Annexes à l'Arrêté Ministériel n° 2022-331
du 13 juin 2022

ANNEXE AU « JOURNAL DE MONACO » N° 8.596

DU 24 JUIN 2022

Annexe 1 - Règles de sécurité applicables aux systèmes d'information des services exécutifs de l'État

Préambule

Le présent document définit les mesures de sécurité applicables aux systèmes d'information de l'État.

La politique de sécurité des systèmes d'information de l'État s'adresse :

- aux autorités hiérarchiques, qui sont responsables de la sécurité des informations traitées au sein de leurs services ;
- aux chefs de service exploitant des systèmes d'information ;
- aux personnes chargées de la sécurité et de l'exploitation des systèmes d'information ;
- à l'ensemble des fonctionnaires et agents non titulaires de l'État dans l'utilisation quotidienne des systèmes d'information, par application de la « Charte des systèmes d'information de l'État » publiée par arrêté ministériel n° 2015-703 du 26 novembre 2015 ;
- aux administrateurs, qu'ils soient fonctionnaires, agents publics ou préposés des services publics qui sont tenus de respecter les dispositions de la « Charte Administrateurs Réseaux et Système d'Information de l'État » annexée à l'arrêté ministériel n° 2018-281 du 4 avril 2018 susvisé.

La Politique de Sécurité des Systèmes d'Information de l'État énonce des mesures techniques générales, qui constituent un socle minimal. Pour certaines applications ou systèmes, ce socle minimal ne devra pas être considéré comme suffisant (en particulier pour les informations classifiées). Chaque département ministériel s'appuiera sur la politique de sécurité des systèmes d'information de l'État, les normes existantes et les guides techniques et recommandations rédigés par l'Agence Monégasque de Sécurité Numérique pour élaborer des mesures techniques détaillées.

La Politique de Sécurité des Systèmes d'Information de l'État sera d'autant plus facile à appliquer que le nombre de systèmes et d'intervenants sera réduit.

La Politique de Sécurité des Systèmes d'Information de l'État se décline en quatre parties. La première énonce les 10 principes stratégiques voulus par la PSSI-E. La seconde décrit la structure de l'organisation de la sécurité à mettre en place. La troisième détaille les 13 objectifs à atteindre. Enfin, la quatrième énonce les règles permettant de contribuer à la réalisation de chaque objectif.

La mise à jour de la présente annexe est réalisée par l'Agence Monégasque de Sécurité Numérique en liaison avec le RSSI et les chefs de service responsables de l'administration des systèmes d'information en fonction des évolutions législatives et règlementaires en matière de Sécurité des Systèmes d'Information et pourra prendre en compte :

- les évolutions des menaces et les retours d'expérience des traitements d'incidents ;
- les résultats d'analyses de risques ainsi que les actions découlant de contrôles ou d'inspections ;
- les évolutions des contextes organisationnels, juridiques, réglementaires, normatifs et technologiques ;
- des documents complémentaires et des directives permettant d'en faciliter ou d'en préciser la mise en œuvre.

La mise à jour est publiée par arrêté ministériel, lequel précise les modalités de transition et date d'effet.

1. Les principes stratégiques

- Principe n°1 : La maîtrise des systèmes d'information exige que les services de l'État fassent appel à des prestataires qualifiés par l'AMSN. S'il n'en existe pas, le recours à des opérateurs et des prestataires reconnus est à privilégier ;
- Principe n°2 : Tout système d'information de l'État doit faire l'objet d'une analyse de risques permettant une prise en compte préventive de sa sécurité, adaptée aux enjeux du système considéré. Toutes ces analyses s'inscrivent dans une démarche d'amélioration continue de la sécurité des systèmes, pendant toute leur durée de vie et permettent également de maintenir à jour une cartographie précise des systèmes d'information en service ;
- Principe n°3 : Les moyens humains et financiers consacrés à la sécurité des systèmes d'information de l'État doivent être planifiés, quantifiés et identifiés au sein des ressources globales des systèmes d'information ;
- Principe n°4 : Des moyens d'authentification forte, sont mis en place sur les systèmes d'information pour les activités d'administration ainsi que sur les systèmes d'information sensibles lorsque l'homologation le prévoit ;
- Principe n°5 : Les opérations de gestion et d'administration des systèmes d'information de l'État doivent être tracées et contrôlées ;
- Principe n°6 : La protection des systèmes d'information doit être assurée par l'application rigoureuse de règles précises. Ces règles font l'objet de la présente Politique de Sécurité des Systèmes d'Information de l'État ;
- Principe n°7 : Chaque fonctionnaire et agent non titulaire de l'État, en tant qu'utilisateur d'un système d'information, doit être informé de ses droits et devoirs mais également formé et sensibilisé à la cyber sécurité ;
- Principe n°8 : Les administrateurs et les utilisateurs des systèmes d'information doivent appliquer, après formation, les règles élémentaires d'hygiène informatique ;
- Principe n°9 : Les produits et services acquis par les services exécutifs de l'État qui sont destinés à assurer la sécurité des systèmes d'information doivent être qualifiés ou certifiés par l'AMSN. S'il n'en existe pas, le choix doit s'orienter vers des prestataires ou des industriels de confiance ;
- Principe n°10 : Les informations de l'Administration considérées comme sensibles, en raison de leurs besoins en confidentialité, intégrité ou disponibilité, sont hébergées sur le territoire monégasque.

2. Organisation de la protection

La présente partie fixe les conditions de mise en œuvre de la Politique de Sécurité des Systèmes d'Information de l'État.

2.1. Formation des agents

Les départements ministériels forment leurs personnels chargés d'appliquer la politique de sécurité des systèmes d'information de l'État.

Ces derniers doivent être sensibilisés à la sécurité des systèmes d'information (SSI) et au respect des règles de sécurité a minima tous les 3 ans. Les agents exploitant les systèmes d'information ou assurant des missions en lien avec la sécurité des systèmes d'information font l'objet de formations adaptées, dispensées par des professionnels de la sécurité des systèmes d'information.

2.2. Mise en application de la politique de sécurité des systèmes d'information de l'État dans les départements ministériels

Au sein de chaque département ministériel, chaque service concerné met en place un dispositif organisationnel de suivi des risques pour ses systèmes d'information, ou le délègue formellement à un tiers, qui doit permettre une meilleure maîtrise de la sécurité desdits systèmes, par la mise en œuvre de mesures de protection proportionnées aux enjeux et en adéquation avec les risques encourus.

Ce dispositif de gestion s'appuie sur un processus régulier d'identification, d'appréciation et de traitement des risques.

Il doit également permettre de s'assurer que les mesures de sécurité sont adaptées. Le choix de ces mesures est effectué en s'assurant que les actions prévues et les coûts engendrés sont proportionnés à la réduction du risque.

Les services concernés peuvent s'appuyer sur les guides et recommandations rédigés par l'Agence Monégasque de Sécurité Numérique ou l'Agence Nationale de la Sécurité des Systèmes d'Information https://www.ssi.gouv.fr/administration/bonnes-pratiques/ .

Dans ce but, chaque service concerné :

- met en place une organisation en application de la politique de sécurité des systèmes d'information de l'État ;
- établit un inventaire de ses systèmes d'information et en évalue la sensibilité ;
- conduit une analyse de risques pour ses systèmes d'information, selon la méthode préconisée par l'Agence Monégasque de Sécurité Numérique et met en place les mesures de sécurité applicables ;
- organise des actions de sensibilisation et formation à la sécurité des systèmes d'information, communication claire sur les sanctions encourues avec le support du RSSI et de l'AMSN ;
- conduit des actions régulières de contrôle du niveau de sécurité de ses systèmes d'information et met en œuvre les actions correctives nécessaires ;
- met en place les processus lui permettant de faire face aux alertes, aux incidents de sécurité et aux situations d'urgence.

2.3. Contrôle et suivi de l'application de la politique de sécurité des systèmes d'information de l'État

Le respect de la politique de sécurité des systèmes d'information de l'État peut faire l'objet de contrôles réguliers, par l'AMSN et le RSSI.

Lors de ces contrôles, la conformité des dispositions prises par les services concernés avec les exigences de la présente politique de sécurité des systèmes d'information de l'État est vérifiée.

Des actions de contrôle peuvent être engagées à la suite d'incidents de sécurité majeurs, ou en cas de forte suspicion de non-conformité.

2.4. Traitement des incidents et gestion de crise

La rapidité des attaques informatiques rend nécessaire une veille renforcée et une réaction coordonnée des différents acteurs. Afin de rétablir le fonctionnement rapide des activités vitales de la Principauté, une stratégie de traitement des incidents et de gestion de crise est mise en place.

L'ensemble des acteurs (utilisateurs, responsables d'applications, des réseaux et des centres serveurs...) doit faire connaître à l'Agence Monégasque de Sécurité Numérique tout événement affectant ou pouvant

affecter la disponibilité, l'intégrité, la confidentialité ou la traçabilité des systèmes d'information d'un service concerné.

Une alerte est une action d'information portant à la connaissance des acteurs concernés des situations ou des faits techniques relatifs à la sécurité des systèmes d'information et nécessitant un traitement et une vérification des mesures prises. Les alertes sont issues de la veille permanente effectuée par le réseau des centres d'alerte et de réaction aux attaques informatiques appelés également « Computer Emergency Response Team » au niveau international (CERT) dont fait partie l'Agence Monégasque de Sécurité Numérique. Les alertes significatives sont signalées par l'Agence Monégasque de Sécurité Numérique aux responsables des systèmes d'information. Leur prise en compte au sein de chaque département ministériel ou service concerné est organisée sous leur responsabilité.

Une situation d'urgence de sécurité des systèmes d'information résulte de toute alerte ou incident sur un ou plusieurs systèmes d'information générant un dysfonctionnement majeur des activités du département ministériel ou du service concerné. Une situation de cette nature impose une forte réactivité et une coordination planifiée des différents acteurs concernés. Il est donc impératif que les départements ministériels prennent en compte la problématique de la sécurité des systèmes d'information dans leur organisation de gestion de crise et leurs plans de continuité et de reprise d'activité. Ces actions doivent être menées en cohérence avec la planification gouvernementale de gestion de crise.

3. Objectifs

Les objectifs de la politique de sécurité des systèmes d'information de l'État se déclinent sur plusieurs axes.

3.1. Politique, organisation, gouvernance

- Mettre en place une organisation adéquate, garantissant la prise en compte préventive et réactive de la sécurité.

3.2. Gestion des ressources humaines

- Accompagner, encadrer, sensibiliser les utilisateurs et administrateurs des services concernés.

3.3. Gestion des biens

- Tenir à jour une cartographie détaillée et complète des systèmes d'information.
- Qualifier l'information de façon à adapter les mesures de protection.

3.4. Intégration de la sécurité dans le cycle de vie des systèmes d'information

- Apprécier, traiter, et communiquer sur les risques relatifs à la sécurité des systèmes d'information.
- Maintenir en conditions opérationnelles et de sécurité les systèmes d'information.
- Gérer dynamiquement les mesures de protection, tout au long de la vie du système d'information.
- Utiliser des produits et services dont la sécurité est évaluée et attestée par l'Agence Monégasque de Sécurité Numérique, afin de renforcer la protection des systèmes d'information.
- Maîtriser les prestations de service. Veiller aux exigences de sécurité lorsqu'il est fait appel à de la prestation par des tiers.

3.5. Sécurité physique des locaux abritant les systèmes d'information

- Prendre en compte la sécurisation physique des systèmes d'information dans la sécurisation physique des locaux et dans les processus associés.

3.6. Sécurité physique des centres informatiques

- Dimensionner les protections physiques des centres informatiques en fonction des enjeux liés à la concentration des moyens et données abrités.
- Traiter de manière globale la sécurité des systèmes d'information et de communication qui assurent la sûreté d'un site.

3.7. Sécurité des réseaux

- Utiliser les infrastructures nationales, en respectant les règles de sécurité qui leur sont attachées.
- Maîtriser les interconnexions de réseaux locaux. Configurer de manière adéquate les équipements de réseau actifs.
- Ne pas porter atteinte à la sécurité du système d'information par le déploiement d'accès non supervisés.
- Maîtriser le déploiement, la configuration et l'usage des réseaux sans fil.
- Configurer les mécanismes de commutation et de routage pour se protéger des attaques.
- Tenir à jour une cartographie détaillée et complète des réseaux et des interconnexions.
- Appliquer les principes de défense en profondeur à l'architecture matérielle et logicielle des centres informatiques.

3.8. Exploitation des systèmes d'information

- Définir et mettre en œuvre des mesures de protection renforcées pour les informations sensibles.
- Durcir les configurations des ressources informatiques, et surveiller les interventions opérées sur celles-ci.
- Authentifier les usagers et contrôler leurs accès aux ressources des systèmes d'information de l'État, en fonction d'une politique explicite d'autorisations.
- Fournir aux administrateurs les outils nécessaires à l'exercice des tâches de sécurité des systèmes d'information et configurer ces outils de manière sécurisée.
- Défendre les systèmes d'information nécessite une vigilance de tous, et des actions permanentes.
- Exploiter de manière sécurisée les centres informatiques en s'appuyant sur des procédures adaptées et sur la maîtrise des outils de supervision.

3.9. Sécurité du poste de travail

- Durcir les configurations des postes de travail en protégeant les utilisateurs.
- Paramétrer les imprimantes et copieurs multifonctions afin de diminuer leur surface d'attaque.
- Sécuriser la téléphonie pour protéger les utilisateurs contre des attaques malveillantes.
- Contrôler régulièrement la conformité des paramétrages de sécurité appliqués aux postes de travail.

3.10. Sécurité du développement des systèmes

- Reconnaître la sécurité comme une fonction essentielle, et la prendre en compte dès la conception des projets.
- Mener les développements logiciels selon une méthodologie de sécurisation du code produit.
- Accompagner le développement sécurisé d'applications à risques par des contre-mesures minimisant l'impact d'attaques nouvelles.

3.11. Traitement des incidents

- Partager l'information (alertes, incidents) dans le respect des règles de prudence et mutualiser les opérations de remise en état, de façon à lutter efficacement contre les attaques.

3.12. Continuité d'activité

- Se doter de plans de continuité d'activité, et les tester.

3.13. Contrôles

- Effectuer des contrôles (audits, inspections) et des exercices réguliers de façon à mesurer les progrès accomplis et corriger les manquements.

4. Règles applicables

4.1. Politique, organisation, gouvernance

Mettre en place une organisation adéquate, garantissant la prise en compte préventive et réactive de la sécurité.

4.1.1. ORG-SSI : organisation de la sécurité des systèmes d'information

Une organisation de la SSI est définie au sein de chaque département et au sein de chaque entité. Cette organisation identifie les acteurs, définit les responsabilités internes et à l'égard des tiers, les modalités de coordination avec les autorités, le RSSI et l'AMSN, ainsi que les modalités d'application des mesures de protection. Des procédures d'applications sont écrites et portées à la connaissance de tous.

4.2. Ressources humaines

Faire des utilisateurs et des administrateurs des contributeurs avisés de la sécurité des systèmes d'information.

4.2.1. RH-SSI : utilisateurs

Une charte d'application de la PSSI-E, récapitulant les mesures pratiques d'utilisation sécurisée des ressources informatiques élaborée par la direction informatique, est communiquée à l'ensemble des agents de chaque entité. Le personnel non permanent (stagiaires, intérimaires, prestataires…) est informé de ses devoirs dans le cadre de son usage des systèmes d'information des institutions officielles de la Principauté.

4.2.2. RH-MOTIV : personnel permanent

Une attention particulière doit être portée au recrutement des personnes en charge de la sécurité des systèmes d'information. Les administrateurs doivent être régulièrement sensibilisés aux devoirs liés à leur fonction, et doivent veiller à respecter ces exigences dans le cadre de leurs activités quotidiennes.

4.2.3. RH-UTIL : sensibilisation des utilisateurs des systèmes d'information

Chaque utilisateur permanent doit être régulièrement informé des exigences de sécurité le concernant et à leur respect. Il doit être formé à l'utilisation des outils de travail conformément aux règles de la PSSI-E.

4.2.4. RH-MOUV : mouvement de personnel permanent

Une procédure permettant de gérer les arrivées, les mutations et les départs des collaborateurs dans les systèmes d'information doit être formalisée et appliquée strictement. Cette procédure doit couvrir au minimum :

- la gestion/révocation des comptes et des droits d'accès aux systèmes d'information, y compris pour les partenaires et les prestataires externes ;
- la gestion du contrôle d'accès aux locaux ;
- la gestion des équipements mobiles ;
- la gestion du contrôle des habilitations.

4.2.5. RH-NPERM : gestion du personnel non permanent

Les règles de la PSSI-E. s'appliquent à tout personnel non permanent utilisateur (stagiaires, intérimaires, prestataires, …) d'un système d'information de l'État. Pour tout personnel non permanent, un tutorat par un agent permanent est mis en place, afin de l'informer de ces règles et d'en contrôler l'application.

4.3. Gestion des biens

Tenir à jour une cartographie détaillée et complète des SI

4.3.1. GDB-INVENT : inventaire des ressources informatiques

Chaque entité établit et maintient à jour un inventaire des ressources informatiques sous sa responsabilité, en s'appuyant sur un outillage adapté. Cet inventaire est communiqué annuellement au RSSI et à l'AMSN pour les besoins de coordination opérationnelle. Il comprend la liste des « briques » matérielles et logicielles utilisées, ainsi que leurs versions exactes.

4.3.2. GDB-CARTO : cartographie

La cartographie précise les centres informatiques, les architectures des réseaux (sur lesquelles sont identifiés les points névralgiques et la sensibilité des informations manipulées) et qualifie le niveau de sécurité attendu. Cette cartographie est maintenue à jour et tenue à disposition du RSSI et de l'AMSN.

Qualifier l'information de façon à adapter les mesures de protection.

4.3.3. GDB-QUALIF-SENSI : qualification des informations

La sensibilité de toute information doit être évaluée. Le marquage systématique des documents, en fonction du niveau de sensibilité, est obligatoire conformément aux textes règlementaires en vigueur.

4.3.4. GDB-PROT-IS : protection des informations

L'utilisateur doit protéger les informations qu'il est amené à manipuler dans le cadre de ses fonctions, selon leur sensibilité et tout au long de leur cycle de vie, depuis la création du brouillon jusqu'à son éventuelle destruction.

4.4. Intégration de la SSI dans le cycle de vie des systèmes d'information

Apprécier, traiter, et communiquer sur les risques relatifs à la sécurité des systèmes d'information.

4.4.1. INT-HOMOLOG-SSI : homologation de sécurité des systèmes d'information

Tout système d'information doit faire l'objet d'une décision d'homologation avant sa mise en exploitation dans les conditions d'emploi définies. L'homologation est l'acte selon lequel l'autorité d'emploi atteste formellement auprès des utilisateurs que le système d'information est protégé conformément aux objectifs de sécurité fixés. La décision d'homologation est prise par l'autorité d'homologation, après avis de la commission d'homologation mise en place à cet effet.

La décision d'homologation s'appuie sur une analyse de risques adaptée aux enjeux du système considéré, et précise les conditions d'emploi du système d'information.

Gérer dynamiquement les mesures de protection, tout au long de la vie du SI

4.4.2. INT-SSI : intégration de la sécurité dans les projets

La sécurité des systèmes d'information doit être prise en compte dans toutes les phases des projets informatiques, sous le contrôle de l'autorité d'homologation, de la conception et de la spécification du système jusqu'à son retrait du service.

4.4.3. INT-QUOT-SSI : mise en œuvre au quotidien de la SSI

La sécurité des systèmes d'information se traite au quotidien par des pratiques d'hygiène informatique. Des procédures écrites définissent les actes élémentaires du maintien en condition de sécurité lors des phases de conception, évolution ou retrait d'un système.

Utiliser des produits et services dont la sécurité est évaluée et attestée par l'AMSN, afin de renforcer la protection des systèmes d'information.

4.4.4. INT-AQ-PSL : acquisition de produits et services de confiance.

Lorsqu'ils sont disponibles, des produits ou des services de sécurité labellisés par l'AMSN doivent être utilisés.

Veiller aux exigences de sécurité lorsqu'il est fait appel à de la prestation par des tiers.

4.4.5. INT-PRES-CS : clauses de sécurité

Toute prestation dans le domaine des systèmes d'information est encadrée par des clauses de sécurité. Ces clauses spécifient les mesures de sécurité des systèmes d'information que le prestataire doit respecter dans le cadre de ses activités.

4.4.6. INT-PRES-CNTRL : suivi et contrôle des prestations fournies

Le maintien d'un niveau de sécurité au cours du temps nécessite un double contrôle :

- l'un, effectué périodiquement par l'équipe encadrant la prestation, qui porte sur les actions du sous-traitant et la conformité au cahier des charges ;
- l'autre, effectué par le RSSI ou le CSSI qui porte sur la pertinence du cahier des charges en amont des projets, la conformité des réponses apportées par le sous-traitant en phase de recette et le niveau de sécurité global obtenu en production.

4.4.7. INT-REX-AR : analyse de risques

Toute opération d'externalisation s'appuie sur une analyse de risques préalable, de façon à formaliser des objectifs de sécurité et définir des mesures adaptées. L'ensemble des objectifs de sécurité ainsi formalisés permet de définir une cible de sécurité servant de cadre au contrat établi avec le prestataire.

4.4.8. INT-REX-HB : hébergement

L'hébergement d'informations sensibles de l'Administration sur le territoire national est obligatoire, sauf accord du Ministre d'État après dérogation délivrée dans les conditions de l'article 2 du présent arrêté.

4.4.9. INT-REX-HS : hébergement et clauses de sécurité

Tout contrat d'hébergement détaille les dispositions mises en œuvre pour prendre en compte la sécurité des systèmes d'information. Ce sont notamment les mesures prises pour assurer le maintien en condition de sécurité des systèmes et permettre une gestion de crise efficace (conditions d'accès aux journaux, mise en place d'astreintes, etc.).

4.5. Sécurité physique des locaux abritant les SI

Inscrire la sécurisation physique des SI dans la sécurisation physique des locaux et dans les processus associés.

4.5.1. PHY-ZONES : découpage des sites en zones de sécurité

Un découpage des sites en zones physiques de sécurité doit être effectué, en liaison avec les services en charge : de l'immobilier, de la sécurité, de la Direction de la Sûreté Publique assistée par l'AMSN. Pour chaque zone de sécurité, des critères précis d'autorisation d'accès sont établis.

4.5.2. PHY-PUBL : accès réseau en zone d'accueil du public

Tout accès réseau installé dans une zone d'accueil du public doit être filtré ou isolé du reste du réseau informatique de l'entité.

4.5.3. PHY-SENS : protection des informations sensibles au sein des zones d'accueil du public

Le traitement d'informations sensibles au sein des zones d'accueil est à éviter. Si un tel traitement est strictement nécessaire, il doit rester ponctuel et exceptionnel. Des mesures particulières sont alors adoptées, notamment en matière de protection audiovisuelle, ainsi qu'en matière de protection des informations stockées sur les supports.

4.5.4. PHY-TECH : sécurité physique des locaux techniques

L'accès aux locaux techniques abritant des équipements d'alimentation et de distribution d'énergie, ou des équipements de réseau et de téléphonie, doit être physiquement protégé.

4.5.5. PHY-TELECOM : protection des câbles électriques et de télécommunications

Il convient de protéger le câblage réseau contre les dommages et les interceptions des communications qu'ils transmettent. En complément, les panneaux de raccordements et les salles des câbles doivent être placés en dehors des zones d'accueil du public et leur accès doit être contrôlé.

4.6. Sécurité physique des centres informatiques

Dimensionner les protections physiques des centres informatiques en fonction des enjeux liés à la concentration des moyens et données abrités.

4.6.1. PHY-CI-HEBERG : convention de service en cas d'hébergement tiers

Dans le cas où un tiers gère tout ou partie des locaux du centre informatique, une convention de service, définissant les responsabilités mutuelles en matière de sécurité, doit être établie entre ce tiers et l'entité ou le département. La gestion par un tiers de la sécurité du centre informatique doit avoir fait l'objet de la certification suivant la norme ISO 27001 et cette dernière doit être maintenue dans la durée.

4.6.2. PHY-CI-CTRLACC : contrôle d'accès physique aux zones internes et restreintes

L'accès aux zones internes (autorisées uniquement au personnel du centre informatique ou aux visiteurs accompagnés) et restreintes (autorisées aux seules personnes habilitées ou aux visiteurs accompagnés) doit reposer sur un dispositif de contrôle d'accès physique. Ce dispositif doit s'appuyer sur des produits qualifiés, lorsqu'ils sont disponibles, et bénéficier d'un maintien en condition de sécurité rigoureux.

4.6.3. PHY-CI-MOYENS : délivrance des moyens d'accès physique aux zones internes et restreintes

La délivrance des moyens d'accès physique doit respecter un processus formel permettant de s'assurer de l'identité de la personne, s'appuyant sur le processus d'arrivée et de départ du personnel. Le personnel autre que celui explicitement autorisé et habilité, mais néanmoins appelé à intervenir dans les zones sensibles (entretien ou réparation des bâtiments, des équipements non informatiques, nettoyage, visiteurs, …), intervient systématiquement et impérativement sous surveillance permanente.

4.6.4. PHY-CI-TRACE : traçabilité des accès aux zones internes et restreintes

Une traçabilité des accès, par les visiteurs externes, aux zones restreintes doit être mise en place. Ces traces sont alors conservées un an, dans le respect des textes protégeant les données personnelles.

4.6.5. PHY-CI-ENERGIE : règles de sécurité s'appliquant à l'énergie

L'alimentation secteur des équipements devra être conforme aux règles de l'art, de façon à se prémunir les atteintes à la sécurité des personnes et équipements liées à un défaut électrique.

4.6.6. PHY-CI-CLIM : règles de sécurité s'appliquant à la climatisation

Un dispositif de climatisation dimensionné en fonction des besoins énergétiques du système informatique doit être installé. Des procédures de réaction en cas de panne, connues du personnel, doivent être élaborées et vérifiées annuellement. Ces dispositions visent à prévenir toute surchauffe des équipements, pouvant engendrer une perte du service voire une détérioration du matériel.

4.6.7. PHY-CI-INC : règles de lutte contre l'incendie

L'installation de matériel de protection contre le feu est obligatoire. Des procédures de réaction à un incendie sont définies et régulièrement testées. Les salles techniques doivent être propres. Aucun carton, papier, ou autre source potentielle de départ de feu ne doit être entreposé dans ces locaux.

4.6.8. PHY-CI-EAU : règles de lutte contre les voies d'eau

Une étude sur les risques dus aux voies d'eau doit être réalisée. Cette étude doit notamment prendre en compte le risque de fuite sur un collecteur d'eau douce et les inondations dues aux intempéries.

4.7. Système d'information de sûreté

Traiter de manière globale la sécurité des systèmes d'information et de communication qui assurent la sûreté d'un site.

Les sites importants s'appuient sur des services supports des activités de sûreté physique. Dans ce cadre, l'appellation « services de systèmes d'information et de communication de sûreté » regroupe :

- les services support des activités de contrôle d'accès et détection d'intrusion (CTA), permettant au personnel de sûreté :
  - d'authentifier, d'autoriser et de tracer l'accès à une ressource physique (contrôle d'accès),
  - de détecter, d'alerter et de tracer en cas de tentative d'accès non autorisé (détection d'intrusion) ;
- les services support des activités de vidéosurveillance (VS), fournissant au personnel de sûreté un système de caméras disposées sur l'ensemble du site, de transport des flux vidéo, d'enregistrement, d'archivage et de visionnage de ces vidéos ;
- les services support de la gestion technique des bâtiments (GTB), permettant de superviser et de gérer l'ensemble des équipements des bâtiments du site, et d'avoir une vue globale de l'état de ces bâtiments ;
- les services support de la « sécurité incendie » (INC), regroupant l'ensemble des moyens informatiques mis en œuvre pour détecter, informer, intervenir et/ou évacuer tout ou partie du site en cas d'incendie.

4.7.1. PHY-SI-SUR : sécurisation du système d'information de sûreté

Pour les sites physiques considérés comme importants, des mesures de protection doivent être définies et appliquées en se basant sur les conclusions d'une analyse de risques. L'analyse de risques conduit à la désignation des briques essentielles dont il faut assurer la protection contre des actes malveillants. La gestion de la sécurité du système d'information de sûreté doit être documentée. L'emploi de produits labellisés, quand ils existent, est fortement recommandé.

4.8. Sécurité des réseaux

Utiliser les infrastructures nationales, en respectant les règles de sécurité qui leur sont attachées.

4.8.1. RES-MAITRISE : systèmes autorisés sur le réseau

Seuls les équipements gérés et configurés par les équipes informatiques habilitées peuvent être connectés au réseau local d'une entité.

4.8.2. RES-INTERCO : interconnexion avec des réseaux externes

Toute interconnexion entre les réseaux locaux d'une entité et un réseau externe (réseau d'un tiers, Internet, etc.) doit être réalisée via les infrastructures nationales. La décision d'interconnexion doit être motivée et validée lors de l'homologation.

4.8.3. RES-ENTSOR : mise en place de filtrage réseau pour les flux sortants et entrants

Dans l'optique de réduire les possibilités offertes à un attaquant, les connexions des machines du réseau interne vers l'extérieur doivent être filtrées.

4.8.4. RES-PROT : protection des informations

Dès lors que des informations sensibles doivent transiter sur des réseaux non maîtrisés, il convient de les protéger spécifiquement par chiffrement adapté.

Maîtriser les interconnexions de réseaux locaux. Configurer de manière adéquate les équipements de réseau actifs.

4.8.5. RES-CLOIS : cloisonner le SI en sous-réseaux de niveaux de sécurité homogènes

Par analogie avec le cloisonnement physique d'un bâtiment, le système d'information doit être segmenté selon des zones présentant chacune un niveau de sécurité homogène.

4.8.6. RES-INTERCOGEO : interconnexion des sites géographiques locaux d'une entité

L'interconnexion au niveau local de réseaux locaux d'une entité n'est possible que si la proximité géographique le justifie et sous réserve de la mise en place de connexions dédiées à cet effet, et de passerelles sécurisées et validées lors de l'homologation.

4.8.7. RES-RESS : cloisonnement des ressources en cas de partage de locaux

Dans le cas où une entité partage des locaux (bureaux ou locaux techniques) avec des entités externes, des mesures de cloisonnement des ressources informatiques doivent être mises en place. Si le cloisonnement n'est pas physique, les mesures prises doivent être validées lors de l'homologation.

Ne pas porter atteinte à la sécurité du SI par le déploiement d'accès non supervisés.

4.8.8. RES-INTERNET-SPECIFIQUE : cas particulier des accès spécifiques dans une entité

Les accès spécifiques à Internet nécessitant des droits particuliers pour un usage métier ne peuvent être mis en place que sur dérogation dûment justifiée, et sur des machines isolées physiquement et séparées du réseau de l'entité, après validation préalable de l'autorité d'homologation.

Maîtriser le déploiement, la configuration et l'usage des réseaux sans fil.

4.8.9. RES-SSFIL : mise en place de réseaux sans fil

Le déploiement de réseaux sans fil doit faire l'objet d'une analyse de risques spécifique. Les protections intrinsèques étant insuffisantes, des mesures complémentaires, validées lors de l'homologation, doivent être prises dans le cadre de la défense en profondeur. En particulier, une segmentation du réseau doit être mise en place de façon à limiter à un périmètre déterminé les conséquences d'une intrusion depuis la voie radio. À défaut de mise en œuvre de mesures spécifiques, le déploiement de réseaux sans fil sur des systèmes d'information manipulant des données sensibles est proscrit.

Configurer les mécanismes de commutation et de routage pour se protéger des attaques.

4.8.10. RES-COUCHBAS : implanter des mécanismes de protection contre les attaques sur les couches basses

Une attention particulière doit être apportée à l'implantation des protocoles de couches basses, de façon à se prémunir des attaques usuelles par saturation ou empoisonnement de cache. Cela concerne, par exemple, le protocole « Address Resolution Protocol » (ARP).

4.8.11. RES-ROUTDYN : surveiller les annonces de routage

Lorsque l'utilisation de protocoles de routage dynamiques est nécessaire, celle-ci doit s'accompagner de la mise en place d'une surveillance des annonces de routage, et de procédures permettant de réagir rapidement en cas d'incidents.

4.8.12. RES-ROUTDYN-IGP : configurer le protocole « Interior Gateway Protocol » (IGP) de manière sécurisée

Le protocole de routage dynamique de type IGP doit être activé exclusivement sur les interfaces nécessaires à la construction de la topologie du réseau et désactivé sur le reste des interfaces. La configuration du protocole de routage dynamique doit systématiquement s'accompagner d'un mot de passe de type MESSAGE-DIGEST-KEY.

4.8.13. RES-ROUTDYN-EGP : sécuriser les sessions « Exterior Gateway Protocol » (EGP)

Lors de la mise en place d'une session EGP avec un pair extérieur sur un média partagé, cette session doit s'accompagner d'un mot de passe de type message-digest-key.

4.8.14. RES-SECRET : modifier systématiquement les éléments d'authentification par défaut des équipements et services

Les mots de passe par défaut doivent être impérativement modifiés, de même en ce qui concerne les certificats. Les dispositions nécessaires doivent être prises auprès des fournisseurs de façon à pouvoir modifier les certificats installés par défaut.

4.8.15. RES-DURCI : durcir les configurations des équipements de réseaux

Les équipements de réseaux (comme les routeurs) doivent faire l'objet d'un durcissement spécifique comprenant notamment, outre le changement des mots de passe et certificats, la désactivation des interfaces et services inutiles, ainsi que la mise en place de mécanismes de protection du plan de contrôle.

Tenir à jour une cartographie détaillée et complète des réseaux et des interconnexions.

4.8.16. RES-CARTO : élaborer les documents d'architecture technique et fonctionnelle

L'architecture réseau du système d'information doit être décrite et formalisée à travers des schémas d'architecture, et des configurations, maintenus au fil des évolutions apportées au système d'information. Les documents d'architecture sont sensibles et font l'objet d'une protection adaptée. La cartographie réseau s'insère dans la cartographie globale des systèmes d'information.

4.9. Architecture des systèmes d'information

Appliquer les principes de défense en profondeur à l'architecture matérielle et logicielle des centres informatiques.

4.9.1. ARCHI-HEBERG : principes d'architecture de la zone d'hébergement

D'une manière générale, l'architecture des infrastructures des centres informatiques est conçue de façon à satisfaire l'ensemble des besoins en disponibilité, confidentialité, traçabilité et intégrité. Le principe de défense en profondeur doit être respecté, en particulier par la mise en œuvre successive d'environnements de sécurité en zone d'hébergement, de machines virtuelles ou physiques dédiées, de réseaux locaux virtuels (VLAN) appropriés, d'un filtrage strict des flux applicatifs et d'administration.

4.9.2. ARCHI-STOCKCI : architecture de stockage et de sauvegarde

Le réseau de stockage/sauvegarde pour les besoins des centres informatiques repose sur une architecture dédiée à cet effet.

4.9.3. ARCHI-PASS : passerelle Internet

Les interconnexions Internet passent obligatoirement par les passerelles homologuées.

4.10. Exploitation des SI

Définir et mettre en œuvre des mesures de protection renforcées pour les informations sensibles.

4.10.1. EXP-PROT-INF : protection des informations sensibles en confidentialité, en intégrité et en disponibilité

Des mesures doivent être mises en œuvre afin de garantir la protection des informations sensibles en confidentialité et en intégrité et en disponibilité. À défaut d'utilisation d'un réseau homologué, ces informations doivent être chiffrées à l'aide d'un moyen de chiffrement labellisé.

Durcir les configurations des ressources informatiques, et surveiller les interventions opérées sur celles-ci.

4.10.2. EXP-TRAC : traçabilité des interventions sur le système

Les interventions de maintenance sur les ressources informatiques de l'entité doivent être tracées par le service informatique concerné, et ces traces doivent être accessibles durant un an.

4.10.3. EXP-CONFIG : configuration des ressources informatiques

Les systèmes d'exploitation et les logiciels doivent faire l'objet d'un durcissement. Les configurations et mises à jour sont appliquées dans le strict respect des guides ou procédures en vigueur.

4.10.4. EXP-DOC-CONFIG : documentation des configurations

La configuration standard des ressources informatiques doit être documentée et mise à jour à chaque changement notable.

Authentifier les usagers et contrôler leurs accès aux ressources des SI des institutions officielles de la Principauté, en fonction d'une politique explicite d'autorisations.

4.10.5. EXP-ID-AUTH : identification, authentification et contrôle d'accès logique

L'accès à toute ressource non publique doit nécessiter une identification et une authentification individuelle de l'utilisateur. Dans le cas de l'accès à des données sensibles, des moyens d'authentification forte doivent être utilisés. A cette fin, l'usage d'une carte à puce doit être privilégié. Le contrôle d'accès doit être géré et s'appuyer sur un processus formalisé en cohérence avec la gestion des ressources humaines.

4.10.6. EXP-DROITS : droits d'accès aux ressources

Après avoir déterminé le niveau de sensibilité, le besoin de diffusion et de partage des ressources, les droits d'accès aux ressources doivent être gérés suivant les principes suivants : besoin d'en connaître (chaque utilisateur n'est autorisé à accéder qu'aux ressources pour lesquelles on lui accorde explicitement le bénéfice de l'accès), moindre privilège (chaque utilisateur accède aux ressources minimums de privilèges lui permettant de conduire les actions explicitement autorisées pour lui).

4.10.7. EXP-PROFILS : gestion des profils d'accès aux applications

Les applications manipulant des données sensibles doivent permettre une gestion fine par profils d'accès. Les principes du besoin d'en connaître et du moindre privilège s'appliquent.

4.10.8. EXP-PROC-AUTH : autorisations d'accès des utilisateurs

Toute action d'autorisation d'accès d'un utilisateur à une ressource des systèmes d'information doit s'inscrire dans le cadre d'un processus d'autorisation formalisé, qui s'appuie sur le processus d'arrivée et de départ du personnel.

4.10.9. EXP-REVUE-AUTH : revue des autorisations d'accès

Une revue des autorisations d'accès doit être réalisée annuellement sous le contrôle du RSSI.

4.10.10. EXP-CONF-AUTH : confidentialité des informations d'authentification

Les informations d'authentification (mots de passe d'accès aux systèmes d'information, clés privées liées aux certificats électroniques, etc.) doivent être considérées comme des données sensibles.

4.10.11. EXP-GEST-PASS : gestion des mots de passe

Les utilisateurs ne doivent pas stocker leurs mots de passe en clair (par exemple dans un fichier) sur leur poste de travail. Les mots de passe ne doivent pas transiter en clair sur les réseaux.

4.10.12. EXP-INIT-PASS : initialisation des mots de passe

Chaque compte utilisateur doit être créé avec un mot de passe initial aléatoire unique. Si les circonstances l'imposent, un mot de passe plus simple mais à usage unique peut être envisagé.

4.10.13. EXP-POL-PASS : politiques de mots de passe

Les règles de gestion et de protection des mots de passe donnant accès aux applications et infrastructures doivent être respectées dans chaque entité. Les politiques d'application du RSSI doivent être appliquées pour tous les comptes.

4.10.14. EXP-QUAL-PASS : contrôle systématique de la qualité des mots de passe

Des moyens techniques permettant d'imposer la politique de mots de passe (par exemple pour s'assurer du respect de l'éventuelle obligation relative à l'usage de caractères spéciaux) doivent être mis en place.

4.10.15. EXP-SEQ-ADMIN : séquestre des identifiants et mots de passe « administrateur »

Les identifiants et mots de passe permettant l'administration des ressources des systèmes d'information doivent être placés sous séquestre et tenus à jour, dans un coffre ou une armoire fermée à clé. L'authentifié doit être informé de l'existence de ces opérations de gestion, de leurs finalités et limites. Tout accès d'administration à une ressource informatique doit pouvoir être tracé et permettre de remonter à la personne exerçant ce droit. Les informations d'authentification bénéficiant d'un moyen de protection physique (notamment carte à puce) n'ont, par défaut, pas besoin d'être l'objet d'opérations de séquestre de la part d'autres personnels que l'authentifié lui-même.

4.10.16. EXP-POL-ADMIN : politique de mots de passe « administrateur »

Chaque administrateur doit disposer d'un mot de passe propre et destiné à l'administration.

4.10.17. EXP-DEP-ADMIN : gestion du départ d'un administrateur des systèmes d'information

En cas de départ d'un administrateur disposant de privilèges sur des composants des systèmes d'information, les comptes individuels dont il disposait doivent être immédiatement désactivés. Les éventuels mots de passe d'administration dont il avait connaissance doivent être changés (exemples : mots de passe des comptes fonctionnels, comptes génériques ou comptes de service utilisés dans le cadre des fonctions de l'administrateur).

Fournir aux administrateurs les outils nécessaires à l'exercice des tâches SSI et configurer ces outils de manière sécurisée.

4.10.18. EXP-RESTR-DROITS : restriction des droits d'administration

Sauf exception dûment motivée et validée par le RSSI, les utilisateurs n'ont pas de droits d'administration.

4.10.19. EXP-PROT-ADMIN : protection des accès aux outils d'administration

L'accès aux outils et interfaces d'administration doit être strictement limité aux personnes habilitées, selon une procédure formelle d'autorisation d'accès.

4.10.20. EXP-HABILIT-ADMIN : habilitation des administrateurs

L'habilitation des administrateurs s'effectue conformément à l'article 7 du présent arrêté. Le nombre de personnes habilitées pour des opérations d'administration doit être connu et validé par l'autorité d'homologation.

4.10.21. EXP-GEST-ADMIN : gestion des actions d'administration

Les opérations d'administration doivent être tracées de manière à pouvoir gérer au niveau individuel l'imputabilité des actions d'administration.

4.10.22. EXP-SEC-FLUXADMIN : sécurisation des flux d'administration

Les opérations d'administration sur les ressources informatique doivent s'appuyer sur des protocoles sécurisés. Un réseau dédié à l'administration des équipements, ou au moins un réseau logiquement séparé de celui des utilisateurs, doit être utilisé. Les postes d'administrateurs doivent être dédiés et ne doivent pas pouvoir accéder à Internet.

4.10.23. EXP-CENTRAL : centraliser la gestion du système d'information

Afin de gérer efficacement un grand nombre de postes d'utilisateurs, de serveurs ou d'équipements réseau, les administrateurs doivent utiliser des outils centralisés, permettant l'automatisation de traitements quotidiens et offrant une vue globale et pertinente sur le système d'information.

4.10.24. EXP-SECX-DIST : sécurisation des outils de prise de main à distance

La prise de main à distance d'une ressource informatique ne doit être réalisable :

- que par les fonctionnaires, agents publics ou préposés des services publics habilités chargés de l'administration des systèmes d'information, sur les ressources informatiques de leur périmètre ;
- qu'avec la validation préalable et explicite de l'utilisateur.

A cet effet, des mesures de sécurité spécifiques doivent être définies et respectées.

4.10.25. EXP-DOM-POL : définir une politique de gestion des comptes du domaine

Une politique explicite de gestion des comptes du domaine doit être documentée.

4.10.26. EXP-DOM-PASS : configurer la stratégie des mots de passe des domaines

La politique de gestion des mots de passe doit être conçue de façon à protéger contre les attaques par essais successifs de mots de passe. Une complexité minimale dans le choix des mots de passe doit être imposée aux utilisateurs.

4.10.27. EXP-DOM-NOMENCLAT : définir et appliquer une nomenclature des comptes du domaine

La gestion des comptes doit s'appuyer sur une nomenclature adaptée, afin de pouvoir distinguer selon leur usage : comptes d'utilisateur standard, comptes d'administration (domaine, serveurs, postes de travail) et comptes de service.

4.10.28. EXP-DOM-RESTADMIN : restreindre au maximum l'appartenance aux groupes d'administration du domaine

L'appartenance aux groupes du domaine ADMINISTRATEURS DE L'ENTREPRISE et ADMINISTRATEURS DU DOMAINE n'est nécessaire que dans de très rares cas. Les opérations les plus courantes doivent être effectuées avec des comptes du domaine membres des groupes locaux d'administration des ordinateurs ou ayant une délégation d'administration.

4.10.29. EXP-DOM-SERV : maîtriser l'utilisation des comptes de service

Les comptes de service ont la particularité d'avoir généralement leurs mots de passe inscrits en dur dans des applications ou dans des systèmes. Afin de pouvoir être en mesure de changer ces mots de passe en urgence, il est nécessaire de maîtriser leur utilisation.

4.10.30. EXP-DOM-LIMITSERV : limiter les droits des comptes de service

Les comptes de service doivent faire l'objet d'une restriction des droits, en suivant le principe du moindre privilège.

4.10.31. EXP-DOM-OBSOLET : désactiver les comptes du domaine obsolètes

Il est nécessaire de désactiver immédiatement, voire de supprimer, les comptes obsolètes, que ce soient des comptes d'utilisateur (administrateur, de service ou utilisateur standard) ou des comptes de machine.

4.10.32. EXP-DOM-ADMINLOC : améliorer la gestion des comptes d'administrateur locaux

Afin d'empêcher la réutilisation des empreintes d'un compte utilisateur local d'une machine à une autre, il faut soit utiliser des mots de passe différents pour les comptes d'administration, soit interdire la connexion à distance via ces comptes.

4.10.33. EXP-MAINT-EXT : maintenance externe

Les données non chiffrées doivent être effacées avant l'envoi en maintenance externe de toute ressource informatique. Les opérations de chiffrement doivent faire appel à des produits certifiés, qualifiés ou respectant des normes reconnues. L'effacement des données sensibles doit s'appuyer sur des produits qualifiés, ou respecter des procédures établies en concertation avec l'AMSN.

4.10.34. EXP-MIS-REB : mise au rebut

Lorsqu'une ressource informatique est amenée à quitter définitivement l'entité, les données présentes sur les disques durs ou la mémoire intégrée doivent être effacées de manière sécurisée.

L'effacement des données sensibles doit s'appuyer sur des produits qualifiés, certifiés, ou respecter des normes reconnues. Les disques doivent ensuite être détruis conformément aux exigences de la norme DIN 66399 classe 2, niveau 5. Si les ressources informatiques contenaient des données sensibles la norme DIN 66399 classe 3, niveau 6 s'applique. Un procès-verbal de destruction doit être établi par le prestataire à l'origine de la destruction puis conservé par l'entité.

4.10.35. EXP-PROT-MALV : protection contre les codes malveillants

Des logiciels de protection contre les codes malveillants, appelés communément antivirus, doivent être installés sur l'ensemble des serveurs d'interconnexion, serveurs applicatifs et postes de travail de l'entité. Ces logiciels de protection doivent être distincts pour ces trois catégories au moins, et le dépouillement de leurs journaux doit être corrélé.

4.10.36. EXP-GES-EVTSEC : gestion des événements de sécurité

Les événements de sécurité des systèmes, des serveurs et des postes de travail doivent être centralisés et dans un format harmonisé pour permettre une détection rapide et une investigation efficace (tentatives d'intrusion, infection virale, tentatives de connexion infructueuses, campagnes de spam, etc).

4.10.37. EXP-MAJ-ANTIVIR : mise à jour de la base de signatures

Les mises à jour des bases antivirales et des moteurs d'antivirus doivent être déployées automatiquement sur les serveurs et les postes de travail.

4.10.38. EXP-NAVIG : configuration du navigateur Internet

Le navigateur déployé par l'équipe chargée des systèmes d'information sur l'ensemble des serveurs et des postes de travail nécessitant un accès Internet ou Intranet doit être configuré de manière sécurisée (désactivation des services inutiles, nettoyage du magasin de certificats, etc.).

4.10.39. EXP-POL-COR : définir et mettre en œuvre une politique de suivi et d'application des correctifs de sécurité

Le maintien dans le temps du niveau de sécurité d'un système d'information impose une gestion organisée et adaptée des mises à jour de sécurité. Un processus de gestion des correctifs propre à chaque système ou applicatif doit être défini, et adapté suivant les contraintes et le niveau d'exposition du système.

4.10.40. EXP-COR-SEC : déploiement des correctifs de sécurité

Les correctifs de sécurité des ressources informatiques locales doivent être déployés par l'équipe chargée des systèmes d'information en s'appuyant sur des outils de gestion centralisée.

4.10.41. EXP-OBSOLET : assurer la migration des systèmes obsolètes

L'ensemble des logiciels utilisés sur le système d'information doit être dans une version pour laquelle l'éditeur assure le support, et tenu à jour. En cas de défaillance du support, il convient d'en étudier l'impact et de prendre les mesures adaptées.

4.10.42. EXP-ISOL : isoler les systèmes obsolètes restants

Il est nécessaire d'isoler les systèmes obsolètes, gardés volontairement pour assurer un maintien en condition opérationnelle des projets, et pour lesquels une migration n'est pas envisageable. Chaque fois que cela est possible, cette isolation doit être effectuée au niveau du réseau (filtrage strict), des éléments d'authentification (qui ne doivent pas être communs avec le reste du SI) et des applications (pas de ressources partagées avec le reste du SI).

4.10.43. EXP-JOUR-SUR : journalisation des alertes

Chaque système doit disposer de dispositifs de journalisation permettant de conserver une trace des événements de sécurité. Ces traces doivent être conservées de manière sûre.

4.10.44. EXP-POL-JOUR : définir et mettre en œuvre une politique de gestion et d'analyse des journaux de traces

Une politique de gestion et d'analyse des journaux d'événements de sécurité est définie par le RSSI, validée par l'autorité et mise en œuvre. Celle-ci doit contenir un plan de collecte, de centralisation et d'archivage des traces d'une part, et la définition d'un dispositif organisationnel et technique assurant une analyse de celles-ci (contextualisation et enrichissement des traces, corrélation, alertes ou rapports).

4.10.45. EXP-CONS-JOUR : conservation des journaux

Les journaux des événements de sécurité doivent être conservés sur douze mois glissants, hors contraintes légales et réglementaires particulières imposant des durées de conservation spécifiques.

Défendre les systèmes d'information nécessite une vigilance de tous, et des actions permanentes.

4.10.46. EXP-GES-DYN : gestion dynamique de la sécurité

L'équipe en charge de la sécurité des systèmes d'information doit procéder, notamment via l'analyse des journaux, à la surveillance des comportements anormaux au sein du système d'information, et à la surveillance des flux d'entrée et de sortie du système d'information.

4.10.47. EXP-MAIT-MAT : maîtrise des matériels

Les postes de travail - y compris dans le cas d'une location - sont fournis à l'utilisateur par l'entité, gérés et configurés sous la responsabilité de l'entité. La connexion d'équipements non maîtrisés, non administrés ou non mis à jour par l'entité (qu'il s'agisse d'ordiphones, d'équipements informatiques nomades et fixes ou de supports de stockage amovibles) sur des équipements et des réseaux professionnels est interdite.

4.10.48. EXP-PROT-VOL : rappel des mesures de protection contre le vol

Les postes fixes bénéficient des mesures de protection physique offertes au titre de la directive de sécurité physique de la présente PSSI-E. Chaque utilisateur doit veiller à la sécurité des supports amovibles (clés USB et disques amovibles), notamment en les conservant dans un endroit sûr. Les données professionnelles contenues sur ces supports doivent être chiffrée. Les supports contenant des données sensibles doivent être stockés dans des meubles fermant à clef.

4.10.49. EXP-DECLAR-VOL : déclarer les pertes et vols

Toute perte ou vol d'une ressource d'un système d'information doit être signalée au RSSI et déclarée à l'AMSN à l'aide du *formulaire de déclaration d'incident* disponible et téléchargeable sur https://amsn.gouv.mc/OIV/.

4.10.50. EXP-REAFFECT : réaffectation de matériels informatiques

Une procédure de gestion des postes et supports dans le cadre de départs de personnel ou de réaffectations à de nouveaux utilisateurs doit être mise en place et validée par le RSSI. Elle doit définir les conditions de recours à un effacement des données.

4.10.51. EXP-NOMAD-SENS : déclaration des équipements nomades aptes à traiter des informations sensibles

L'autorité d'homologation du système d'information valide les usages possibles des équipements nomades vis-à-vis du traitement des informations sensibles ; les usages non explicitement autorisés sont interdits.

4.10.52. EXP-ACC-DIST : accès à distance au système d'information de l'organisme

Les utilisateurs distants doivent s'authentifier sur le réseau de l'entité.

4.10.53. EXP-IMP-SENS : impression des informations sensibles

Les impressions d'informations sensibles doivent être effectuées selon une procédure prédéfinie, garantissant le contrôle de l'utilisateur, du déclenchement de l'impression jusqu'à la récupération du support imprimé.

4.10.54. EXP-IMP-2 : sécurité des imprimantes et copieurs multifonctions

Les imprimantes et copieurs multifonctions sont des ressources informatiques à part entière qui doivent être gérées en tant que telles. Elles ne doivent pas pouvoir communiquer avec l'extérieur sauf pour la réalisation d'opérations de télémaintenance. Lorsqu'elles sont connectées à des systèmes d'information sensibles, la télémaintenance doit être désactivée et les opérations de maintenance doivent se faire sur site en présence d'un administrateur.

Exploiter de manière sécurisée les centres informatiques en s'appuyant sur des procédures adaptées et sur la maîtrise des outils de supervision.

Les règles suivantes sont présentées selon le modèle qui structure l'architecture des applications selon trois Tiers (Présentation - Application - Données).

4.10.55. EXP-CI-OS : systèmes d'exploitation

Les systèmes d'exploitation déployés doivent faire l'objet d'un support valide de la part d'un éditeur ou d'un prestataire de service. Seuls les services et applications nécessaires sont installés, de façon à réduire la surface d'attaque. Une attention particulière doit être apportée aux comptes administrateurs.

4.10.56. EXP-CI-PROTFIC : passerelle d'échange de fichiers

Les échanges de fichiers entre applications doivent privilégier les protocoles sécurisés (SSL/TLS, FTPS...).

4.10.57. EXP-CI-FILT : filtrage des flux applicatifs

De façon à garantir un niveau de sécurité satisfaisant face aux attaques informatiques, des mécanismes de filtrage et de cloisonnement doivent être mis en œuvre.

4.10.58. EXP-CI-ADMIN : flux d'administration

D'une manière générale, il convient de différencier deux types de flux d'administration : les flux d'administration de l'infrastructure (réservés aux agents du centre informatique) d'une part, les flux d'administration des applications métier (réservés à la direction métier) d'autre part. L'attribution des droits d'administration doit respecter cette différenciation, et les 2 types de flux d'administration doivent être dans la mesure du possible cloisonnés.

4.10.59. EXP-CI-DNS : service de noms de domaine - DNS technique

Dans le cas du déploiement d'un serveur de noms de domaines pour les besoins techniques internes au centre informatique, les extensions sécurisées DNSSEC peuvent être utilisées.

4.10.60. EXP-CI-DESTR : destruction de support

La fin de vie d'un support de stockage ou d'un matériel embarquant un support de stockage (imprimante, routeur, commutateur, …) doit s'accompagner d'une opération de destruction du support de stockage avant remise du matériel au constructeur.

4.10.61. EXP-CI-TRAC : traçabilité / imputabilité

Afin d'assurer une cohérence dans les échanges entre applications ainsi qu'une traçabilité pertinente des événements techniques et de sécurité, les centres d'exploitation emploient une référence de temps commune (service NTP, Network Time Protocol).

4.10.62. EXP-CI-SUPERVIS : supervision

Un cloisonnement entre les flux de supervision (remontée d'informations) et les flux d'administration (commandes, mises à jour) doit être mis en place.

4.11. Sécurité du poste de travail

Durcir les configurations des postes de travail en protégeant les utilisateurs.

4.11.1. PDT-GEST : fourniture et gestion des postes de travail

Les postes de travail utilisés dans le cadre professionnel sont fournis et gérés par l'équipe chargée des SI.

4.11.2. PDT-VEROUIL-FIXE : verrouillage de l'unité centrale des postes fixes

Lorsque l'unité centrale d'un poste fixe est peu volumineuse, donc susceptible d'être facilement emportée, elle doit être protégée contre le vol par un système d'attache (par exemple un câble antivol).

4.11.3. PDT-VEROUIL-PORT : verrouillage des postes portables

Un câble physique de sécurité doit être fourni avec chaque poste portable. Les utilisateurs doivent être sensibilisés à son utilisation.

4.11.4. PDT-REAFFECT : réaffectation du poste de travail

Une procédure définit les règles concernant le traitement à appliquer aux informations ayant été stockées ou manipulées sur les postes réaffectés.

4.11.5. PDT-PRIVIL : privilèges des utilisateurs sur les postes de travail

La gestion des privilèges des utilisateurs sur leurs postes de travail doit suivre le principe du « moindre privilège » : chaque utilisateur ne doit disposer que des privilèges nécessaires à la conduite des actions relevant de sa mission.

4.11.6. PDT-PRIV : utilisation des privilèges d'accès « administrateur »

Les privilèges d'accès « administrateur » doivent être utilisés uniquement pour les actions d'administration le nécessitant.

4.11.7. PDT-ADM-LOCAL : gestion du compte « administrateur local »

L'accès au compte « administrateur local » sur les postes de travail doit être strictement limité aux équipes en charge de l'exploitation et du support sur ces postes de travail.

4.11.8. PDT-STOCK : stockage des informations

Dans la mesure du possible, les données traitées par les utilisateurs doivent être stockées sur des espaces réseau, eux-mêmes sauvegardés selon les exigences des entités et en accord avec les règles de sécurité en vigueur.

4.11.9. PDT-SAUV-LOC : sauvegarde / synchronisation des données locales

Dans le cas où des données doivent être stockées en local sur le poste de travail, des moyens de synchronisation ou de sauvegarde doivent être fournis aux utilisateurs.

4.11.10. PDT-SUPPR-PART : suppression des données sur les postes partagés

Les données présentes sur les postes partagés (portable de prêt, par exemple) doivent être supprimées entre deux utilisations, dès lors que les utilisateurs ne disposent pas du même besoin d'en connaître.

4.11.11. PDT-CHIFF-SENS : chiffrement des données sensibles

Une solution de chiffrement doit être mise à disposition des utilisateurs et des administrateurs afin de chiffrer les données sensibles stockées sur les postes de travail, les serveurs, les espaces de travail, ou les supports amovibles, conformément aux arrêtés ministériels n° 2018-635, n° 2018-636 et n° 2018-637 pris en application du Règlement Général de Sécurité de la Principauté, Arrêté Ministériel n° 2020-461 du 6 juillet 2020 portant application de l'article 13 de l'Ordonnance Souveraine n° 8.099 du 16 juin 2020 fixant les conditions d'application de la loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée, relative aux services de confiance.

4.11.12. PDT-AMOV : fourniture de supports de stockage amovibles

Les supports de stockage amovibles (clés USB et disque durs externes, notamment) doivent être fournis aux utilisateurs par le gestionnaire des systèmes d'information.

4.11.13. PDT-NOMAD-ACCESS : accès à distance aux systèmes d'information de l'entité

Les accès à distance aux systèmes d'information (accès dits « nomades ») doivent être réalisés via les infrastructures nationales. Lorsque l'accès à distance utilise d'autres infrastructures, l'usage de réseaux privés virtuels (VPN) de confiance est nécessaire.

4.11.14. PDT-NOMAD-STOCK : stockage local d'information sur les postes nomades

Le stockage local d'information sur les postes de travail nomades doit être limité au strict nécessaire. Les informations sensibles doivent être obligatoirement chiffrées par un moyen de chiffrement labellisé.

4.11.15. PDT-NOMAD-FILT : filtre de confidentialité

Pour les postes de travail nomades manipulant des données sensibles, un filtre de confidentialité doit être fourni et être positionné sur l'écran dès lors que le poste est utilisé en dehors de l'entité.

4.11.16. PDT-NOMAD-CONNEX : configuration des interfaces de connexion sans fil

La configuration des interfaces de connexion sans fil doit interdire les usages dangereux de ces interfaces.

4.11.17. PDT-NOMAD-DESACTIV : désactivation des interfaces de connexion sans fil

Des règles de configuration des interfaces de connexion sans fil (Wifi, Bluetooth, 4G, 5G…), permettant d'interdire les usages non maîtrisés et d'éviter les intrusions via ces interfaces, doivent être appliquées.

Les interfaces sans fil ne doivent être activées qu'en cas de besoin.

Paramétrer les imprimantes et copieurs multifonctions afin de diminuer leur surface d'attaque.

4.11.18. PDT-MUL-DURCISS : durcissement des imprimantes et copieurs multifonctions

Les imprimantes et copieurs multifonctions hébergés localement dans une entité doivent faire l'objet d'un durcissement en termes de sécurité : changement des mots de passe initialement fixés par le « constructeur », désactivation des interfaces réseau inutiles, suppression des services inutiles, chiffrement des données sur le disque dur lorsque cette fonctionnalité est disponible, configuration réseau statique.

4.11.19. PDT-MUL-SECNUM : sécurisation de la fonction de numérisation

Lorsqu'elle est activée, la fonction de numérisation sur les copieurs multifonctions hébergés dans une entité doit être sécurisée. Les mesures de sécurité suivantes doivent notamment être appliquées : envoi de documents uniquement à destination d'une adresse de messagerie interne à l'entité, envoi uniquement à une seule adresse de messagerie.

Sécuriser la téléphonie pour protéger les utilisateurs contre des attaques malveillantes.

4.11.20. PDT-TEL-MINIM : sécuriser la configuration des autocommutateurs

Les autocommutateurs doivent être maintenus à jour au niveau des correctifs de sécurité. Leur configuration doit être durcie. La définition et l'affectation des droits d'accès et des privilèges aux utilisateurs (transfert départ-départ, entrée en tiers, interphonie, autorisation de déblocage, renvoi sur numéro extérieur, substitution, substitution de privilège, interception d'appel dirigé, etc.) doivent faire l'objet d'une attention particulière. Une revue de la programmation téléphonique doit être organisée périodiquement.

4.11.21. PDT-TEL-CODES : codes d'accès téléphoniques

Il est nécessaire de sensibiliser les utilisateurs au besoin de modifier le code d'accès de leur téléphone et de leur messagerie vocale.

4.11.22. PDT-TEL-DECT : limiter l'utilisation du DECT

Les communications réalisées au travers du protocole DECT sont susceptibles d'être interceptées, même si les mécanismes d'authentification et de chiffrement que propose ce protocole sont activés. Il est recommandé d'attribuer des postes téléphoniques filaires aux utilisateurs dont les échanges sont les plus sensibles.

Contrôler régulièrement la conformité des paramétrages de sécurité appliqués aux postes de travail.

4.11.23. PDT-CONF-VERIF : utiliser des outils de vérification automatique de la conformité

Un outil de vérification régulière de la conformité des éléments de configuration des postes de travail doit être mis en place, afin d'éviter une dérive dans le temps de ces éléments de configuration.

4.12. Sécurité du développement des systèmes

Reconnaître la sécurité comme une fonction essentielle, et la prendre en compte dès la conception des projets.

4.12.1. DEV-INTEGR-SECLOC : intégrer la sécurité dans les développements locaux

Toute initiative locale de développement informatique doit respecter les exigences nationales en matière de sécurité des systèmes d'information, concernant la prise en compte de la sécurité dans les projets et les développements informatiques. Le service à l'origine du projet se porte garant de l'application du référentiel général de sécurité de la Principauté annexé à l'arrêté ministériel n° 2020-461 du 6 juillet 2020, et de l'application d'une démarche d'homologation du système. S'agissant de développement en langage C ou RUST, il est demandé de suivre les préconisations des guides de bonnes pratiques notamment ceux de l'ANSSI :

https://www.ssi.gouv.fr/guide/regles-de-programmation-pour-le-developpement-securise-de-logiciels-en-langage-c/ ;

https://www.ssi.gouv.fr/administration/guide/regles-de-programmation-pour-le-developpement-dapplications-securisees-en-rust/.

4.12.2. DEV-SOUS-TRAIT : intégrer des clauses de sécurité dans les contrats de sous-traitance de développement informatique

Lors de l'écriture d'un contrat de sous-traitance de développement, plusieurs clauses relatives à la sécurité des systèmes d'information doivent être intégrées :

- formation obligatoire des développeurs sur le développement sécurisé et sur les vulnérabilités classiques ;
- utilisation obligatoire d'outils permettant de minimiser les erreurs introduites durant le développement (outils gratuits d'analyse statique de code, utilisation de bibliothèques réputées pour leur sécurité, etc.) ;
- production de documentation technique décrivant l'implantation des protections développées (gestion de l'authentification, stockage des mots de passe, gestion des droits, chiffrement, etc.) ;
- respect de normes de développement sécurisé, qu'elles soient propres au développeur, publiques ou propres au commanditaire ;
- obligation pour le prestataire de corriger, dans un temps raisonnable et pour un prix défini, les vulnérabilités introduites durant le développement et qui lui sont remontées, en incluant automatiquement les corrections des autres occurrences des mêmes erreurs de programmation.

Mener les développements logiciels selon une méthodologie de sécurisation du code produit.

4.12.3. DEV-FUITES : limiter les fuites d'information

Les fuites d'informations techniques sur les logiciels utilisés permettent aux attaquants de déceler plus facilement d'éventuelles vulnérabilités. Il est impératif de limiter fortement la diffusion d'informations au sujet des produits utilisés, même si cette précaution ne constitue pas une protection en tant que telle.

4.12.4. DEV-LOG-ADHER : réduire l'adhérence des applications à des produits ou technologies spécifiques

Le fonctionnement d'une application s'appuie sur un environnement logiciel et matériel. En phases de conception et de spécification technique, il est nécessaire de s'assurer que les applications n'ont pas une trop forte adhérence vis-à-vis des environnements sur lesquels elles reposent. En effet, l'apparition de failles sur un environnement a de fait un impact sur la sécurité des applications qui en dépendent. En plus du maintien en condition de sécurité propre à l'application, il est donc nécessaire de pouvoir faire évoluer son environnement pour garantir sa sécurité dans la durée.

4.12.5. DEV-LOG-CRIT : instaurer des critères de développement sécurisé

Une fois passées les phases de définition des besoins et de conception de l'architecture applicative, le niveau de sécurité d'une application dépend fortement des modalités pratiques suivies lors de sa phase de développement.

4.12.6. DEV-LOG-CYCLE : intégrer la sécurité dans le cycle de vie logiciel

La sécurité doit être intégrée à toutes les étapes du cycle de vie du projet, depuis l'expression des besoins jusqu'à la maintenance applicative, en passant par la rédaction du cahier des charges et les phases de recette.

4.12.7. DEV-LOG-WEB : améliorer la prise en compte de la sécurité dans les développements Web

Les développements Web (et les développements en PHP en particulier) font l'objet de problèmes de sécurité récurrents qui ont conduit à la constitution de référentiels de sécurité.

Ces référentiels ont pour objectif de fixer des règles de bonnes pratiques à l'usage des développeurs. Ce sont des règles d'ordre générique ou pouvant être spécifiques à un langage (PHP, ASP, NET, etc.).

4.12.8. DEV-LOG-PASS : calculer les empreintes de mots de passe de manière sécurisée

Lorsqu'une application doit stocker les mots de passe de ses utilisateurs, il est important de mettre en œuvre des mesures permettant de se prémunir contre les attaques documentées : attaques par dictionnaire, attaques par tables arc-en-ciel, attaques par force brute, etc.

Accompagner le développement sécurisé d'applications à risques par des contre-mesures minimisant l'impact d'attaques nouvelles.

4.12.9. DEV-FILT-APPL : mettre en œuvre des fonctionnalités de filtrage applicatif pour les applications à risque

Devant les applications à risques, il est recommandé de faire usage d'une solution tierce de filtrage applicatif.

4.13. Traitement des incidents

Partager l'information (alertes, incidents) dans le respect des règles de prudence et mutualiser les opérations de remise en état, de façon à lutter efficacement contre les attaques.

4.13.1. TI-OPS-SSI : chaînes opérationnelles de la sécurité des systèmes d'information

La gestion des alertes et des incidents est réalisée selon des procédures testées lors d'exercices. La coordination des compétences est organisée à l'échelon national par l'AMSN. Les situations d'urgence peuvent faire appel à des mesures définies préalablement dans le cadre des plans gouvernementaux.

4.13.2. TI-MOB : mobilisation en cas d'alerte

En cas d'alerte de sécurité identifiée au niveau national, le RSSI et les CSSI s'assurent de la bonne application des exigences formulées par les instances nationales, dans les meilleurs délais.

4.13.3. TI-QUAL-TRAIT : qualification et traitement des incidents

L'AMSN, le RSSI et la chaîne hiérarchique sont informés de tout incident de sécurité. L'AMSN assure la qualification de l'incident et le pilotage de son traitement.

4.13.4. TI-INC-REM : remontée des incidents

Tout incident de sécurité, même apparemment mineur, dont l'impact dépasse ou est susceptible de dépasser le système d'information d'une entité ou d'un département, fait l'objet d'un compte-rendu au centre opérationnel de la sécurité des systèmes d'information (CERT-MC) de l'AMSN à travers le formulaire disponible et téléchargeable en ligne sur le site de l'AMSN : https://amsn.gouv.mc/OIV/.

Cette remontée est immédiate pour les incidents dont la portée est susceptible de dépasser à court terme le périmètre de l'entité ou du département, et pour les incidents correspondant à des signalements spécifiques, notamment de la part de l'AMSN. La remontée prend la forme d'une synthèse mensuelle pour les autres incidents.

Chaque entité doit maintenir à jour un historique clair des suites liées à l'escalade de chaque incident, afin de capitaliser les enseignements associés à la résolution (ou non) de ces incidents.

L'aspect difficile de la caractérisation des attaques (ambiguïté de la source, du dommage, du moyen, de la finalité) rend nécessaire les échanges d'informations - même sur des « signaux faibles » - ainsi que la coordination continue des actions.

4.14. Continuité d'activité

Se doter de plans de continuité d'activité, et les tester.

4.14.1. PCA-DEP : définition du plan de continuité d'activité des systèmes d'information

Un plan de continuité d'activité des systèmes d'information permettant d'assurer, en cas de sinistre, la continuité d'activité des systèmes d'information doit être défini.

4.14.2. PCA-SUIVI : suivi de la mise en œuvre du plan de continuité d'activité des systèmes d'information (PCA des SI)

Le RSSI s'assure de la bonne mise en œuvre des dispositions prévues dans le plan de continuité d'activité des systèmes d'information.

4.14.3. PCA-PROC : mise en œuvre des dispositifs techniques et des procédures opérationnelles

Les équipes informatiques mettent en œuvre les dispositifs techniques et les procédures opérationnelles contribuant à la continuité des systèmes d'information, en assurent la supervision au quotidien et la maintenance dans le temps.

4.14.4. PCA-SAUVE : protection de la disponibilité des sauvegardes

Les sauvegardes de données ne doivent pas être soumises aux mêmes risques de sinistres que les données sauvegardées.

4.14.5. PCA-PROT : protection de la confidentialité des sauvegardes

Les sauvegardes doivent être traitées de manière à garantir leur confidentialité et leur intégrité.

4.14.6. PCA-EXERC : exercice régulier du plan de continuité d'activité des systèmes d'information

Le RSSI organise des exercices réguliers, afin de tester le plan de continuité d'activité des systèmes d'information.

4.14.7. PCA-MISAJOUR : mise à jour du plan de continuité d'activité des systèmes d'information

Le RSSI assure le maintien à jour du plan de continuité d'activité des systèmes d'information.

4.15. Conformité, audit, inspection, contrôle

Effectuer des contrôles (audits, inspections) et des exercices réguliers de façon à mesurer les progrès accomplis et corriger les manquements.

4.15.1. CONTR-SSI : contrôles locaux

La conformité à la PSSI-E est vérifiée par des contrôles réguliers. Le RSSI conduit des actions d'évaluation de la conformité à la PSSI-E et contribue à la consolidation de l'état d'avancement de sa mise en œuvre.

4.15.2. CONTR-OPS : contrôles opérationnels de sécurité

Des contrôles opérationnels de sécurité sont réalisés régulièrement par l'entité, sur les systèmes clés contribuant à la sécurité du système d'information (systèmes de filtrage réseau, annuaires et gestion des droits, configurations des serveurs, configuration des applications à fort besoin d'intégrité...). Les résultats sont analysés pour en déterminer les actions préventives/correctives et sont communiqués au RSSI.

4.15.3. CONTR-BILAN-SSI : bilan annuel

Les services établissent un bilan annuel mesurant leur maturité en termes de sécurité des systèmes d'information globale. L'Agence Monégasque de Sécurité Numérique consolide l'ensemble de ces bilans à l'effet de remettre ce document de synthèse au Ministre d'État, aux Conseillers de Gouvernement - Ministres et au RSSI.

Annexe 2 - Clauses contractuelles liées à la sécurité des systèmes d'information

Tout contrat ou convention concernant les systèmes d'information des services exécutifs de l'Etat comportent des clauses contractuelles comprenant :

- Les obligations en termes de sécurité intégrées dans le marché ;
- Le Plan d'Assurance Sécurité (PAS) dument complété par le titulaire et annexé au marché.

Ces documents sont tenus à disposition par le RSSI.

Annexe 3 - Tableau d'évaluation du niveau de sécurité

Disponible et téléchargeable sur https://amsn.gouv.mc/OIV/

imprimé sur papier recyclé

IMPRIMERIE GRAPHIC SERVICE
GS COMMUNICATION S.A.M. MONACO