e)[13] :

certifie avoir été mis(e) en garde en présence de :

contre les risques que pourrait faire courir l'habilitation de[14] :

à connaître des informations et supports classifiés au(x) niveau(x)[15]:

- ☐ TRÈS SECRET de SÉCURITÉ NATIONALE
- ☐ TRÈS SECRET de SÉCURITÉ NATIONALE avec Classification spéciale (précisez lesquelles) :
- ☐ SECRET de SÉCURITÉ NATIONALE

A

Le

Signature de l'autorité compétente ou de l'officier de sécurité

[12] À remplir par l'autorité compétente ou l'officier de sécurité.
[13] Préciser les nom et prénom, grade ou titre, fonction
[14] Nom et prénom, grade ou titre, fonction du candidat à l'habilitation
[15] Préciser le(s) niveau(x) de classification auquel (auxquels) il est donné accès

Appendice 6 – Modèle d'attestation de mise en éveil

Département :

Organisme :

Date et numéro d'enregistrement :

ATTESTATION DE MISE EN EVEIL

Je[16] soussigné(e)[17]:

reconnais avoir été mis(e) en éveil le :

en présence de[18]:

sur les risques que pourrait faire courir mon habilitation à connaître des informations et supports classifiés au(x) niveau(x) :[19]

- ☐ TRÈS SECRET de SÉCURITÉ NATIONALE
- ☐ TRÈS SECRET de SÉCURITÉ NATIONALE avec Classification spéciale (précisez lesquelles) :
- ☐ SECRET de SÉCURITÉ NATIONALE

Je m'engage à ne pas divulguer les informations et supports classifiés dont je pourrais avoir connaissance dans l'exercice de mes fonctions ou l'accomplissement de ma mission et à signaler immédiatement à mon officier de sécurité ou mon autorité d'emploi, toute tentative de pression dont je pourrais faire l'objet.

Intéressé(e)	Officier de sécurité	Autorité d'habilitation ou représentant
signature	signature	signature

[16] À remplir par le candidat à l'habilitation.[140].[141].[142]
[17] Nom et prénom, grade ou titre, fonction
[18] Nom et prénom, grade ou titre, fonction
[19] Cocher la case concernée

Appendice 7 – Modèle d'engagement de responsabilité

Département :

Organisme :

Date et numéro d'enregistrement :

ENGAGEMENT DE RESPONSABILITE

VOLET 1

Je, soussigné(e) : déclare :

- *avoir été informé(e) de la décision en date du m'autorisant l'accès à des informations et supports classifiés au(x) niveau(x):*

☐ TRÈS SECRET de SÉCURITÉ NATIONALE
☐ TRÈS SECRET de SÉCURITÉ NATIONALE avec Classification spéciale (précisez lesquelles) :
☐ SECRET de SÉCURITÉ NATIONALE

- *avoir pris connaissance de l'Arrêté Ministériel n° 2016-723 du 12 décembre 2016, portant application de l'article 18 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale et fixant les niveaux de classification des informations, modifié ;*
- *être pleinement conscient(e) de mes responsabilités en ce qui concerne la protection des informations et supports classifiés ;*
- *être informé(e) des conséquences prévues par les dispositions législatives (article 19 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale et fixant les niveaux de classification des informations, notamment pour le cas où, sciemment ou par négligence, je laisserais ces informations et supports classifiés parvenir à des personnes non qualifiées.*

En conséquence, **je m'engage à ne pas divulguer**, même après la cessation de mes fonctions ou de ma mission, à des personnes non qualifiées les informations et supports classifiés dont j'aurais eu connaissance dans l'exercice de mes fonctions ou l'accomplissement de ma mission.

A , le

Nom et signature de l'officier de sécurité Signature de l'intéressé(e)

VOLET 2

À compter de la date de cessation des fonctions ou de ma mission, pour lesquelles une décision d'habilitation à connaître d'informations et supports classifiés m'a été délivrée, **je m'engage à ne pas divulguer à des personnes non qualifiées** les informations et supports classifiés dont j'ai eu connaissance dans l'exercice de mes fonctions ou pendant l'accomplissement de ma mission et à **ne conserver par devers moi aucun support classifié**.

Je reconnais être informé(e) des **conséquences** prévues par les dispositions législatives (article 19 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale et fixant les niveaux de classification des informations) et réglementaires, notamment pour le cas où, sciemment ou par négligence, je porterais à la connaissance de personnes non qualifiées, ces informations et supports classifiés.

A , le

Nom et signature de l'officier de sécurité Signature de l'intéressé(e)

Appendice 8 – Modèle de décision de refus d'habilitation ou d'abrogation d'une décision d'habilitation

Département :

Organisme :

Date et numéro d'enregistrement :

DECISION DE REFUS D'HABILITATION OU D'ABROGATION D'UNE DECISION D'HABILITATION

☐ *Refus d'habilitation*

☐ *Abrogation de la décision d'habilitation*[20]

concernant

Madame/Monsieur[21]:

Date et lieu de naissance :

Grade ou titre :

Organisme :

Fonctions ou missions :

La présente décision est notifiée à l'intéressé(e) conformément à l'arrêté ministériel 2016-723 du 12 décembre 2016, portant application de l'article 18 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale et fixant les niveaux de classification des informations, modifié.

A

Le

Nom, qualité, signature de l'autorité d'habilitationet cachet de l'organisme

[20] Référence et date de la décision d'habilitation.
[21] Nom et prénom

Appendice 9 – Modèle de récépissé de notification d'une décision de refus d'habilitation ou d'abrogation d'une décision d'habilitation

Département :

Organisme :

Date et numéro d'enregistrement :

RECEPISSE DE NOTIFICATION D'UNE DECISION DE REFUS D'HABILITATION OU D'ABROGATION D'UNE DECISION D'HABILITATION

Je soussigné(e) :

reconnais que l'officier de sécurité de[22]:

m'a notifié et remis ce jour la décision[23]:

prise par[24]:

portant refus de délivrance ou d'abrogation de l'autorisation d'accéder aux informations et supportsclassifiés au(x) niveau(x) :

- ☐ TRÈS SECRET de SÉCURITÉ NATIONALE
- ☐ TRÈS SECRET de SÉCURITÉ NATIONALE avec Classification spéciale (précisez lesquelles) :
- ☐ SECRET de SÉCURITÉ NATIONALE

Je prends connaissance des voies et délais de recours relatifs à cette décision, indiqués ci-après.

En application de l'Ordonnance n° 2.984 du 16 avril 1963 sur l'organisation et le fonctionnement du Tribunal Suprême, modifiée, toute décision administrative peut faire l'objet, à peine d'irrecevabilité, dans un délai de deux mois, d'un recours contentieux devant le Tribunal Suprême.

Ce recours peut être précédé d'un recours administratif préalable, soit devant l'auteur de la décision - le recours est alors dit gracieux-, soit devant son supérieur - le recours est alors dit hiérarchique.

Il doit lui aussi, à peine d'irrecevabilité, être introduit dans le délai du recours contentieux (2 mois).

En cas de rejet ou de silence gardé par l'autorité saisie pendant quatre mois, le requérant dispose à nouveau du délai de deux mois du recours contentieux pour saisir le Tribunal Suprême.

A

Le

Signature de l'intéressé(e)

[22] Organisme.
[23] Référence et date de la décision
[24] Autorité d'habilitation ou autorité ayant reçu délégation à cet effet

Appendice 10 – Modèle de certificat de sécurité

Département :
Organisme :
Date et numéro d'enregistrement :

CERTIFICAT DE SÉCURITÉ

Attestation of personnel security clearance

Délivré par (Département, organisme) :
Issued by (Ministry, entity)

Date et lieu de délivrance :
Date and place of issue

Numéro:
Number

valable jusqu'au[25] :
valid until

Objet / mission :
Object/mission

Il est certifié par le présent document que Madame/Monsieur
It is hereby certified that Ms/Mr

Nom et prénom :
Family name, given name

Grade et fonctions :
Rank and functions

Date et lieu de naissance :
Date and place of birth

Détenteur(trice) du passeport / de la carte d'identité n° :
Passport/identity card number

Délivré à :
Place of issue

en date du :
date of issue

a fait l'objet de la décision d'habilitation n° :

has been granted the personnel security clearance n°

valable jusqu'au :

until

pour accéder à des informations et supports classifiés au niveau[26] **:**

for access to classified information up to the level

Nom, qualité, signature de l'autorité délivrant le certificat et cachet del'organisme

Fin de validité :

[25] Certificat à détruire à l'expiration de sa date de validité.
[26] Niveau de classification maximum (maximum level of classification)

Appendice 11 – Modèle d'attestation d'avis de sécurité

Département de l'Intérieur

Direction de la Sûreté Publique

Date et numéro d'enregistrement :

ATTESTATION D'AVIS DE SECURITE

Attestation of a positive clearance procedure

Délivré par (Département, organisme) :

Issued by (ministry, entity)

Date et lieu de délivrance :

Date and place of issue

Il est certifié par le présent document que Madame/Monsieur

It is hereby certified that Ms/Mr

Nom et prénom:
Family name, given name

Grade et fonctions :
Rank and functions

fait l'objet d'un avis de sécurité (sans objection, restrictif ou défavorable)[27] délivré par :

holds a security notice delivered by
valable jusqu'au :

expiring on DD/MM/AAAA

pour l'accès aux informations et supports classifiés au niveau[28]**:**

for access up to and including the level

Nom, qualité, signature de l'autorité d'habilitation
et cachet de l'organisme

[27] Rayer la mention inutile.
[28] Niveau de classification maximum (maximum level of classification

Appendice 12 – Récapitulatif des obligations des personnes morales ayant accès au secret de sécurité nationale

Obligations / Situation	Habilitation			Mise en place des chaînes de sécurité		Obtention d'une attestation d'aptitude physique à détenir des ISC		Homologation des systèmes d'information classifiés en cas de détention d'un tel système	Vecteur juridique de référence
	Personne morale	**Responsable de l'organisme ayant accès à des ISC[29]**	**Personnes physiques de l'organisme ayant accès à des ISC**	**ISC**	**Adaptation de la chaîne SSI[30]**	**Niveau *Secret***	**Niveau *Très secret***		
Services de l'État	Non	Oui, sauf si besoin d'en connaître non avéré	Toute personne de l'organisme nécessitant, dans les limites du besoin d'en connaître, d'accéder à des informations ou supports classifiés dans l'exercice de sa fonction ou pour l'accomplissement de sa mission, conformément au catalogue des emplois de l'organisme	Oui, même en l'absence de détention au sein de l'organisme	Si hébergement ou exploitation d'un système d'information classifié	Non	Oui, préalablement à la détention	Oui, préalablement au déploiement et à l'exploitation du système	Arrêté Ministériel n° 2016-723 du 12 décembre 2016 Le cas échéant, directives techniques particulières
Etablissements publics de l'État	Non	Oui, sauf si besoin d'en connaître non avéré				Oui, à l'occasion des contrôles organisés par l'officier de sécurité désigné par le DINT, la DSP ou l'AMSN	Oui, préalablement à la détention		
Opérateurs d'importance vitale	Non	Non, sauf si besoin d'en connaître avéré par le ministre coordonnateur	Officier de sécurité Toute autre personne nécessitant d'accéder pour la réalisation par l'opérateur de ses missions d'importance vitale et conformément au catalogue des emplois de l'opérateur	Oui, même en l'absence de détention au sein de l'organisme	Si hébergement ou exploitation d'un système d'information classifié	Oui, à l'occasion des contrôles organisés par l'officier de sécurité désigné par le DINT, la DSP ou l'AMSN	Oui, préalablement à la détention	Oui, préalablement au déploiement et à l'exploitation du système	Arrêté Ministériel n° 2020-902 du 21 décembre 2020 Plan particulier de protection

[29] Informations et supports classifiés
[30] Sécurité des systèmes d'information.

Obligations / Situation	Habilitation			Mise en place des chaînes de sécurité		Obtention d'une attestation d'aptitude physique à détenir des ISC		Homologation des systèmes d'information classifiés en cas de détention d'un tel système	Vecteur juridique de référence
	Personne morale	Responsable de l'organisme ayant accès à des ISC[152]	Personnes physiques de l'organisme ayant accès à des ISC	ISC	Adaptation de la chaîne SSI[153]	Niveau *Secret*	Niveau *Très secret*		
Convention au sens du présent arrêté	Non, sauf si la convention en stipule autrement	Oui	Tout personnel de la collectivité territoriale ou de la personne morale de droit privée ayant besoin d'accéder à des informations ou supports classifiés pour l'exécution de la convention inscrit au catalogue des emplois mentionné dans le plan contractuel de sécurité	Oui, même en l'absence de détention au sein de l'organisme	Si hébergement ou exploitation d'un système d'information classifié	Oui, au plus tard à l'occasion des contrôles organisés par l'officier de sécurité dont dépend le cocontractant	Oui, préalablement à la détention	Oui, préalablement au déploiement et à l'exploitation du système	Plan contractuel de sécurité
Contrat de la commande publique/ contrat de sous-traitance ou sous-contrat à un contrat de la commande publique / contrat de subvention	Oui, exigence préalable à la signature du contrat	Oui, exigence préalable à la signature du contrat	Tout personnel du cocontractant ayant besoin d'accéder à des informations ou supports classifiés pour l'exécution du contrat inscrit au catalogue des emplois mentionné dans le plan contractuel de sécurité			Oui, préalablement à l'exécution des prestations du contrat nécessitant la détention d'ISC par le cocontractant			Plan contractuel de sécurité

Appendice 13 – Clauses-types générales contractuelles de protection du secret de sécurité nationale à insérer dans les conventions et les contrats

Les présentes clauses sont insérées dans les conventions et les contrats en application de la présente annexe de l'arrêté à laquelle elle est rattachée. Elles peuvent être adaptées ou complétées par l'autorité contractante ou l'acheteur mais ne peuvent pas leur être contraires.

- *Clauses générales de protection du secret de sécurité nationale*

En application des dispositions législatives et réglementaires en matière de protection du secret de sécurité nationale, le titulaire de la convention ou du contrat s'engage à assurer la protection des informations et supports classifiés qu'il aura à connaître et, le cas échéant détenir, en tenant compte des dispositions particulières stipulées dans le plan contractuel de sécurité.

Il reconnaît avoir pris connaissance des textes suivants portant sur ses obligations résultant de la connaissance et de la détention d'informations et supports classifiés :

- *l'Arrêté Ministériel 2016-723 du 12 décembre 2016 portant application de l'article 18 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale et fixant les niveaux de classification des informations, modifié ;*
- *le cas échéant : [les directives techniques particulières [xxx]].*
- *Le cas échéant : [l'accord entre la Principauté de Monaco et la République française]*

Il déclare se soumettre aux obligations résultant pour lui de l'application de ces dispositions ainsi qu'à celles découlant de l'ensemble des textes législatifs et réglementaires relatifs à la protection du secret de sécurité nationale.

Toute violation ou inobservation par le titulaire des mesures de sécurité, même dans les cas où elles résultent d'une imprudence ou d'une négligence, peut entraîner l'abrogation de la décision d'habilitation au secret de sécurité nationale de la personne morale et, par voie de conséquence, la résiliation de la convention ou du contrat, sans préjudice des peines prévues par les dispositions de l'article 19 de la loi n° 1.430du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale

- *Stipulations additionnelles relatives aux conventions ou aux contrats nécessitant la détention d'informations et supports classifiés*

Les lieux du titulaire de la convention ou du contrat voués à abriter des informations et supports classifiés, ainsi que les systèmes d'information utilisés pour traiter des informations et supports classifiés doivent présenter toutes les garanties pour assurer la protection du secret de sécurité nationale et peuvent faire l'objet d'inspections, de contrôles ou d'audits de la part de l'autorité administrative.

Le titulaire s'engage à signaler toute modification susceptible de remettre en cause les garanties que présentent ses locaux ainsi que les systèmes d'information utilisés pour la protection des informations et supports classifiés communiqués au titre de la convention ou du contrat.

À l'achèvement des prestations du contrat nécessitant l'accès à des informations et supports classifiés, le titulaire dispose d'un délai d'un mois pour en informer l'autorité contractante qui détermine, dans la fiche de clôture du plan contractuel de sécurité, la destination à donner aux informations et supports classifiés jusqu'alors détenus par le titulaire ainsi que les conditions de démantèlement du système d'information classifié. Le titulaire s'engage à respecter ces dispositions. En cas d'inexécution, le titulaire s'expose à des sanctions pénales et contractuelles.

- *Stipulations additionnelles pour les contrats de recherche ou d'étude*

Le titulaire du contrat reconnaît à l'autorité contractante le pouvoir de faire rechercher, parmi les documents et matériels qui se trouveraient en sa possession, les informations et supports classifiés se rapportant au contrat et à faire apposer les scellés sur les meubles de sécurité et les locaux à l'intérieur desquels les documents et matériels réclamés par l'administration sont conservés en vue d'assurer leur protection.

Les informations et supports classifiés énumérés dans le plan contractuel de sécurité doivent être intégralement retournés à l'autorité contractante au terme du contrat.

Les locaux de travail du titulaire du contrat doivent présenter toutes les garanties pour assurer la protection du secret de sécurité nationale et peuvent faire l'objet d'inspections, de contrôles ou d'audits de la part de l'autorité administrative.

- *Stipulations relatives à la protection du secret dans le contrat de travail d'une personne habilitée*

En application des dispositions législatives et réglementaires en matière de protection du secret de sécurité nationale, le titulaire du contrat de travail s'engage à respecter les mesures qui lui sont prescrites pour assurer, lors de l'exécution dudit contrat, la protection des informations et supports classifiés qu'il peut, sous réserve du besoin d'en connaître, être amené à connaître ou détenir, au titre de la décision d'habilitation délivrée par l'autorité administrative compétente.

Il reconnaît avoir pris connaissance de l'article 19 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale et fixant les niveaux de classification des informations et de l'Arrêté Ministériel n° 2016-723 du 12 décembre 2016 portant application de l'article 18 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale et fixant les niveaux de classification des informations, modifié.

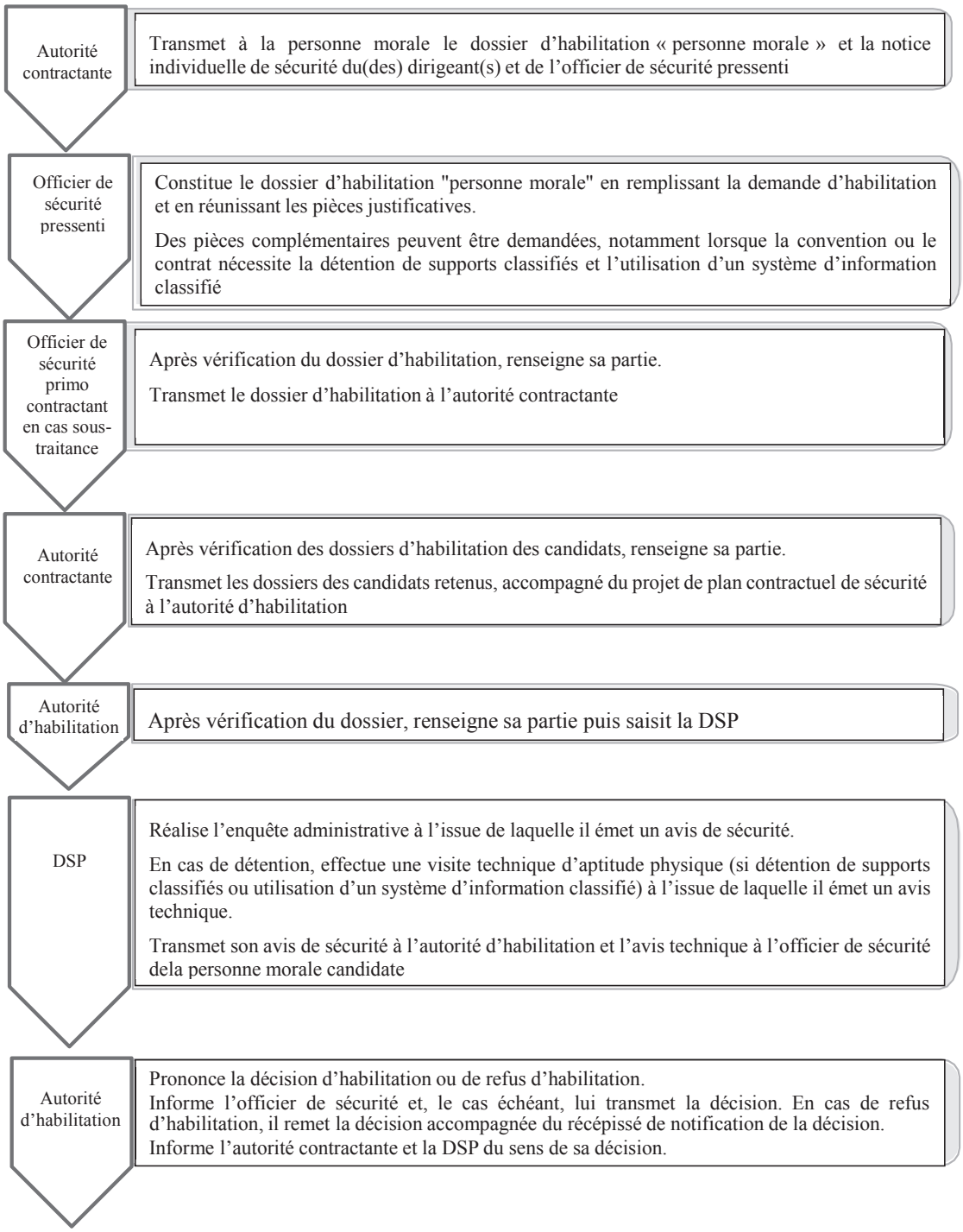
- *Stipulations relatives à la protection du secret dans le contrat de travail d'une personne non habilitée*

En application des dispositions législatives et réglementaires en matière de protection du secret de sécurité nationale, le titulaire du contrat de travail s'engage à respecter les mesures qui lui sont prescrites pour assurer, lors de l'exécution du contrat, la protection des informations et supports classifiés qui peuvent être détenus dans le service au profit duquel le contrat est exécuté ou dans tout lieu dans lequel ce contrat est exécuté. Le titulaire est informé qu'il n'est pas autorisé à connaître d'informations et supports couverts parle secret de sécurité nationale.

- *Stipulations relatives à la protection du secret en cas de disparition de la personne morale*

En cas de cessation d'activité ou de dissolution, le titulaire du contrat [restitue/détruit/archive] les informations et supports classifiés qu'il détient au titre du contrat selon les modalités suivantes : [modalités à définir par l'autorité publique contractante].

Appendice 14 – Schéma présentant la procédure d'habilitation d'une personne morale



Appendice 15 – Modèle de désignation d'un officier de sécurité

Je soussigné(e)[31]:

désigne[32]:

pour exercer la fonction d'officier de sécurité de[33]:

Adresse de la personne morale :

Le cas échéant, n° RCI :

chargé, sous ma responsabilité, de mettre en œuvre les dispositions législatives et réglementaires en matière de protection du secret de sécurité nationale pour assurer la protection des informations et supports classifiés confiés dans le cadre d'une convention/d'un contrat. Je m'engage à lui donner les moyens nécessaires pour accomplir les missions qui lui sont confiées, qu'il exerce pour mon compte et sous ma responsabilité.

A
Le
Signature

[31] Nom, prénom du représentant légal de la personne morale.
[32] Nom, prénom de l'officier de sécurité
[33] Raison ou dénomination sociale de la personne morale

Appendice 16 – Modèle de dossier de demande d'habilitation d'une personne morale

1- À remplir par la personne morale	
Dénomination ou raison sociale (*en lettres majuscules, sans acronyme*) : N° RCI :	Date et signature du représentant de la personne morale
Procédure d'habilitation engagée :	☐ ADMISSION ☐ RENOUVELLEMENT ☐ RÉVISION

2- À remplir par l'autorité contractante/le maître d'œuvre/l'acheteur/le primo-contractant (dans le cas d'une sous-traitance/d'un sous-contrat)	
Niveau d'habilitation demandé :	☐ TRÈS SECRET DE SECURITE NATIONALE ☐ TRÈS SECRET DE SECURITE NATIONALE, le cas échéant, préciser la classificationspéciale : ☐ SECRET DE SECURITE NATIONALE
Nature des informations et supports classifiés	☐ France ☐ MONACO ☐ Autres, préciser :
Modalités d'accès et production d'informations et supports classifiés	
Objet du contrat : Motif du besoin d'en connaître :	
Accès à des informations et supports classifiés en phase précontractuelle	☐ OUI ☐ NON
Accès sans détention d'informations et supports classifiés	☐ OUI ☐ NON
Accès avec détention d'informations et supports classifiés dans les locaux de la personne morale	☐ OUI ☐ NON
Le cas échéant, préciser le(s) lieu(x) :	
Utilisation d'un système d'information classifié :	☐ OUI ☐ NON

Renseignements relatifs au contrat[34]
1. Description de la prestation confiée à la personne morale : 2. Lieux d'exécution du contrat :
3. Date prévisionnelle de notification du contrat : 4. Date et durée d'exécution du contrat : 5. En cas de sous-traitance/sous-contrat, préciser : dénomination ou raison sociale du contractant : N° d'identification et date de notification : N° d'identification et date d'approbation du plan contractuel de sécurité : 6. Conséquences (opérationnelles, calendaires, financières, techniques, etc.) si l'entreprise : - n'est pas habilitée à la date prévisionnelle indiquée au point 5 : - ne peut pas être habilitée :
Nom de l'autorité contractante/acheteur : Date et signature Nom, prénom et coordonnées de la personne en charge du dossier :

3- À remplir par l'autorité d'habilitation
Département : Date et signature N° de la demande d'habilitation : Nom, prénom et coordonnées de la personne en charge du dossier :

[34] Ne concerne que les contrats prévoyant les prestations suivantes : travaux, fournitures, services

Notice de sécurité personne morale[35]

À renseigner intégralement en utilisant, si nécessaire, l'espace « renseignements complémentaires »

Représentant de la personne morale		
Nom - prénom :		
Date et lieu de naissance :		
Fonction :		
Tél. bureau :	Tél. portable :	Fax :
Email :		
Officier de sécurité *(à remplir s'il est différent du représentant de la personne morale)*		
Nom - prénom :		
Fonction :		
Tél. bureau :	Tél. portable :	Fax :
Email :		

Habilitation déjà détenue par la personne morale	☐ Cocher si sans objet
La personne morale a-t-elle déjà été habilitée au secret de sécurité nationale ? Si oui, préciser : - l'autorité d'habilitation : - la date de la décision d'habilitation : - la date de fin de validité de l'avis de sécurité : - le niveau d'habilitation : - la nature de l'habilitation (France, Monaco, autres) :	☐ OUI ☐ NON
La personne morale dispose-t-elle d'un local apte à conserver des informations et supports classifiés ? Si oui, préciser : - l'emplacement et le numéro du local : - l'autorité ayant délivré l'avis technique d'aptitude physique : - la date de délivrance de cet avis : - le niveau de classification des supports pouvant être conservés dans le local :	☐ OUI ☐ NON
La personne morale dispose-t-elle d'un système d'information homologué pour traiter des informations classifiées ? Si oui, préciser : - l'autorité ayant délivré la décision d'homologation : - la date de délivrance de la décision d'homologation : - le niveau de classification des informations pouvant être traitées sur le système d'information :	☐ OUI ☐ NON

Informations relatives à la personne morale *(dans le cadre d'un contrat de la commande publique, d'un contrat de sous-traitance ou de sous-contrat à un contrat de la commande publique, d'un contrat de subvention)*

[35] À renseigner également par les indépendants, les microentreprises

La personne morale détient-elle l'exclusivité du savoir-faire pour les travaux classifiés ? ☐ Oui, décrire le savoir-faire : ☐ Non. Si une autre entreprise détient ce savoir-faire, expliquer la raison pour laquelle elle n'a pas été retenue ou pas consultée ?

Capital social *(dans le cadre d'un contrat de la commande publique, d'un contrat de sous-traitance ou de sous-contrat à un contrat de la commande publique, d'un contrat de subvention).* **Pour les entreprises non cotées, fournir l'actionnariat détaillé**					
1er niveau					
Nom (et prénom) du ou des actionnaires	Nationalité(s)	Date et lieu de naissance des personnes physiques	N° RCI pour les personnes morales (Extrait à fournir)	% détenu	Droit de vote (%)
2e niveau d'actionnariat pour tout actionnaire détenant 40 % et plus des parts sociales du 1er niveau					
Nom (et prénom) du ou des actionnaires	Nationalité(s)	Date et lieu de naissance	N° RCI pour les personnes morales (Extrait à fournir)	% détenu	Droit de vote (%)
3e niveau d'actionnariat pour tout actionnaire détenant 40 % et plus des parts sociales du 2e niveau					
Nom (et prénom) du ou des actionnaires	Nationalité(s)	Date et lieu de naissance	N° RCI pour les personnes morales (Extrait à fournir)	% détenu	Droit de vote (%)

Liste des pièces requises pour le dossier d'habilitation « personne morale »

- *Par la personne morale, en complément de la notice de sécurité :*
- *Demande d'habilitation de la personne morale*
- *Demande d'habilitation de chaque dirigeant de droit de la personne morale*
- *Demande d'habilitation de l'officier de sécurité de la personne morale pressenti, candidat à l'habilitation, et lettre de désignation*
- *Extrait du registre du commerce complet récent*
- *Extrait du registre du commerce complet récent des personnes morales détenant la majorité du capital social*
- *Extrait en cours de validité du répertoire du commerce et de l'industrie ou copie du bail de location*
- *Statuts à jour*
- *Composition du conseil d'administration et des organes de gouvernance (conseil desurveillance, directoire, etc.)*
- *Liste des autres conseils d'administration au sein desquels les représentants de la personne morale siègeraient*
- *Organigramme positionnant la société dans le groupe*
- *Organigramme fonctionnel de la personne morale (y compris les membres n'ayant pas le pouvoir d'engager la société) pour le siège social*
- *Organigramme fonctionnel et nominatif de l'établissement*
- *Plaquette de présentation de l'entreprise*
- *Liste des dettes principales par origine (prêts des établissements bancaires, etc.)*
- *Dernier bilan*
- *Liste des sous-traitants ou sous-contractants intervenant dans l'établissement, en identifiant les prestataires de services au titre d'un contrat sensible*

Si la personne morale a déjà été habilitée :

- *Attestation d'habilitation de l'autorité d'habilitation ou attestation d'avis de sécurité en cas de changement d'autorité d'habilitation*
- *Attestation de non-changement (fait et droit) de la personne morale depuis la dernièrehabilitation*

Si le présent contrat/convention prévoit la détention d'informations et supports classifiés :

- *Copie de l'avis technique d'aptitude physique de la DSP*
- *Attestation de conformité physique*
- *Identification et description de la protection, actuelle et envisagée, du local dans lequel estenvisagé la conservation des informations et supports classifiés*
- *Plan de masse de l'établissement*
- *Organisation et moyens de protection et de gardiennage de l'établissement*
- *En cas d'avis technique avec réserve ou défavorable, lettre du dirigeant de la personne morale par laquelle celui-ci s'engage à mettre en place, avant le début de l'exécution des prestations du contrat nécessitant l'accès à des informations et des supports classifiés, les dispositions nécessaires à la protection des informations et supports classifiés qui lui seront confiés*

Si le présent contrat/convention prévoit l'utilisation d'un système d'information classifié :

- *Copie de la décision d'homologation*
- *Dossier de sécurité du système d'information*

À transmettre par l'autorité contractante ou l'acheteur :

- *Plan contractuel de sécurité ou projet*

Appendice 17 – Modèle d'attestation d'avis de sécurité d'une personne morale

Département de l'Intérieur :

Direction de la Sûreté Publique :

Date et numéro d'enregistrement :

ATTESTATION D'AVIS DE SECURITE D'UNE PERSONNE MORALE

Attestation of a positive facility clearance procedure

Délivré par le Directeur de la Sûreté Publique

Issued by

Date et lieu de délivrance :

Date and place of issue

Il est certifié, par le présent document, que la personne morale

It is hereby certified that the company

Dénomination ou raison sociale :

Full company name

fait l'objet d'un avis de sécurité (sans objection, restrictif ou défavorable)[36] délivré par :

hold a security notice delivered by

valable jusqu'au :

expiring on DD/MM/AAAA

pour l'accès aux informations et supports classifiés au niveau[37] :

for access up to and including the level

Nom, qualité, signature de l'autorité d'habilitationet cachet de l'organisme

[36] Rayer la mention inutile.

[37] Niveau de classification maximum (maximum level of classification)

Appendice 18 – Modèle d'attestation d'habilitation d'une personne morale

Département :

Organisme :

Date et numéro d'enregistrement :

ATTESTATION D'HABILITATION D'UNE PERSONNE MORALE

Attestation of facility security clearance decision

Délivré par (Département, organisme) :

Issued by (ministry, entity)

Date et lieu de délivrance :

Date and place

Il est certifié par le présent document que la personne morale

It is hereby certified that the company

Dénomination ou raison sociale :

Full facility name

fait l'objet d'une décision d'habilitation délivrée par :

hold a facility security clearance decision delivered by

valable jusqu'au :

expiring on DD/MM/AAAA

pour l'accès aux informations et supports classifiés au niveau[38] **:**

for access up to and including the level

Nom, qualité, signature de l'autorité compétenteet cachet de l'organisme

[38] Niveau de classification maximum

Appendice 19 – Modèle de décision d'habilitation d'une personne morale

Département :

Organisme :

Date et numéro d'enregistrement :

DECISION D'HABILITATION D'UNE PERSONNE MORALE

Le[39] :
décide que

Dénomination ou raison sociale :

Adresse :

N° RCI :

est habilitée jusqu'au[40]**:**

pour accéder à des informations et supports classifiés au(x) niveau(x) :

- ☐ TRÈS SECRET DE SECURITE NATIONALE
- ☐ TRÈS SECRET DE SECURITE NATIONALE, avec classification spéciale (à préciser)
- ☐ SECRET DE SECURITE NATIONALE

dans le domaine suivant[41] **:**

A

Le

Signature et cachet de l'autorité d'habilitation

[39] Autorité d'habilitation ou autorité ayant reçu délégation à cet effet.
[40] Date d'expiration de la décision.
[41] Préciser le domaine en cas de limitation du champ de l'habilitation

Appendice 20 – Modèle de décision de refus d'habilitation ou d'abrogation d'une décision d'habilitation d'une personne morale

Département :

Organisme :

Date et numéro d'enregistrement :

DECISION DE REFUS D'HABILITATION OU D'ABROGATION D'UNE DECISION D'HABILITATION D'UNE PERSONNE MORALE

- *Refus d'habilitation*
- *Abrogation de la décision d'habilitation*[42]*:*

concernant

Dénomination ou raison sociale :

Adresse :

N° RCI :

La présente décision sera notifiée au représentant légal de la personne morale conformément à l'arrêté ministériel n° 2016-723 du 12/12/2016 portant application de l'article 18 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale et fixant les niveaux de classification des informations, modifié.

À

Le

Nom, qualité, signature de l'autorité compétente[43]et cachet de l'organisme

[42] Référence et date de la décision d'habilitation.
[43] Autorité de décision ayant reçu délégation à cet effet

Appendice 21 – Modèle de récépissé de notification d'une décision de refus d'habilitation ou d'abrogation d'une décision d'habilitation d'une personne morale

Département :

Organisme :

Date et numéro d'enregistrement :

RECEPISSE DE NOTIFICATION D'UNE DECISION DE REFUS D'HABILITATION OU D'ABROGATION D'UNE DECISION D'HABILITATION D'UNE PERSONNE MORALE

Je soussigné(e)[44]:

reconnais que l'autorité suivante[45] :

m'a notifié et remis ce jour la décision[46]:

prise par[47]:
portant refus de délivrance ou d'abrogation de l'autorisation d'accéder aux informations et supports classifiés au(x) niveau(x) :

- ☐ TRÈS SECRET DE SECURITE NATIONALE
- ☐ TRÈS SECRET DE SECURITE NATIONALE, avec classification spéciale (à préciser)
- ☐ SECRET DE SECURITE NATIONALE SECRET

Je prends connaissance des voies et délais de recours relatifs à cette décision, indiqués ci-après :

En application de l'Ordonnance n° 2.984 du 16 avril 1963 sur l'organisation et le fonctionnement du Tribunal Suprême, modifiée, toute décision administrative peut faire l'objet, à peine d'irrecevabilité, dans un délai de deux mois, d'un recours contentieux devant le Tribunal Suprême.

Ce recours peut être précédé d'un recours administratif préalable, soit devant l'auteur de la décision - le recours est alors dit gracieux-, soit devant son supérieur - le recours est alors dit hiérarchique.

Il doit lui aussi, à peine d'irrecevabilité, être introduit dans le délai du recours contentieux (2 mois).

En cas de rejet ou de silence gardé par l'autorité saisie pendant quatre mois, le requérant dispose à nouveau du délai de deux mois du recours contentieux pour saisir le Tribunal Suprême.

A

[44] Nom, prénom du responsable de la personne morale.
[45] Dénomination de l'autorité d'habilitation ou de l'autorité administrative compétente
[46] Référence et date de la décision
[47] Autorité d'habilitation ou autorité ayant reçu délégation à cet effet.

Le
Signature

Appendice 22 – Modèle d'attestation de conformité physique

Organisme :

Date et numéro d'enregistrement :

ATTESTATION DE CONFORMITE PHYSIQUE

Je soussigné(e)[48] :

atteste que les lieux où seront reçus, manipulés, élaborés, conservés et émis des informations et supports classifiés au sein de mon organisme[49]pour les établissements ci-dessous mentionnés :

au titre de la convention/du contrat :

bénéficient des conditions de protection prévues par la réglementation en vigueur.

La vérification de ces lieux a été effectuée le :

par la Direction de la Sûreté Publique :

et a donné lieu à un avis technique d'aptitude physique[50]:

A

Le

Signature

[48] Nom, prénom, qualité du responsable de la personne morale.
[49] Dénomination ou raison sociale
[50] Date et référence de l'avis technique d'aptitude physique

Appendice 23 – Modèle de certificat de mise aux normes de sécurité physique

Organisme :

Date et numéro d'enregistrement :

CERTIFICAT DE MISE AUX NORMES DE SECURITE PHYSIQUE

Je soussigné(e)[51]:

certifie que les locaux où seront reçus, manipulés, élaborés, conservés et émis des informations et supports classifiés au sein de mon organisme[52]

pour les établissements ci-dessous mentionnés :

au titre de la convention/du contrat :

à la suite de la vérification de ces locaux effectuée le :

par la Direction de la Sûreté Publique et ayant donné lieu à l'avis technique[53]:

ont fait l'objet de travaux de mise en conformité et bénéficient des conditions de protection prévues par la réglementation en vigueur.

A

Le

Signature

[51] Nom, prénom, qualité du responsable de la personne morale

[52] Dénomination ou raison sociale.

[53] Date et référence de l'avis technique

Appendice 24 – Prescriptions relatives aux plans contractuels de sécurité, aux plans de sécurité d'opérateurs et aux plans particuliers de protection

Ces plans comportent notamment les éléments suivants :

- *l'engagement pris par le contractant ou l'opérateur d'importance vitale de s'assurer que les personnes qui ont besoin d'accéder à des informations et supports classifiés dans l'exercice de leurs fonctions ou l'accomplissement d'une mission ont fait l'objet d'une décision d'habilitation au niveau requis ;*
- *l'engagement pris par le contractant ou l'opérateur d'importance vitale de s'assurer que toutes les personnes qui ont accès à des informations et supports classifiés sont informées de leur responsabilité en matière de protection desdits informations et supports en vertu des lois et règlements appropriés ;*
- *l'engagement de signaler toute infraction effective ou supposée aux lois et règlements afférents à la protection des informations et supports classifiés couverts par la convention, le contrat ou l'activité d'importance vitale ;*
- *l'identification des personnes parties à la chaîne de sécurité et chargées de coordonner la protection des informations et supports classifiés couverts par la convention, le contrat ou l'activité d'importance vitale, en particulier, l'officier de sécurité et le cas échéant, toute autre personne exerçant une fonction en lien avec la protection du secret ;*
- *les locaux dans lesquels la convention ou le contrat doit être exécuté et les informations et supports classifiés abrités et conservés ; la liste de ces locaux peut évoluer ;*
- *les systèmes d'information utilisés pour l'exécution de la convention ou du contrat ou l'activité d'importance vitale, dont la liste peut évoluer ;*
- *la liste des informations et supports classifiés et pouvant être générés, leurs niveaux respectifs de classification (guide de classification) et les modalités de déclassification ou déclassement ainsi que les conditions de protection dont chaque information ou support doit faire l'objet, conformément aux dispositions de l'arrêté ministériel auquel est rattaché la présente annexe, et aux textes réglementaires qui la déclinent, ainsi que leurs modalités d'archivage et de destruction ;*
- *les mesures particulières de sécurité qui doivent être prises pour l'exécution de ce contrat en vue de garantir la protection des informations et supports classifiés ;*
- *les modes de diffusion, y compris par voie dématérialisée, des informations et supports classifiés ;*
- *la liste des sous-contractants et sous-traitants identifiés lors de la rédaction du plan contractuel de sécurité et devant être mise à jour ;*
- *les modalités de diffusion des informations et supports classifiés aux sous-contractants et sous-traitants ;*
- *les modalités de gestion prévisionnelle des informations et supports classifiés et des systèmes d'information classifiés à la fin de la convention ou du contrat ou de la caducité du plan de sécurité opérateur ou du plan particulier de protection ;*
- *les modalités de destruction, d'archivage ou de restitution des informations et supports classifiés détenus par le contractant et, le cas échéant, ses sous-contractants et sous-traitants participant à l'exécution du contrat, en cas de cessation d'activité ou de dissolution du contractant ou, le cas échéant, de l'un de ses sous-contractants et sous-traitants participant à l'exécution du contrat.*

Un exemplaire du plan contractuel de sécurité est transmis à la Direction de la Sûreté Publique chargée du suivi de la personne morale par l'autorité contractante ou l'acheteur.

Pour les titulaires d'une convention ou d'un contrat, ces éléments sont complémentaires des clauses-types générales (cf. Appendice 13).

Appendice 25 – Types de mesures de protection physique

L'ensemble des mesures de protection se compose de quatre éléments combinés ou dissociés en fonction du niveau de classification :

- *un ou plusieurs dispositifs de dissuasion (indications) ;*
- *un ou plusieurs dispositifs de détection et d'alarme ;*
- *un ou plusieurs dispositifs de freinage (les obstacles) ;*
- *des moyens d'intervention articulés sur des procédures et des consignes préétablies.*

Ainsi, selon une logique de défense en profondeur, un dispositif de sécurité satisfaisant a pour objectif, en retardant l'intrusion (aucun obstacle n'étant infranchissable), de permettre la mise en œuvre des moyens d'intervention, alertés et guidés par les dispositifs de détection avant que les informations ou supports classifiés ne soient compromis.

Pour être efficace, un système de protection physique doit s'appuyer sur une analyse de risques et :

- *être multifonctions, c'est-à-dire comporter plusieurs dispositifs successifs, complémentaires, de nature différente, associés ou combinés à un ou plusieurs dispositifs de détection-alarme reposant eux-mêmes sur des principes différents ;*
- *être homogène, c'est-à-dire garantir la même efficacité en tous points, l'intrusion s'opérant toujours dans la zone de moindre résistance et la valeur d'un système équivalant à celle de son élément le plus faible ;*
- *être dissuasif, c'est-à-dire contribuer à réduire le risque d'une tentative d'intrusion ;*
- *être contrôlé, c'est-à-dire être testé fréquemment afin de vérifier qu'il est en état opérationnel ;*
- *être traçable, c'est-à-dire fournir tout moyen pouvant apporter un historique du fonctionnement des différents composants.*

Afin d'éviter l'intrusion, à l'intérieur d'un site ou d'un local protégé, d'une personne non autorisée qui représente toujours une menace pour les informations et supports classifiés détenus, la protection physique comprend nécessairement un système d'information de sûreté dont la composante « contrôle d'accès » est décrite en Appendice 27.

Appendice 26 – Barrières de protection physique et logique, répartition en classes et tableaux de combinaison des classes

Principes généraux à appliquer en matière de protection

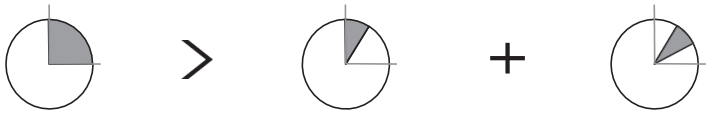
La protection des informations et supports classifiés s'obtient par une combinaison globale de moyens techniques, humains et organisationnels ainsi que, pour les systèmes d'information (SI), logiques.

Les moyens physiques doivent répondre au besoin de détecter et freiner l'intrusion de façon à permettre l'intervention. Ils doivent, en outre, permettre d'assurer la traçabilité en cas d'effraction. Ils s'inscrivent dans la profondeur en étageant différentes couches de protection, appelées également barrières (périphériques, périmétriques et intérieures), qui s'appuient essentiellement sur :

- *l'emprise et/ou le bâtiment ;*
- *le local (ou un groupe de locaux regroupés en zone) ;*
- *le meuble ;*
- *le système d'information (au niveau du poste utilisateur) contenant les informations et supports classifiés.*

Le choix du dispositif global de protection par le responsable d'organisme, sur les conseils de l'officier de sécurité, doit être conforme aux exigences fixées par l'équation de protection, définie comme suit (T pour « temps ») :

T freinage > T de détection et de traitement de l'alarme + T intervention



Le temps de freinage équivaut au temps mis par l'intrus pour franchir les différentes barrières de protection placées entre la détection et les actifs ou la zone à protéger. Il est matérialisé par la présence de moyens de freinage en nombre et en nature suffisants.

Le temps de détection et de traitement de l'alarme correspond au délai existant entre l'alarme par le premier moyen de détection d'intrusion et le déclenchement effectif de l'intervention par le poste chargé de traiter l'alarme. À titre d'exemple :

- *dans le cas d'une alarme fondée sur une détection électronique :*
- *T détection et de traitement de l'alarme = 0 + validation de l'information (levée de doute effectuée) + délais de transmission et prise en compte effective par le poste pouvant exécuter l'intervention immédiatement, 24h/24 et 7j/7 ;*
- *dans le cas de rondes en l'absence d'alarme ou de surveillance à distance :*

  T détection et detraitement de l'alarme = intervalle entre les rondes + validation de l'information (levée de doute effectuée) + délais de transmission et de prise en compte effective par le poste pouvant exécuter l'intervention immédiatement, 24h/24 et 7j/7.

Le temps d'intervention est le temps mis par l'élément chargé de l'intervention (interne ou externe) ou les forces de sécurité intérieures pour se trouver au cœur de la zone d'action. Dans le cas d'un élément d'intervention externe ou d'une force de sécurité intérieure, le temps d'intervention tient compte de la distance, du temps moyen constaté pour la parcourir et de la disponibilité moyenne de l'élément d'intervention. En cas de doute, le temps majorant est retenu.

Il convient de s'assurer que la somme des délais de freinage, depuis la première barrière (l'extérieur du bâtiment ou de l'emprise) jusqu'aux informations et supports classifiés, est supérieure au temps cumulé nécessaire à l'intervention.

Détermination des classes

Chaque barrière est répartie en plusieurs classes (de la moins sécurisée à la plus sécurisée). Chacune de ces classes correspond aux moyens techniques, humains et organisationnels mis en œuvre pour assurer un niveau de protection au moins égal à celui décrit ci-après.

Classes du bâtiment et/ou de l'emprise ou du site

CLASSE	DESCRIPTION
4	Emprise (ou site) dont le périmètre est délimité physiquement, dotée d'un contrôle d'accès conforme à l'Annexe 27, d'une protection mécanique (clôture dont le franchissement n'est pas possible sans facilitateur[54])et dont tous les points d'accès sont équipés d'une serrure mécanique fonctionnelle. ou Bâtiment doté d'un contrôle d'accès conforme à l'Annexe 27, dont les ouvrants proches d'un point d'accès sont, dans la mesure du possible rendus discrets (film opacifiant) et systématiquement dotés d'une protection mécanique (limiteur d'ouverture, barreaux, etc.) et dont tous les points d'accès sont équipés d'une serrure mécanique fonctionnelle.
3	Enceinte de classe 4 : + contrôle d'accès par identification en périmétrie pour les flux piétons et véhicules, + personnel de surveillance[55] présent en permanence, effectuant des rondes dans l'enceinte et ses sous-ensembles, + élément d'intervention extérieur mobilisable sur alarme du personnel desurveillance ; ou Enceinte de classe 4 : + contrôle d'accès par identification en périmétrie pour les flux piétons et véhicules ; + moyen de détection d'ouverture sur les ouvrants accessibles et les points d'accès reliés à une centrale d'intrusion + système de vidéosurveillance/détection sur les zones sensibles pour la levée de doute. Ces dispositifs techniques de détection-alarme sont reliés à un élément d'intervention extérieur.
2	Enceinte de classe 3 : + présence de personnel de surveillance effectuant des rondes dans l'enceinte et sessous-ensembles ; + ensemble de télé-sécurité (télésurveillance + intervention) ; + dispositifs techniques de détection-alarme ; + moyen de détection volumétrique sur les lieux de passage permettant d'accéder auxlieux abritant des informations et supports classifiés ; + traçabilité des entrées et sorties au niveau du bâtiment hébergeant les lieux abritant des informations et supports classifiés.
1	Enceinte de classe 2 : + dispositifs de détection-alarme placés sur tous les points d'accès de l'ensemble deslocaux ; + présence d'un système de vidéosurveillance sur les accès aux lieux abritant lesinformations et supports classifiés ; + moyen de détection d'intrusion placé au point d'accès de tous lieux abritant des informations et supports classifiés ; + présence permanente sur site d'un élément humain d'intervention.

[54] Pierre servant de marchepieds, perche, canne, escalade, etc.
[55] Par exemple, agent privé de sécurité, gardien-veilleur, garde

Classes du local

Si l'emprise ne présente pas de dispositif de détection-alarme, un dispositif de ce type doit être installé au niveau du local.

Les parois (plafonds, sols et murs) des locaux ainsi que les ouvrants (portes, fenêtres, etc.)[56], leurs serrures et leurs sûretés doivent présenter une résistance mécanique suffisante et homogène pour retarder l'intrusion et permettre la mise en œuvre des moyens d'intervention.

Toutes les serrures des portes des locaux sont équipées de sûretés à clés mécaniques, comme dispositif principal ou comme moyen de secours de dispositifs électroniques.

Les fabricants de sûreté à clef justifient que leurs produits possèdent :

- *une technologie qui s'oppose aux techniques d'ouverture à l'aide d'outils manuels ;*
- *une conception qui complique l'usage de moyens d'ouverture fine (outils spécifiques dit « de crochetage »).*

La fourniture et la reproduction de la clef ne doivent être possibles qu'après l'authentification d'une personne désignée auprès du fournisseur. La présence d'une carte dite de propriété ne peut pas, à elle seule, suffire comme moyen de protection contre la copie.

CLASSE	DESCRIPTION
d	Local avec bloc-porte à serrure mono-point et baies fermées (fenêtres, évacuateur de fumées, bloc d'un climatiseur, etc.).
c	Local avec : - bloc-porte (métallique ou en bois plein ou matériau équivalent) à serrure mécanique multipoints ; - sûreté à clef présentant un temps de résistance de 5 minutes au moins ; - contrôle d'accès par identification ; - fenêtres protégées lorsqu'elles sont accessibles (depuis le sol, toit, corniche, descente d'eau pluviale, promontoire, etc.). À l'intérieur des lieux abritant des informations et supports classifiés : - moyen de détection volumétrique double technologie relié à une centrale d'intrusion ; - ou moyen de détection d'intrusion sur les ouvrants et serrure mécanique de fermeture sur les points d'accès (bloc-portes, baies, etc.).

[56] Les dispositifs électromécaniques ou électromagnétiques de fermeture des ouvrants ne peuvent pas à eux seuls garantir l'intégrité des accès aux bâtiments ou aux emprises. Ils doivent obligatoirement être complétés par des systèmes mécaniques de verrouillage mis en service en dehors des périodes d'occupation des bâtiments

b	Local avec : - bloc-porte renforcé équipé d'un système anti-dégondage, à serrure mécanique multipoints avec détecteur ; - sûreté à clef présentant un temps de résistance de 15 minutes au moins ; - fenêtres protégées lorsqu'elles sont accessibles (depuis le sol, toit, corniche, descente d'eau pluviale, promontoire, etc.) ; - contrôle d'accès par authentification avec traçabilité des entrées et sorties. À l'intérieur des lieux abritant les informations et supports classifiés : - moyen de détection intrusion sur les ouvrants et serrure mécanique de fermeture sur les points d'accès (bloc-portes, baies, etc.) ; - moyen de détection volumétrique double technologie relié à une centrale d'intrusion ; - système permettant la levée de doute en dehors des heures de service (vidéosurveillance par ex.).
a	Chambre forte dont le bloc-porte est au minimum équipé des systèmes de sécurité des armoires fortes de classe B.

Classes du meuble

Les meubles de sécurité destinés à la conservation des informations et supports classifiés ne peuvent pas êtreouverts frauduleusement sans effraction : toute tentative d'ouverture illégitime laisse des traces visibles détectables par l'utilisateur. Ils sont dotés par défaut de serrure à combinaison mécanique conforme à la norme EN1300 niveau B minimum.

Les meubles prévus pour protéger des équipements électroniques en fonctionnement sont naturellement pourvus d'ouïes de ventilation. En raison de l'accès visuel sur le contenu offert par leur présence, ces meubles ne doivent pas contenir de supports à lecture directe.

CLASSE	DESCRIPTION
C	Armoire forte à structure métallique d'au moins 2 millimètres d'épaisseur, munie d'une serrure mécanique à combinaison silencieuse et à manœuvre discrète. Les battants possèdent un système d'accrochage du côté du pivot interdisant le démontage des portes en cas de sectionnement des gonds, lorsque le meuble est condamné. Les pênes, inaccessibles de l'extérieur, ne doivent pas pouvoir être démontés.
B	Armoire forte de structure identique à la classe C : + renforcement de la structure de la zone située entre la face avant de la porte et les organes essentiels dont la présence peut être vérifiée visuellement par démontage du foncet de porte (face intérieure de la porte) ; + dispositif délateur, à déclenchement mécanique et thermique, bloquantdéfinitivement les mécanismes d'ouverture en cas de tentative d'ouverture illégitime ; + plombage du foncet de porte (face intérieure de la porte) permettant de détecter aisément un démontage ; + système à clef interdisant l'accès au dispositif de changement de la combinaison pour les modèles mécaniques ; + système d'asservissement, interdisant la sortie des pênes de la porte principale lorsque l'autre battant n'est pas fermé, s'il ne s'agit pas d'un meuble à porteunique ; + dispositif qui interdise aux pênes de la porte principale, une fois sortis, de se rétracter à moins que la combinaison soit à nouveau composée ; + compteur d'ouverture non falsifiable et non réutilisable, sans dispositif de remise à zéro et protégé par le foncet ; + une serrure mécanique à combinaison silencieuse et à manœuvre discrète est à recommander. L'emploi d'une serrure électronique, conforme à la norme EN1300 niveau B au minimum, disposant d'un dispositif de composition discret et assurant la traçabilité des combinaisons, peut être autorisé s'il est justifié. Le meuble équipé d'une combinaison électronique comporte une serrure mécanique à clef facilement permutable en supplément. Cette clef est prisonnière de la serrure tant que le pêne de la combinaison et les pênes du meuble ne sont pas sortis portes fermées ; + système de tringlerie métallique en acier assurant sur la porte principale une répartition géographique de plusieurs pênes horizontaux et verticaux. Si une poignée actionne ce système, elle possède un point de rupture pour éviter un effort trop conséquent sur la tringlerie. Les portes sont dépourvues de toute plaque de propreté et de tout enjoliveur.
A	Coffre-fort blindé sur toutes ses faces, d'un poids minimum à vide de 500 kg ou, à défaut, fixé au mur, au sol ou sur une plaque métallique dont la plus petite dimension est supérieure à la plus grande dimension des issues du local. Ce meuble comporte tous les systèmes de sécurité de la classe B + une ou plusieurs serrures pouvant s'adapter à un nouveau jeu de clefs (serrures mécaniques dites à clef facilement permutable) ; + au moins une serrure dont la clef reste prisonnière du mécanisme tant que le pêne de la combinaison et les pênes du meuble ne sont pas sortis porte fermée. La marque et le numéro de série du meuble sont estampillés de façon apparente et inaltérable, à l'extérieur de celui-ci, sur le corps et sur toutes les portes du meuble ; le numéro de série et l'année de fabrication de chaque serrure figurent sur celles-ci.

Classes des postes utilisateurs classifiés

Il est possible de déroger aux mesures de protection logiques prévues ci-dessous en mettant en œuvre des mesures de protection compensatoires, sous réserve de leur validation formelle par l'autorité d'homologation pour le niveau *Secret de Sécurité Nationale* ou, pour le niveau *Très Secret de Sécurité Nationale,* par l'autorité qualifiée de la sécurité des systèmes d'information.

DESCRIPTION	**CLASSE γ DE BASE**	CLASSE **β** RENFORCE	CLASSE **α** FORT
Intégrité physique des éléments constitutifs du SI	Scellés génériques de contrôle d'ouverture de l'équipement avec traçabilité des équipements ayant reçu des scellés Contrôle ponctuel de l'intégrité des scellés par l'utilisateur.	Protection de la classe **γ** + Contrôle annuel de l'intégrité des scellés.	Dispositif de détection d'ouverture de l'équipement ou scellés numérotés de contrôle d'ouverture de l'équipement avec traçabilité des équipements ayant reçu ces scellés Contrôle semestriel de l'intégrité des scellés.
Confidentialité des données lorsque le terminal[57] n'est pas en fonctionnement	Chiffrement des données utilisateur par un logiciel agréé pour la protection des informations portant la mention *Diffusion Restreinte* ou Stockage à distance des données sur l'infrastructure d'hébergement du SI ou Mémoire de masse extractible ou équipement mobile stockable dans un meuble de classe adaptée à la classification des données en clair	Chiffrement intégral du disque par un logiciel agréé pour la protection des informations portant la mention *Diffusion Restreinte* ou Stockage à distance des données sur l'infrastructure d'hébergement du SI ou Mémoire de masse extractible ou équipement mobile stockable dans un meuble de classe adaptée à la classification des données en clair	Protection de la classe β
Sécurité du contrôle d'accès del'utilisateur	Mot de passe avec politique de sécurité des mots de passe conforme à la politique de sécurité de l'organisme	Dispositif d'authentification forte, par exemple basée sur une infrastructure de gestion de clefs (IGC)	Dispositif d'authentification forte, par exemple basée sur une IGC qualifiée au moins RGSP.

[57] Le terminal s'entend comme le poste utilisateur fixe, nomade ou mobile, qui permet l'accès et le traitement des informations classifiées lorsqu'il est en fonctionnement.

		conforme au RGSP[58] homologuée par l'organisme -	
Accès aux dispositifs d'import - export du poste utilisateur	Réservé aux utilisateurs authentifiés sur le terminal + supports amovibles préalablement « enrôlés » sur le système et autorisés pour cet utilisateur	Protection de la classe γ	Réservé aux utilisateurs assurant une fonction d'enregistrement des documents classifiés ou de gestion des échanges
Contrôle des équipements connectés au réseau	Désactivation des services non utilisés (conformité)	Protection de la classe γ + Authentification des équipements au réseau	Protection de la classe β
Cloisonnement et filtrage	Cloisonnement par fonction homogène au sein du SI (cloisonnement des réseaux locaux-LANs-par population)	Cloisonnement entre les utilisateurs d'une même population, exemple P-VLAN.	Cloisonnement par le chiffre pour chaque poste utilisateur (tunnel dédié vers les services)
Capacité à restreindre la visualisation des IC par un tiers.	Disposition des terminaux par rapport aux ouvertures du local (portes, fenêtres, vasistas, hublots, etc.) et protection des vis-à-vis	Protection de la classe γ	Protection de la classe β

Tableaux de combinaison des classes

L'objectif final est d'égaler ou de surpasser le temps de freinage énoncé dans les principes généraux pourobtenir un niveau de sécurité minimal pour les informations et supports classifiés.

La détermination de ce niveau est réalisée en deux temps :

- *la classification des barrières (emprise, bâtiment, local, meuble ou moyen logique) à travers les moyens de détection d'intrusion ou de freinage qui leurs sont associées ;*
- *la vérification de la validité de la combinaison des classes des barrières en fonction du niveau de classification des informations et supports classifiés.*

Dans le cas où le niveau minimal de sécurité ne peut être atteint, il faut faire évoluer la classe d'une ou desbarrières pour atteindre ce niveau.

[58] Le référentiel général de sécurité de la Principauté(RGSP) publié par l'AMSN est le cadre règlementaire permettant d'instaurer la confiance dans les échanges au sein de l'administration et avec les usagers.

Protection des informations et supports classifiés

La protection des informations et supports classifiés est assurée par trois barrières physiques successives auniveau du bâtiment, du local et du meuble.

Les tableaux 1 et 2 définissent, pour chaque niveau de classification, la classe minimale du meuble enfonction des classes de protection du bâtiment et du local.

Tableau 1 : niveau *Secret de Sécurité Nationale*

CLASSE DU BATIMENT	CLASSE DU LOCAL			
	a	b	c	d
1	C	C	C	C
2	C	C	C	C
3	C	C	C	B
4	C	C	B	interdit

Si des informations et supports classifiés au niveau *Secret de Sécurité Nationale*, hors systèmes d'information classifiés, nepeuvent être conservés dans un meuble de sécurité en raison de leur dimension, ils sont alors conservés dans un local renforcé correspondant aux caractéristiques suivantes :

- *l'emprise ou le bâtiment est au minimum de classe 3. Un contrôle permanent de la zone est organisé en s'appuyant sur un dispositif de détection-alarme relié à un élément d'intervention extérieur ;*
- *le local est au minimum de classe c avec un dispositif de détection-alarme indépendant de ceux de l'emprise/bâtiment*[59].

S'agissant des systèmes d'informations classifiés au niveau *Secret de Sécurité Nationale*, les mesures de sécurité sont conformes à celles définies au tableau 3.

Tableau 2 : niveau *Très Secret de Sécurité Nationale*

CLASSE DU BATIMENT	**CLASSE DU LOCAL**			
	a	b	c	d
1	C	C	interdit	interdit
2	C	C	interdit	interdit
3	C	C	interdit	interdit
4	interdit	interdit	interdit	interdit

Si des informations et supports classifiés au niveau *Très Secret de Sécurité Nationale* ne peuvent être conservés dans un meuble de sécurité en raison de leur dimension, ils sont alors conservés dans un local renforcé correspondant aux caractéristiques suivantes :

- *l'emprise ou le bâtiment est au minimum de classe 2. Un contrôle permanent de la zone est organisé en s'appuyant sur un dispositif de détection-alarme relié à un élément d'intervention extérieur ;*

[59] Les détecteurs sont généralement raccordés à une centrale locale placée dans le local ou la zone, sans qu'aucun élément (câblage par exemple) ne sorte de la zone à protéger. C'est la liaison entre les centrales locale et générale qui peut sortir de la zone, sous réserve qu'elle soit chiffrée. C'est en cela que le système est indépendant. Il ne s'agit donc pas obligatoirement de déployer deux systèmes d'information de détection d'intrusion.

- *le local est au minimum de classe b avec un dispositif de détection-alarme indépendant de ceux de l'emprise/bâtiment*[9].
- *S'agissant des systèmes d'informations classifiés au niveau Très Secret de Sécurité Nationale, les mesures de sécurité sontconformes à celles définies au tableau 4.*

Protection des systèmes d'information classifiés

La protection des systèmes d'information classifiés est assurée par la combinaison de deux barrières physiques et d'une barrière logique.

Le tableaux 3 définit, pour le niveau S*ecret de Sécurité Nationale*, la classe minimale de la protection logique en fonction des classes de protection physique du bâtiment et du local. La lettre grecque désigne la classe du système d'information classifié.

Tableau 3 : niveau *Secret de Sécurité Nationale*

CLASSE DU BATIMENT	CLASSE DU LOCAL			
	a	b	c	d
1	γ	γ	β	β
2	γ	γ	β	β
3	γ	γ	β	α
4	γ	γ	α	interdit

Dans l'hypothèse où les barrières physiques sont assurées par le local et un meuble adapté[60], sans considération du niveau de protection du bâtiment, le tableau 4 définit, pour le seul niveau de classification *Secret de Sécurité Nationale,* la classe minimale de protection logique.

Tableau 4 : niveau *Secret de Sécurité Nationale*

CLASSE DU MEUBLE	CLASSE DU LOCAL			
	a	b	c	d
A	γ	γ	β	α
B	γ	γ	β	α
C	γ	β	α	α

[60] Par exemple, baie technique blindée ou armoire forte dédiée aux serveurs

Appendice 27 – Contrôle d'accès

Le contrôle d'accès s'intègre dans un dispositif global de sécurité fondé sur son association avec les protections décrites à l'Annexe 26. Composant d'un système de management de la sûreté, il est déployé en cohérence avec les systèmes de détection d'intrusion et de vidéosurveillance. Il comprend les moyens suivants :

- *identification pour recueillir les droits d'accès de l'individu et les transmettre à un moyen de traitement ;*
- *traitement qui valide, selon les droits accordés, les informations fournies par le moyen de contrôle afin de lever l'obstacle et de libérer le passage. Il recouvre trois méthodes : l'action d'une personne, celle d'un système automatisé ou la combinaison des deux ;*
- *freinage pour faire obstacle à l'intrusion et gagner le temps nécessaire à l'intervention ;*
- *les mesures organisationnelles et humaines qui permettent sa mise en œuvre et la conduite à tenir en cas d'incident.*

Le contrôle d'accès consiste à vérifier si une personne demandant à accéder à un lieu est autorisée à pénétrerdans une enceinte ou un bâtiment. Il repose sur les principes suivants :

- *l'homogénéité entre les moyens de contrôle d'accès et les autres moyens de protection retenus ;*
- *la succession de filtres (le contrôle des accédants doit être réparti dans la profondeur, en plusieurs couches) ;*
- *la proportionnalité à la menace (le contrôle doit être adapté aux agresseurs potentiels) ;*
- *l'adaptation aux accédants (il doit être accepté par ses utilisateurs courants).*

Les solutions techniques retenues dépendent des besoins :

- *son utilité : accès à une emprise, un bâtiment, une zone, un local ;*
- *objet du contrôle : militaires, civils, scientifiques, personnel d'entretien, techniciens, personnel de maintenance ;*
- *menace dont il faut se protéger : menace interne, vandalisme ou renseignement.*

Avant tout choix de conception, un audit est nécessaire afin d'avoir une bonne connaissance du site, ce qui permet :

- *d'identifier, localiser, hiérarchiser les cibles d'un site et les zones précises à contrôler ;*
- *d'analyser les flux d'individus, de véhicules à chaque point d'accès ;*
- *de constater les niveaux existant de protection des zones (ouvertures, parois, existence ou non de systèmes de contrôle comme les lecteurs de badges, obstacles au passage, niveau de résistance de ces obstacles à l'effraction, homogénéité de ces différents points, etc.) ;*
- *d'identifier les menaces potentielles (intrusion involontaire ou de curieux, pénétration délibérée de personnes initiées et/ou équipées, complicité interne, etc.) ;*
- *de prendre en compte les contraintes architecturales et réglementaires (incendie, protection du secret de sécurité nationale, etc.).*

Exemples de moyens pour contrôler les accès : portillons, portes à unicité de passage, barrières, sas, interphones, vidéophones, serrures à clefs, claviers à code, lecteurs de badge, lecteurs biométriques, lecteur de plaque d'immatriculation, etc.

Appendice 28 – Mesures applicables aux zones réservées

Dès lors que des informations et supports classifiés au niveau *Très Secret de Sécurité Nationale* sont traités dans des locaux, des mesures particulières de sécurité doivent être mises en place. Ces mesures de sécurité permettent de définir les zones réservées, elles-mêmes obligatoirement situées en zone protégée.

Le traitement ou la conservation d'informations et supports classifiés dans ces locaux ne peut intervenir, sauf en cas d'impossibilité majeure, qu'après avis technique d'aptitude physique de la Direction de la Sûreté Publique quant à l'aptitude de ces locaux à accueillir des informations de niveau *Très Secret de Sécurité Nationale*.

Lorsque des services ou des organismes sont amenés à traiter de telles informations, pour des raisons opérationnelles et de manière temporaire, une zone réservée temporaire soumise aux mesures de sécurité détaillées plus haut peut être créée, y compris lorsque les conditions de création d'une zone protégée ne sont pas réunies.

Les lieux abritant des informations et supports classifiés au niveau *Très Secret de Sécurité Nationale*, faisant l'objet d'une classification spéciale, répondent aux normes complémentaires suivantes :

- *un local pourvu d'ouvertures en nombre restreint à la protection renforcée ;*
- *ce local contient un meuble de sécurité approuvé ;*
- *un contrôle permanent du lieu est organisé, s'appuyant au minimum sur un des systèmes de protection décrits en Appendice 25.*

1. Contrôles des locaux

Pour chaque lieu, un responsable s'assure que les mesures de protection prévues, dont notamment les règles d'accès au site, sont appliquées.

Pendant les heures de travail, le contrôle du lieu incombe aux personnes qui y sont employées. Avant toute absence, ils vérifient la mise en sûreté des supports classifiés ainsi que la fermeture des meubles de sécurité et des bureaux.

En dehors des heures ouvrables, les autorités responsables s'organisent pour contrôler :

- *le fonctionnement des systèmes de détection ;*
- *la fermeture des bureaux, des meubles de sécurité, etc. ;*
- *le vidage des corbeilles à papier et l'absence dans celles-ci de brouillons ou de documents préparatoires aux informations classifiées ;*
- *l'absence, hors des coffres, de supports classifiés, hormis les matériels qui ne pourraient pas être soustraits aux vues directes.*

Des rondes de sécurité sont régulièrement effectuées par des gardiens ayant fait l'objet d'une enquête administrative et qui disposent de consignes écrites précisant leur mission. Ils ne sont pas autorisés à pénétrer dans ces zones réservées en l'absence du personnel de ces dernières, sauf nécessité de service (levée de doute, réglementation particulière, urgence avérée).

2. Contrôle des personnes et des visiteurs dans des lieux abritant des informations et supports classifiés Très Secret de Sécurité Nationale

Les personnes en service ayant accès, en raison de leurs fonctions au lieu abritant des éléments classifiés du niveau *Très Secret de Sécurité Nationale*, disposent d'un badge apparent.

Les visiteurs :

- *font l'objet d'une autorisation individuelle de l'autorité responsable ;*
- *sont accompagnés pendant toute la durée de leur visite par une personne habilitée autorisée.*

Le personnel d'entretien :

- *a satisfait à une enquête administrative ;*
- *appartient à une société ayant au préalable satisfait à une enquête administrative ;*
- *porte un badge apparent avec photographie ;*
- *intervient en présence d'une personne habilitée autorisée.*

Appendice 29 – Clauses-types contractuelles de protection du secret de sécurité nationale pour les contrats sensibles

Dans le cadre des dispositions législatives et réglementaires en matière de protection du secret de sécurité nationale, le titulaire s'engage à prendre toutes les mesures utiles pour assurer lors de l'exécution du contrat la protection des informations et supports classifiés qui peuvent être détenus dans le service, au profit duquel le contrat est exécuté ou dans tout lieu dans lequel ce contrat est exécuté.

- *Le titulaire reconnaît :*
- *avoir pris connaissance des articles 18 et 19 de la loi n° 1.430 du 13 juillet 2016, suscitée ;*
- *qu'il n'a pas à connaître ou détenir les informations couvertes par le secret de sécurité nationale.*
- *Le titulaire reconnaît avoir fait signer une déclaration individuelle à l'ensemble du personnel appelé, sous sa responsabilité à un titre quelconque, à intervenir pour son compte pour exécuter les prestations. Par ce document, le personnel atteste :*
- *avoir pris connaissance des articles 18 et 19 de la loi n° 1.430 du 13 juillet 2016, suscitée ;*
- *qu'il n'a pas, sous peine de poursuites pénales, à connaître ou détenir des informations couvertes par le secret sécurité nationale.*
- *Le titulaire s'engage à ce que seules les personnes ayant préalablement souscrit la déclaration précitée accèdent au lieu d'exécution des prestations.*
- *Le titulaire s'engage à remettre à l'autorité contractante la ou les déclarations individuelles ci-dessus avant tout accès du personnel concerné au lieu d'exécution des prestations.*
- *Il ne peut être dérogé aux prescriptions ci-dessus, y compris en cas de remplacement inopiné, fortuit ou même urgent d'un personnel du titulaire.*
- *Le non-respect ou l'inobservation par le titulaire de ces mesures de sécurité, même dans les cas où elles résultent d'une imprudence ou d'une négligence, peut entraîner le prononcé d'une sanction contractuelle, sans préjudice des sanctions pénales.*

Appendice 30– Modèle de fiche navette

Département :

Organisme :

Date et numéro d'enregistrement :

FICHE NAVETTE

AVIS SUR UNE PERSONNE MORALE DANS LE CADRE D'UN CONTRAT SENSIBLE

Dénomination ou raison sociale de l'entreprise :

N° RCI de l'entreprise :

Adresse du siège social :

Identification de l'autorité contractante/acheteur bénéficiaire de la prestation :

Justification du recours au contrat sensible :

Dates prévisionnelles de début et de fin de travaux :

Lieu(x) d'exécution des prestations du contrat sensible :

Date d'expiration de la présente enquête administrative (s'il y a lieu) :

Avis de la Direction de la Sûreté Publique :

☐ *Sans réserve*

☐ *Avec réserve*

A	A
Le	Le
Autorité contractante/acheteur	DSP
Nom, prénom, qualité, signature	Signature

Appendice 31 – Guide des mesures de sécurité applicables au cours d'une réunion impliquant des informations et supports classifiés

1. *Avant la réunion*

- *l'organisateur détermine le niveau de classification de la réunion ;*
- *l'autorité destinataire de l'invitation adresse en temps utile à l'organisateur les noms et fonctions des personnes chargées de les représenter ainsi que leur niveau d'habilitation au moyen d'un certificat de sécurité ;*
- *l'organisateur établit la liste des participants, quel que soit leur qualité (auditeurs, conférenciers, assistants, techniciens chargés des projections ou essais, etc.). Cette liste est transmise à l'officier de sécurité ;*
- *l'officier de sécurité vérifie que l'habilitation des participants est valide et correspond au niveau des informations et supports qui vont être traités ;*
- *l'officier de sécurité s'assure que la salle accueillant la réunion répond aux conditions de sécurité inhérentes au niveau de classification des informations qui seront abordées et prend toutes les précautions utiles pour s'assurer qu'aucun appareil électronique ne soit susceptible de capter, réémettre ou enregistrer des sons, images ou informations sauf autorisation de sa part.*

2. *Au début de la réunion*

- *l'organisateur s'assure, conformément à la liste des participants, de l'identité et du niveau d'habilitation de ceux qui sont présents au vu de leur certificat de sécurité ;*
- *il leur indique le niveau maximal de classification des informations qui seront abordées au cours de la réunion et les règles de sécurité correspondantes ;*
- *assisté de l'officier de sécurité, l'organisateur s'assure que personne ne détienne, lors de la réunion, d'appareil permettant la captation, la réémission et l'enregistrement d'informations tels que, par exemple, un téléphone mobile ou un ordinateur portable ou tout objet connecté. Dans certains établissements affectés aux besoins de sécurité nationale, des installations radioélectriques de brouillage peuvent être utilisées aux fins de rendre inopérants, tant pour l'émission que pour la réception, les appareils de communications électroniques de tous types (téléphones mobiles et ordinateurs portables par exemple).*

3. *Pendant la réunion*

- *le niveau maximal de classification des informations évoquées au cours de la réunion ne doit pas dépasser le niveau d'habilitation de chaque participant ainsi que les capacités de protection de la salle accueillant la réunion ;*
- *l'organisateur peut interdire toute prise de note par les auditeurs. Il veille, en application des principes stricts de cloisonnement de l'information classifiée, en particulier au niveau Très Secret de Sécurité Nationale, y compris pour les classifications spéciales de ce niveau, à ce que la communication demeure limitée à l'objet de la réunion ;*
- *pendant les pauses, les participants sont autorisés à quitter la salle si la sécurité des supportsclassifiés qui y sont laissés est assurée. Les informations classifiées ne doivent pas être discutées en dehors de la salle de réunion ;*
- *toute faille dans la sécurité pendant la réunion doit être notifiée à l'organisateur et à l'officier de sécurité qui en informe les participants.*

4. À l'issue de la réunion

- *les documents classifiés sont récupérés, rangés ou détruits sous la responsabilité de l'organisateur et de l'officier de sécurité dès lors qu'ils cessent d'être utiles ;*
- *l'organisateur rédige un document succinct, éventuellement classifié, dans lequel il est fait mention de la liste des participants, des domaines d'informations classifiées exposés ainsi que des mesures prises pour en assurer la protection. Ce document peut être diffusé aux personnes qualifiées puis est géré dans les conditions fixées par le présent arrêté ;*
- *lorsque les participants sont autorisés à prendre des notes au cours de la réunion, ils sont informés, par l'organisateur, de leur responsabilité en matière de protection du secret de sécurité nationale ;*
- *l'organisateur fait procéder à la récupération et à la mise en sécurité des supports classifiés éventuellement mis à la disposition des auditeurs (documents, graphiques, plans, films, bandes d'enregistrement, etc.) ainsi qu'à la destruction des supports provisoires et préparatoires ;*
- *les participants assument la pleine responsabilité de la protection de leurs documents de travail et de leurs notes, qui sont à classifier au niveau correspondant à celui des informations recueillies. Ces documents sont détruits par leurs soins dès qu'ils ont cessé d'être utiles.*

Appendice 32 – Exemple de document classifié

SECRET de SÉCURITÉ NATIONALE

SPÉCIAL MONACO

À *lieu*,
le *date*

Déclassifié le [*date*]
N° *enregistrement lors de l'émission*

Objet : [NP] Intitulé

[NP] Paragraphe d'introduction contenant des éléments non classifiés et non protégés.

1. *Chapitre contenant des informations classifiées jusqu'au niveau Secret de Sécurité Nationale et protégées par la mention Spécial Monaco*

[NP] Paragraphe contenant des éléments non protégés.

Paragraphe contenant des éléments classifiés au niveau *Secret de Sécurité Nationale* et protégés par la mention *Spécial Monaco*

2. *Chapitre contenant des informations classifiées jusqu'au niveau Secret de Sécurité Nationale et protégées par la mention Spécial Monaco*

[DR] Paragraphe contenant des éléments protégés par la mention *Diffusion Restreinte*

Paragraphe contenant des éléments classifiés au niveau *Secret de Sécurité Nationale* et protégés par la mention *Spécial Monaco*

SECRET DE SÉCURITÉ NATIONALE

Appendice 34 – Modèles de timbres de classification et de protection

Les timbres sont apposés avec une encre indélébile de couleur rouge, sauf le timbre *Spécial Monaco* qui est de couleur bleue.

1. Couverture et page de garde pour les documents reliés

Le timbre est apposé au milieu du bas de la couverture, selon les règles de marquage suivantes :

- *Niveau de classification : centré, police Arial, gras, taille 18. Texte : taille 6 ;*
- *Epaisseur du cadre : 3 points.*

La mention complémentaire de protection *Spécial Monaco* est apposée sous le timbre de classification et respecte les règles de marquage prévues au point 2.

2. Pages du document

Le timbre est apposé au milieu du haut et du bas de la page (à l'exception du marquage *Spécial Monaco* qui est apposé uniquement en haut de la page), selon les règles de marquage suivantes :

- *Niveau de classification / Spécial Monaco : centré, police Arial, gras, taille 18 ;*
- *Epaisseur du cadre : 2,5 points.*

Appendice 34 – Modèles de timbres de déclassement et de déclassification

- *Pour réévaluer le niveau de classification :*

Classification à réévaluer le [*date*]

- *Pour abaisser le niveau de classification :*

Le déclassement du niveau *Très Secret de Sécurité Nationale*
au niveau
Secret de Sécurité Nationale
intervient le :
par décision n°:
du :

- *Pour rehausser le niveau de classification :*

Le reclassement du niveau *Secret de Sécurité Nationale*
au niveau *Très Secret de Sécurité Nationale*
intervient le
par décision n° :
du :

- *Pour déclassifier une information ou un support*

À déclassifier
sur ordre de l'autorité émettrice

Déclassifié le [*date*]

DÉCLASSIFIÉ
Par décision n°
du

Appendice 35 – Modèle de demande de reproduction d'un support classifié Très Secret de Sécurité Nationale

Département :

Organisme :

Date et numéro d'enregistrement :

DEMANDE DE REPRODUCTION D'UN SUPPORT CLASSIFIE *Très Secret de Sécurité Nationale*

Renseignements[61] concernant le support classifié *Très Secret de Sécurité Nationale* dont la reproduction est demandée

- *Numéro d'enregistrement :*
- *Date d'enregistrement :*
- *Numéro de l'exemplaire à partir duquel la reproduction sera effectuée :*

Organisme demandeur :

Motif de la demande :

Copies demandées

- *Nombre :*
- *Numérotation :*
- *Diffusion :*

A

Le

Nom, qualité, signature de l'autorité responsable de la demande et cachetde l'organisme

[61] L'objet du support ne doit en aucun cas être mentionné

Appendice 36 – Modèle d'autorisation de reproduction d'un support classifie Très Secret de Sécurité Nationale

Département :

Organisme :

Date et numéro d'enregistrement :

AUTORISATION DE REPRODUCTION D'UN SUPPORT CLASSIFIE *Très Secret de Sécurité Nationale*

Support classifié *Très Secret de Sécurité Nationale* dont la reproduction est autorisée

- *Numéro d'enregistrement :*
- *Date d'enregistrement :*
- *Numéro de l'exemplaire à partir duquel la reproduction sera effectuée :*

Organisme demandeur :

Référence de la demande :

-

Reproduction autorisée

- *Nombre :*
- *Numérotation :*
- *Diffusion :*

A

Le

Nom, qualité, signature de l'autorité responsable de la demande et cachetde l'organisme

Destinataires :

Appendice 37 – Modèle de bordereau de transmission de supports classifiés

Département :

Organisme :

Date et numéro d'enregistrement :

BORDEREAU DE TRANSMISSION DE SUPPORTS CLASSIFIES

A – B – B'

Références *(ne pas mentionner l'objet)*	**Date de création**	**Niveau de classification/ Autres mentions**	**Numéro d'exemplaire**	**Numéro de copie**	**Noms des destinataires**

Nom, qualité, signature de l'expéditeur
et cachet de l'organisme

Reçu le :

Par :

Organisme destinataire :

A : à conserver par le destinataire.
B : à renvoyer sans délai à l'expéditeur après émargement.
B' : à conserver en archives par l'expéditeur jusqu'à réception du feuillet B qui lui sera substitué.

Département :

Organisme :

Date et numéro d'enregistrement :

BORDEREAU DE TRANSMISSION DE SUPPORTS CLASSIFIES

A – **B** – B'

Références *(ne pas mentionner l'objet)*	**Date de création**	**Niveau de classification/ Autres mentions**	**Numéro d'exemplaire**	**Numéro de copie**	**Noms des destinataires**

Nom, qualité, signature de l'expéditeuret cachet de l'organisme

Reçu le :

Par :

Organisme destinataire :

A : à conserver par le destinataire.
B : à renvoyer sans délai à l'expéditeur après émargement.
B' : à conserver en archives par l'expéditeur jusqu'à réception du feuillet B qui lui sera substitué.

Département :

Organisme :

Date et numéro d'enregistrement :

BORDEREAU DE TRANSMISSION DE SUPPORTS CLASSIFIES

A – B – **B'**

Références *(ne pas mentionner l'objet)*	**Date de création**	**Niveau de classification/ Autres mentions**	**Numéro d'exemplaire**	**Numéro de copie**	**Noms des destinataires**

Nom, qualité, signature de l'expéditeuret cachet de l'organisme

Reçu le :

Par :

Organisme destinataire :

Appendice 38 – Modèle de décision de sécurité convoyeur

Département :

Organisme :

Date et numéro d'enregistrement :

DECISION DE SECURITE CONVOYEUR

Le[62] :

décide que

Madame/Monsieur[63]:

Date et lieu de naissance :

Grade ou titre :

Fonctions ou missions :

Peut effectuer le convoyage de supports classifiés jusques et y compris[64]:

Cette décision est valable pour la mission suivante :

A

Le

Nom, qualité, signature de l'autorité compétente[65] etcachet de l'organisme

[62] Autorité d'habilitation ou autorité ayant reçu délégation à cet effet
[63] Nom et prénom
[64] Préciser le niveau de classification et le domaine (Monaco, France, UE ou autres)
[65] Autorité d'habilitation ou autorité ayant reçu délégation à cet effet

Appendice 39 – Modèle de certificat de courrier

Département :

Organisme :

Date et numéro d'enregistrement :

CERTIFICAT DE COURRIER

Pour le convoyage international par porteur autorisé de supports et/ou matériels classifiés

Courier certificate

for international carriage of classified material and/or equipment

Nom du programme/projet :

Name of programme/project

Il est certifié que le porteur

This is to certify that the bearer

Madame/Monsieur (nom, prénom et titre) :

Ms/Mr (family name, first name and title)

Employé(e) par (organisme) :

Employed by (entity)

Né(e) le (jour/mois/année) : Pays :
Born on (day/month/year) *Country*

Nationalité :
Nationality

Titulaire du passeport ou de la carte d'identité n°
Holder of passport/identity card n°

Délivré(e) par (autorité) : Le (jour/mois/année) :
Issued by (issuing authority) *On (day/month/year)*

Est autorisé(e) à effectuer le voyage décrit ci-dessous avec l'envoi suivant (indiquer le n° des paquets,poids et dimensions de chaque colis) *Is authorised to carry on the journey detailed below with the following consignment (number, weight and dimensions of each package)*

Départ le : *Departure on*	Retour prévu le : *Planned return on*
De (pays) : *From (country)*	À (pays) : *To (country)*
Via (pays traversés): *Through (countries)*	
Officier de sécurité de l'organisme *Entity security officer* Date, cachet et signature/*Date, stamp and signature*	**Autorité nationale de sécurité** *National Security Authority or Designed Security Authority* Date, cachet et signature/*Date, stamp and signature*

L'attention des autorités des douanes, de police ou des services d'immigration est attirée sur les points indiqués au dos de ce certificat. *The attention of Customs, Police, and/or Immigration Officials is drawn to the points statedon the back of this certificate.*

Annexe au certificat de courrier n°

L'attention des autorités des douanes, de police et/ou des services d'immigration est attirée sur les points suivants / *The attention of Customs, Police, and/or Immigration Officials is drawn to the following:*

- *Le contenu de cet envoi est classifié dans l'intérêt de la sécurité nationale des pays cités ci-dessus / The content of this consignment is classified in the interests of national security of the countries mentioned above ;*

- *Il est demandé que l'envoi ne soit inspecté que par des personnes dûment autorisées ou titulaires d'une autorisation spéciale / It is requested that the consignment not be inspected other than by properly authorized persons or those with special permission;*

- *Si une inspection est jugée nécessaire, il est demandé qu'elle soit effectuée dans une zone hors de vue des personnes qui n'ont pas une nécessité d'accès aux informations et en présence du porteur / If an inspection is deemed necessary, it is requested that it be carried out in an area out of sight of persons who do nothave a need-to-know and in the presence of the bearer;*

- *Il est demandé que le paquet, s'il a été ouvert pour inspection, soit muni, après avoir été refermé, de la preuve de cette ouverture, par signature et cachet et par annotation des documents d'expédition (s'il y en a) attestant l'ouverture de l'envoi / It is requested that the package, if opened for inspection, be reclosed and marked by sealing and signing it and by annotating the shipping documents (if any) that the consignment has been opened in order to show evidence of the opening;*

- *Les fonctionnaires des douanes, de la police et/ou des services d'immigration des pays traversés, à l'entrée ou à la sortie, sont priés d'apporter leur assistance en cas de besoin afin que l'envoi soit amené à destination en toute sécurité. / Customs, Police, and/or Immigration officials of countries to be crossed, entered or exited are requested to give assistance if necessary to ensure the successful and secure delivery of the consignment.*

INSTRUCTIONS À L'ATTENTION DU PORTEUR AUTORISÉ

Annexe au certificat de courrier n°
Annexe à l'ordre de mission n°

Vous avez été désigné pour convoyer un support classifié. Un certificat de courrier vous a été délivré. Avant le début du voyage, vous êtes informé des règles de sécurité relatives au convoiement de supports classifiés et de vos obligations en matière de sécurité durant ledit voyage (comportement à adopter, itinéraire, horaire, etc.). Il vous est également demandé de signer une déclaration attestant que vous avez lu et compris les obligations relatives à la sécurité.

Votre attention est appelée sur les généralités suivantes :

1) *Vous êtes responsable du convoyage décrit dans le certificat de courrier.*
2) *Tout au long du voyage, l'envoi classifié doit rester en votre possession ou sous votre surveillance directe.*
3) *L'envoi ne doit pas être ouvert en cours de route, sauf dans les circonstances exposées au paragraphe 10 ci-dessous.*
4) *Vous ne devez ni parler de cet envoi classifié, ni le montrer dans un lieu public.*
5) *Cet envoi classifié ne doit en aucun cas être laissé sans surveillance durant les arrêts nocturnes. Les organismes publics ou privés, ayant les habilitations et aptitudes appropriées, peuvent être utilisés. Dans ce domaine, vous êtes renseigné par l'officier de sécurité de votre organisme.*
6) *Durant le convoiement d'un envoi classifié, il vous est interdit de dévier du plan de voyage fourni.*
7) *En cas d'urgence, vous devez prendre les mesures que vous jugez nécessaires à la protection de l'envoi, mais en aucun cas vous ne devez permettre que l'envoi ne reste pas en votre possession ; à cette fin, vos instructions précisent comment entrer en rapport avec les organismes de sécurité despays dans lesquels vous passez en transit (cf. 12)). Si ces précisions ne vous ont pas été fournies, demandez-les à l'officier de sécurité de votre organisme.*
8) *Il appartient, à vous-même et à l'officier de sécurité de votre organisme de vous assurer que les documents nécessaires à votre sortie du territoire et à votre voyage (passeport, certificats de change, carnet sanitaire, etc.) sont complets et en cours de validité.*
9) *Si des circonstances imprévues vous obligent à remettre l'envoi à des personnes autres que les représentants désignés de la société ou du gouvernement que vous devez joindre, vous le remettrez uniquement à des agents autorisés de l'un des points de contact énumérés au point 12).*
10) *Il ne vous est conféré aucune immunité par rapport aux fouilles effectuées par les services de douanes, de police et/ou d'immigration des différents pays dont vous traversez la frontière ; de ce fait, au cas où des agents demanderaient à connaître le contenu de l'envoi, vous leur montrez votre certificat de courrier et la présente note et vous insistez pour les présenter au chef du service de douane, de police et/ou d'immigration en personne. Cette démarche devrait suffire à faire passer l'envoi sans qu'il soit ouvert. Toutefois, si le chef du service de douane, de police et/ou d'immigration demande à voir effectivement le contenu de l'envoi, vous pourrez ouvrir celui-ci, à condition que cela soit fait hors de la vue de tierces personnes.*

    Vous devez prendre la précaution de ne montrer à l'agent intéressé qu'une partie du contenu suffisantepour le convaincre que l'envoi ne contient aucun autre objet et vous lui demandez de refermer l'emballage ou de vous aider à le refermer immédiatement après achèvement de l'inspection.

    Vous demandez au chef du service de douane, de police et/ou d'immigration de fournir la preuve de l'ouverture et de l'inspection des colis en y apposant sa signature et son cachet après fermeture et en confirmant au verso des listes inventaires que l'envoi a été ouvert.

S'il vous a été demandé d'ouvrir l'envoi dans les circonstances exposées ci-dessus, vous devez le faire savoir à l'officier de sécurité de l'organisme destinataire et à l'officier de sécurité de l'organisme expéditrice, qui en informeront les autorités de sécurité compétentes de leur gouvernement respectif (autorité nationale de sécurité/autorité de sécurité déléguée).

11) À votre retour, vous devez produire un récépissé de l'envoi, signé par l'officier de sécurité de l'organisme ayant reçu l'envoi ou par une autorité de sécurité compétente du gouvernement destinataire.

12) Au cours de votre itinéraire, vous contactez les autorités désignées ci-après pour leur demander assistance :

DÉCLARATION DU PORTEUR AUTORISÉ

Annexe au certificat de courrier n°

Je, soussigné(e)[66]:

employé(e) par[67]:

déclare que l'officier de sécurité de :

m'a remis les notes concernant la manipulation et la garde des supports/matériels classifiés que je doistransporter. Je les ai lues et comprises.

Je conserverai à tout moment, durant le voyage, ces supports/matériels classifiés et n'ouvrirai pas le colis à moins d'en être requis par les autorités douanières.

À mon arrivée, je remettrai au dépositaire désigné, contre signature du récépissé, les supports/matérielsclassifiés destinés à l'organisme réceptionnaire.

À

Le

Officier de sécurité
(nom, prénom et signature)

Porteur
(nom, prénom et signature)

[66] Nom, prénom, fonction.
[67] Dénomination de l'organisme

DESCRIPTIF DU TRANSPORT

Annexe au certificat de courrier n°

Transport effectué par (nom et prénom) :
Transported by (family name and given name)

Départ le :
Departure on (date)

Retour prévu le :
Planned return (date)

De (pays) :
From (country)

À (pays) :
To (country)

Via (pays traversés) :
Through (countries)

Arrêts autorisés (pays) :
Authorized stops (countries)

Références du bordereau d'envoi ou du récépissé
References of shipping docket or receipt

Coordonnées des autorités susceptibles d'être contactées en cas de besoin :
Officials you may contact to request assistance

Officier de sécurité
(Nom, prénom et signature)

Compte rendu à remplir et signer à la fin du voyage

Je déclare sur l'honneur que durant le voyage correspondant au présent descriptif, il ne s'est produit à ma connaissance aucun événement ou acte, de mon fait ou du fait d'autrui, de nature à compromettre la sécurité de l'envoi, à l'exception des éléments signalés ci-dessous, le cas échéant :

.....

.....

.....

À

Le

Officier de sécurité
(nom, prénom et signature)

Porteur
(nom, prénom et signature)

LISTE INVENTAIRE

Annexe au certificat de courrier n°

□ Documents, niveau(x) :	□ *Secret de Sécurité Nationale*	□ *Très Secret de Sécurité Nationale*
□ Equipements, niveau(x) :	□ *Secret de Sécurité Nationale*	□ *Très Secret de Sécurité Nationale*
□ Composants, niveau(x) :	□ *Secretde Sécurité Nationale*	□ *Très Secret de Sécurité Nationale*

L'inventaire, inscrit au verso, a été approuvé par[68] :

Dans le cadre du projet/contrat :

Référence de l'autorisation[69]:

Toute inspection a été avalisée par[70]:

Dans le cadre du projet/contrat :

Référence de l'autorisation[71]:

À

Le

Officier de sécurité
(nom, prénom et signature)

Porteur
(nom, prénom et signature)

RÉCÉPISSÉ[72]

Date et heure de remise au destinataire :

Cachet, timbre ou sceau officiel de l'organisme destinataire

Nom et fonction du signataire

[68] Nom, prénom, fonction, organisme, adresse de l'organisme
[69] Accordée par le directeur de programme au niveau *Très Secret de Sécurité Nationale*
[70] Nom, prénom, fonction, organisme, adresse de l'organisme
[71] Accordée par le directeur de programme au niveau *Très Secret*
[72] Rayer si mention inutile. Nombre d'exemplaires :

- *Procédure liste inventaire sans récépissé ;*
- *Procédure liste inventaire avec récépissé ;*
- *Archivage définitif : 1exemplaire officier de sécurité expéditeur (dernier exemplaire en retour)*

INVENTAIRE

Annexe au certificat de courrier n°

Numéro d'ordre	Description précise des documents, équipements et/ou composants classifiés	Nombre d'exemplaires ou quantités	Nombre de pages par document y compris annexes	Nombre total de pages	Nombre de paquets
	Total :	Total :		Total :	

PARTIE RESERVEE EN CAS D'INSPECTION DU OU DES COLIS

Visa et sceau du chef :

des douanes	
de la police	
des services de l'immigration	

Appendice 40 – Modèle de certificat de courrier multi-voyages

Département :

Organisme :

Date et numéro d'enregistrement :

CERTIFICAT DE COURRIER MULTI-VOYAGES

pour le convoyage international par porteur autorisé de supports et/ou matériels classifiés

Multi-journey courier certificate

for international carriage of classified material and/or equipment

Nom du programme/projet :

Name of programme/project

Il est certifié que le porteur

This is to certify that the bearer

Madame/Monsieur (nom, prénom et titre) :

Ms/Mr (family name, first name and title)

Employé(e) par (organisme) :

Employed by (entity)

Né(e) le (jour/mois/année) : Pays :
Born on (day/month/year) *Country*

Nationalité :

Nationality

Titulaire du passeport ou de la carte d'identité n°

Holder of passport/identity card n°

Délivré(e) par (autorité) : Le (jour/mois/année) :
Issued by (issuing authority) *On (day/month/year)*

Est autorisé(e) à transporter des supports et/ou matériels classifiés (indiquer le n° des paquets, poids et dimensions de chaque colis) entre les pays suivants / *Is authorized to carry classified material and/or equipment (number, weight and dimensions of each package) between the following countries :*

Le porteur est autorisé à utiliser le présent certificat autant que de besoin, pour des transports de supports et/ou matériels classifiés entre les pays ci-dessus / *The bearer is authorized to use this certificate as many times as necessary, for the transport of classified material and/or equipment between the countries mentioned above*

jusqu'à (date de validité) :

until (validity date)

Officier de sécurité de l'organisme *Entity security officer* Date, cachet et signature/*Date, stamp and signature*	**Autorité nationale de sécurité ou autorité de sécurité déléguée** *National Security Authority or Designed Security Authority* Date, cachet et signature/*Date, stamp and signature*

L'attention des autorités des douanes, de police ou des services d'immigration est attirée sur les points indiqués au dos de ce certificat. *The attention of Customs, Police, and/or Immigration Officials is drawn to the points stated on the back of this certificate.*

Annexe au certificat de courrier multi-voyages n°

L'attention des autorités des douanes, de police et/ou des services d'immigration est attirée sur les points suivants / *The attention of Customs, Police, and/or Immigration Officials is drawn to the following :*

- *Le contenu de cet envoi est classifié dans l'intérêt de la sécurité nationale des pays cités ci-dessus / The content of this consignment is classified in the interests of national security of the countries mentioned above ;*
- *Il est demandé que l'envoi ne soit inspecté que par des personnes dûment autorisées ou titulaires d'une autorisation spéciale / It is requested that the consignment not be inspected other than by properly authorizedpersons or those with special permission ;*
- *Si une inspection est jugée nécessaire, il est demandé qu'elle soit effectuée dans une zone hors de vue des personnes qui n'ont pas une nécessité d'accès aux informations et en présence du porteur / If an inspection is deemed necessary, it is requested that it be carried out in an area out of sight of persons who do not have a need-to-know and in the presence of the bearer ;*
- *Il est demandé que le paquet, s'il a été ouvert pour inspection, soit muni, après avoir été refermé, de la preuve de cette ouverture, par signature et cachet et par annotation des documents d'expédition (s'il y en a) attestant l'ouverture de l'envoi / It is requested that the package, if opened for inspection, be reclosed and marked by sealing and signing it and by annotating the shipping documents (if any) that the consignment has been opened in order to show evidence of the opening ;*
- *Les fonctionnaires des douanes, de la police et/ou des services d'immigration des pays traversés, à l'entrée ou à la sortie, sont priés d'apporter leur assistance en cas de besoin afin que l'envoi soit amené à destination en toute sécurité. / Customs, Police, and/or Immigration officials of countries to be crossed, entered or exited are requested to give assistance if necessary to ensure the successful and secure delivery of the consignment.*

INSTRUCTIONS À L'ATTENTION DU PORTEUR AUTORISÉ

Annexe au certificat de courrier multi-voyages n°

Annexe à l'ordre de mission n°

Vous avez été désigné pour convoyer un support classifié. Un certificat de courrier vous a été délivré. Avant le début du voyage, vous êtes informé des règles de sécurité relatives au convoiement de supports classifiés et de vos obligations en matière de sécurité durant ledit voyage (comportement à adopter, itinéraire, horaire, etc.). Il vous est également demandé de signer une déclaration attestant que vous avez lu et compris les obligations relatives à la sécurité.

Votre attention est appelée sur les généralités suivantes :

1) *Vous êtes responsable du convoyage décrit dans le certificat de courrier.*
2) *Tout au long du voyage, l'envoi classifié doit rester en votre possession ou sous votre surveillance directe.*
3) *L'envoi ne doit pas être ouvert en cours de route, sauf dans les circonstances exposées au paragraphe 10 ci-dessous.*
4) *Vous ne devez ni parler de cet envoi classifié, ni le montrer dans un lieu public.*
5) *Cet envoi classifié ne doit en aucun cas être laissé sans surveillance durant les arrêts nocturnes. Les organismes publics ou privés, ayant les habilitations et aptitudes appropriées, peuvent être utilisés. Dans ce domaine, vous êtes renseigné par l'officier de sécurité de votre organisme.*
6) *Durant le convoiement d'un envoi classifié, il vous est interdit de dévier du plan de voyage fourni.*
7) *En cas d'urgence, vous devez prendre les mesures que vous jugez nécessaires à la protection de l'envoi, mais en aucun cas vous ne devez permettre que l'envoi ne reste pas en votre possession ; à cette fin, vos instructions précisent comment entrer en rapport avec les organismes de sécurité des pays dans lesquels vous passez en transit (cf. 12)). Si ces précisions ne vous ont pas été fournies, demandez-les à l'officier de sécurité de votre organisme.*
8) *Il appartient, à vous-même et à l'officier de sécurité de votre organisme de vous assurer que les documents nécessaires à votre sortie du territoire et à votre voyage (passeport, certificats de change, carnet sanitaire, etc.) sont complets et en cours de validité.*
9) *Si des circonstances imprévues vous obligent à remettre l'envoi à des personnes autres que les représentants désignés de la société ou du gouvernement que vous devez joindre, vous le remettrez uniquement à des agents autorisés de l'un des points de contact énumérés au point 12).*
10) *Il ne vous est conféré aucune immunité par rapport aux fouilles effectuées par les services de douanes, de police et/ou d'immigration des différents pays dont vous traversez la frontière ; de ce fait, au cas où des agents demanderaient à connaître le contenu de l'envoi, vous leur montrez votre certificat de courrier et la présente note et vous insistez pour les présenter au chef du service de douane, de police et/ou d'immigration en personne. Cette démarche devrait suffire à faire passer l'envoi sans qu'il soit ouvert. Toutefois, si le chef du service de douane, de police et/ou d'immigration demande à voir effectivement le contenu de l'envoi, vous pourrez ouvrir celui-ci, à condition que cela soit fait hors de la vue de tierces personnes.*
11) *Vous devez prendre la précaution de ne montrer à l'agent intéressé qu'une partie du contenusuffisante pour le convaincre que l'envoi ne contient aucun autre objet et vous lui demandez de refermer l'emballage ou de vous aider à le refermer immédiatement après achèvement de l'inspection.*
12) *Vous demandez au chef du service de douane, de police et/ou d'immigration de fournir la preuve de l'ouverture et de l'inspection des colis en y apposant sa signature et son cachet après fermeture et en confirmant au verso des listes inventaires que l'envoi a été ouvert.*

13) S'il vous a été demandé d'ouvrir l'envoi dans les circonstances exposées ci-dessus, vous devez le faire savoir à l'officier de sécurité de l'organisme destinataire et à l'officier de sécurité de l'organisme expéditrice, qui en informeront les autorités de sécurité compétentes de leur gouvernement respectif (autorité nationale de sécurité/autorité de sécurité déléguée).

14) À votre retour, vous devez produire un récépissé de l'envoi, signé par l'officier de sécurité de l'organisme ayant reçu l'envoi ou par une autorité de sécurité compétente du gouvernement destinataire.

15) Au cours de votre itinéraire, vous contactez les autorités désignées ci-après pour leur demander assistance :

DÉCLARATION DU PORTEUR AUTORISÉ

Annexe au certificat de courrier multi-voyages n°

Je, soussigné(e)[73]:

employé(e) par[74]:

déclare que

l'officier de sécurité de :

m'a remis les notes concernant la manipulation et la garde des supports/matériels classifiés que je dois transporter. Je les ai lues et comprises.

Je conserverai à tout moment, durant le voyage, ces supports/matériels classifiés et n'ouvrirai pas le colis àmoins d'en être requis par les autorités douanières.

À mon arrivée, je remettrai au dépositaire désigné, contre signature du récépissé, les supports/matérielsclassifiés destinés à l'organisme réceptionnaire.

À

Le

Officier de sécurité
(nom, prénom et signature)

Porteur
(nom, prénom et signature)

[73] Nom, prénom, fonction.
[74] Dénomination de l'organisme

DESCRIPTIF DU TRANSPORT

Annexe au certificat de courrier multi-voyages n°

Transport effectué par (nom et prénom) :
Transported by (family name and given name)

Départ le :
Departure on (date)

Retour prévu le :
Planned return (date)

De (pays) :
From (country)

À (pays) :
To (country)

Via (pays traversés) :
Through (countries)

Arrêts autorisés (pays) :
Authorized stops (countries)

Références du bordereau d'envoi ou du récépissé
References of shipping docket or receipt

Coordonnées des autorités susceptibles d'être contactées en cas de besoin :
Officials you may contact to request assistance

Officier de sécurité
(Nom, prénom, signature)

Compte rendu à remplir et signer à la fin du voyage

Je déclare sur l'honneur que durant le voyage correspondant au présent descriptif, il ne s'estproduit à ma connaissance aucun événement ou acte, de mon fait ou du fait d'autrui, de nature à compromettre la sécurité de l'envoi, à l'exception des éléments signalés ci-dessous, le cas échéant :

.....

.....

.....

.....

À

Le

Officier de sécurité
(nom, prénom et signature)

Porteur
(nom, prénom et signature)

LISTE INVENTAIRE

Annexe au certificat de courrier multi-voyages n°

□ Documents, niveau(x) :	□ *Secret de Sécurité Nationale*	□ *Très Secret de Sécurité Nationale*
□ Equipements, niveau(x) :	□ *Secret de Sécurité Nationale*	□ *Très Secret de Sécurité Nationale*
□ Composants, niveau(x) :	□ *Secret de Sécurité Nationale*	□ *Très Secret de Sécurité Nationale*

L'inventaire, inscrit au verso, a été approuvé par[75]:

Dans le cadre du projet/contrat :

Référence de l'autorisation[76]:

Toute inspection a été avalisée par[77]:

Dans le cadre du projet/contrat :

Référence de l'autorisation[78]:

À
Le

Officier de sécurité
(nom, prénom et signature)

Porteur
(nom, prénom et signature)

RÉCÉPISSÉ [79]

Date et heure de remise au destinataire :

Cachet, timbre ou sceau officiel de l'organisme destinataire

Nom et fonction du signataire

[75] Nom, prénom, fonction, organisme, adresse de l'organisme
[76] Accordée par le directeur de programme au niveau *Très Secret de Sécurité Nationale*
[77] Nom, prénom, fonction, organisme, adresse de l'organisme
[78] Accordée par le directeur de programme au niveau *Très Secret de Sécurité Nationale*
[79] Rayer si mention inutile. Nombre d'exemplaires :

- *Procédure liste inventaire sans récépissé ;*
- *Procédure liste inventaire avec récépissé ;*
- Archivage définitif : 1exemplaire officier de sécurité expéditeur (dernier exemplaire en retour)

INVENTAIRE

Annexe au certificat de courrier multi-voyages n°

Numéro d'ordre	Description précise des documents, équipements et/ou composants classifiés	Nombre d'exemplaires ou quantités	Nombre de pages par document y compris annexes	Nombre total de pages	Nombre de paquets
	Total :	Total :		Total :	

PARTIE RESERVEE EN CAS D'INSPECTION DU OU DES COLIS

Visa et sceau du chef :

des douanes	
de la police	
des services de l'immigration	

Appendice 41 – Modèle de procès-verbal de destruction de supports classifiés *Secret de Sécurité Nationale* ou *Très Secret de Sécurité Nationale*

Département :

Organisme :

Date et numéro d'enregistrement :

PROCES-VERBAL DE DESTRUCTION DE SUPPORTS CLASSIFIES SECRET OU TRES SECRET DE SECURITE NATIONALE

Date et lieu de la destruction :

Référence de l'ordre de destruction :

Nom, grade, fonction du détenteur responsable :

Référence du support[80]	Date	Catégorie (éventuellement)	Numéro d'exemplaire	Numéro de copie

Nous, soussignés, certifions que le(s) support(s) classifiés désigné(s) ci-dessus a(ont) été détruit(s) ce jour,en notre présence et celle du détenteur responsable.

Nom, fonction et signature du témoin

Nom, fonction, signature du détenteur responsable et cachet de l'organisme

Copie à[81]

[80] Les références doivent être portées sur le procès-verbal de telle manière qu'il soit impossible de les modifier ou de les compléter ultérieurement, ajoutant par exemple, entre deux mentions, les références d'un autre document ou support.

[81] Autorité ayant donné l'ordre de destruction

Appendice 42 – Modèle d'inventaire des supports classifiés

Cote : [À renseigner par le service d'archives].

INVENTAIRE DES SUPPORTS CLASSIFIES CONTENUS DANS LA PRESENTE ENVELOPPE

Numéro d'ordre [à reporter sur le support inventorié]	**Nom du service ayant procédé à la classification ou de l'auteur du support classifié**	**Numéro d'enregistrement**	**Date d'émission**	**Titre ou objet du document**	**Niveau de classification**	**Date d'échéance de la classification**
1						
2						
3						
4						
5						

imprimé sur papier recyclé

IMPRIMERIE GRAPHIC SERVICE
GS COMMUNICATION S.A.M. MONACO