POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION DE LA COMMUNE

Annexe à l'Arrêté Municipal n° 2019-561
du 14 février 2019

ANNEXE AU « JOURNAL DE MONACO » N° 8.422

DU 22 FÉVRIER 2019

TABLE DES MATIÈRES

Préambule

La Politique de Sécurité des Systèmes d'Information de la Commune (P.S.S.I.C.) contribue à :

- assurer la continuité des activités ;
- prévenir la fuite d'informations sensibles ;
- renforcer la confiance des administrés, des utilisateurs et des entreprises dans les télé-procédures.

Le présent document définit les mesures de sécurité applicables aux systèmes d'information de la Commune.

Cette politique de sécurité s'applique aussi aux systèmes informatiques pilotant des systèmes industriels c'est-à-dire aux systèmes de contrôle et d'acquisition de données pour le fonctionnement d'automates (par exemple gestion des bâtiments, etc.).

La Politique de Sécurité des Systèmes d'Information de la Commune 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 élus, des fonctionnaires et agents non titulaires de la Commune dans l'utilisation quotidienne des systèmes d'information, par application de la « Charte d'utilisation des ressources informatiques et des services Internet de la Mairie » conformément à l'arrêté municipal n° 2017-4181 du 17 novembre 2017.

La Politique de Sécurité des Systèmes d'Information de la Commune 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 du secret de la sécurité nationale). La Commune s'appuiera, sur la Politique de Sécurité des Systèmes d'Information de la Commune, sur les normes existantes et sur les guides techniques élaborés par l'Agence Monégasque de Sécurité Numérique pour élaborer des mesures techniques détaillées.

La Politique de Sécurité des Systèmes d'Information de la Commune se décline en trois partie, la première décrit les procédures applicables en la matière, la deuxième détaille les dix principes stratégiques à la base de ladite politique de sécurité* traduits en trente-quatre objectifs à atteindre, enfin, la troisième énonce les règles permettant de contribuer à la réalisation de chaque objectif.

*Cette politique s'appuie sur dix principes stratégiques :

- ✓ **Principe n° 1.** La maîtrise de ses systèmes d'information exige que la Commune fasse appel à des opérateurs et des prestataires de confiance.
- ✓ **Principe n° 2.** Tout système d'information de la Commune doit faire l'objet d'une analyse de risques permettant une prise en compte préventive de sa sécurité, adaptée aux enjeux du système considéré. Cette analyse s'inscrit dans une démarche d'amélioration continue de la sécurité du système, pendant toute sa durée de vie. Cette démarche doit également permettre 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 la Commune doivent être planifiés, quantifiés et identifiés au sein des ressources globales des systèmes d'information.
- ✓ **Principe n° 4.** Des moyens d'authentification forte des fonctionnaires et agents non titulaires de la Commune sur les systèmes d'information doivent être mis en place.
- ✓ **Principe n° 5.** Les opérations de gestion et d'administration des systèmes d'information de la Commune 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 la Commune.
- ✓ **Principe n° 7.** Chaque fonctionnaire et agent non titulaire de la Commune, en tant qu'utilisateur d'un système d'information, doit être informé de ses droits et devoirs mais également formé et sensibilisé à la cybersécurité.
- ✓ **Principe n° 8.** Les administrateurs des systèmes d'information doivent appliquer, après formation, les règles élémentaires d'hygiène informatique.
- ✓ **Principe n° 9.** Les produits et services acquis par la Commune et destinés à assurer la sécurité des systèmes d'information doivent faire l'objet dans la mesure du possible d'une évaluation et d'une attestation préalable de leur niveau de sécurité par l'Agence Monégasque de Sécurité Numérique (« labellisation »).
- ✓ **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 national monégasque.

Définitions

Dans le cadre de la présente Politique de Sécurité des Systèmes d'Information de la Commune les termes ou expressions ci-dessous auront la signification suivante :

- « Systèmes d'information de la Commune [1] » : 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. Cette définition recouvre entre autre tout matériel informatique (câblage, périphérique (tel que imprimantes simples ou multifonctions, webcam, etc.), disquette, disque dur, carte mémoire, CD-Rom, clé USB, ordinateur, tablette, PDA, photocopieurs, scanner, serveurs, baies de stockage, équipements réseau etc.) et toute ressource informatique de toute nature (telle que logiciels, applications, bases de données, etc.), et ce, qu'ils soient accessibles à distance, directement ou en cascade à partir d'un réseau, ainsi les moyens de communication électronique recouvrant internet et les télécommunications (tels que téléphones, équipement sans fil, carte de communication sans fil, terminaux portables, le matériel nomade, messagerie, forum, sites web, etc.) ;

- « Administration » : autorité relevant de la Commune au sens de l'article 1er de la loi n° 959 du 24 juillet 1974. Il s'agit en d'autres termes de l'Administration Communale ;

- « Autorité d'homologation » : personnel habilité désigné par l'autorité administrative d'emploi qui, après instruction du dossier d'homologation, prononce l'homologation de sécurité du système d'information. Lorsque le système est sous la responsabilité de plusieurs autorités, l'autorité d'homologation est désignée conjointement par lesdites autorités ;

- « Commission d'homologation » : commission chargée d'assister l'autorité d'homologation pour l'instruction de l'homologation et d'en préparer la décision. Elle est pilotée par le responsable de la sécurité des systèmes d'information et comprend également des représentants des utilisateurs du système, des responsables de l'exploitation et de la sécurité du système ;

- « Service concerné » : Les services communaux exploitant des systèmes d'information.

1 Article 389-1 du Code pénal.

1. PREMIÈRE PARTIE :

ORGANISATION DE LA PROTECTION

1.1- Objet

Le présent document fixe les conditions de mise en œuvre de la Politique de Sécurité des Systèmes d'Information de la Commune.

1.2- Champ d'application

La Politique de Sécurité des Systèmes d'Information de la Commune s'applique à tous les systèmes d'information des services concernés.

La Politique de Sécurité des Systèmes d'Information de la Commune concerne l'ensemble des personnes physiques ou morales intervenant dans ces système d'information, qu'il s'agisse des élus, des fonctionnaires et agents non titulaires de la Commune ou bien de tiers (prestataires ou sous-traitants) et de leurs employés.

La Politique de Sécurité des Systèmes d'Information de la Commune s'impose aussi aux systèmes aptes à traiter des informations classifiées de défense et sécurité nationale même s'ils sont soumis à un corpus réglementaire spécifique et complémentaire.

La plupart des règles de sécurité de la Politique de Sécurité des Systèmes d'Information de la Commune constituent des règles de base.

1.3- Formation des agents

La Commune forme les personnels chargés d'appliquer la Politique de Sécurité des Systèmes d'Information

Ces derniers doivent être sensibilisés à la sécurité des systèmes d'information (SSI) et au respect des règles de sécurité. 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.

1.4- Pilotage et évolutions de la Politique de Sécurité des Systèmes d'Information de la Commune

La Politique de Sécurité des Systèmes d'Information de la Commune est amenée à évoluer dans le temps. Elle pourra notamment être revue afin de 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 organisationnel, juridique, réglementaire et technologique.

Le suivi de ces évolutions est assuré par le RSSI en liaison avec le Maire et le Secrétaire Général, il a pour principales missions :

✓ de suivre la mise en œuvre de la Politique de Sécurité des Systèmes d'Information ;

✓ de proposer des mises à jour ;

✓ de proposer des documents complémentaires et des directives permettant d'en faciliter ou d'en préciser la mise en œuvre ;

✓ de suivre les évolutions des documents techniques.

1.5- Organisation de la Commune pour la mise en application de sa Politique de Sécurité des Systèmes d'Information

Le Maire et le Secrétaire Général :

✓ constituent l'autorité en charge de la sécurité des systèmes d'information de la Commune. À ce titre, ils sont chargés de valider les mesures de protection des systèmes d'information élaborés par le RSSI et de veiller à leur application. C'est dans ce cadre que la présente Politique de Sécurité des Systèmes d'Information a été définie ;

✓ sont chargés de faire mener des inspections des systèmes d'information au sein des services concernés de la Commune ;

✓ se font présenter régulièrement la situation des systèmes d'information de la Commune en liaison avec les directions des services concernés, le RSSI et les responsables des systèmes d'information.

Le Maire et le Secrétaire Général ont notamment pour mission de désigner, sur leur périmètre de compétence, les autorités d'homologation de sécurité des systèmes d'information de la Commune.

1.6- Mise en application de la Politique de Sécurité des Systèmes d'Information de la Commune

Au sein de la Commune, chaque service concerné met en place un dispositif de gestion des risques pour ses systèmes d'information. Ce dispositif doit permettre une meilleure maîtrise de la sécurité des systèmes d'information par la mise en œuvre de mesures de protection proportionnées aux enjeux et en adéquation avec les risques encourus.

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

Dans ce but, chaque service concerné :

✓ met en place une organisation en application de la Politique de Sécurité des Systèmes d'Information de la Commune ;

✓ 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 ;

✓ conduit des actions de motivation : sensibilisation et formation à la sécurité des systèmes d'information, communication claire sur les sanctions encourues (par exemple, dans charte d'utilisation des ressources informatiques et des services Internet de la Mairie) ;

✓ 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.

Il peut être nécessaire, dans certains cas, de déroger à des règles énoncées par la Politique de Sécurité des Systèmes d'Information. Il appartient alors à l'autorité du service concerné de leur substituer formellement des règles spécifiques, et au Maire et au Secrétaire Général de valider la substitution des règles spécifiques après avis du RSSI qui tient à jour la liste des dérogations.

Chaque service concerné élabore un bilan annuel comportant :

✓ une synthèse de l'état d'avancement de la cartographie des systèmes d'information et de ses mises à jour ;

✓ l'état d'avancement de l'application des règles édictées par la Politique de Sécurité des Systèmes d'Information ;

- ✓ un récapitulatif des actions réalisées pour la mise en conformité à la Politique de Sécurité des Systèmes d'Information ;
- ✓ un récapitulatif des incidents significatifs constatés (accompagnés éventuellement de descriptifs des dispositions mise en œuvre pour les résoudre).

1.7- Contrôle et suivi de l'application de la Politique de Sécurité des Systèmes d'Information de la Commune

Le respect de la Politique de Sécurité des Systèmes d'Information de la Commune fait l'objet de contrôles réguliers à différents niveaux pour chaque service concerné.

Le RSSI vérifie, 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.

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

1.8- 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 Commune, 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 remonter au RSSI 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 les « Computer Emergency Response Team » au niveau international (C.E.R.T.) et par le RSSI. Les alertes significatives sont signalées par l'Agence Monégasque de Sécurité Numérique aux responsables de la sécurité des systèmes d'information. Leur prise en compte au sein de la Commune est organisée sous la responsabilité du Maire et du Secrétaire Général

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 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 responsables de services concernés 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, si besoin, avec la planification gouvernementale de gestion de crise.

2. DEUXIÈME PARTIE :

OBJECTIFS

Les objectifs de la Politique de Sécurité des Systèmes d'Information de la Commune sont les suivants :

2.1- Politique, organisation, gouvernance

Objectif 1 : Organisation de la sécurité des systèmes d'information : mettre en place une organisation adéquate, garantissant la prise en compte préventive et réactive de la sécurité.

2.2- Ressources Humaines

Objectif 2 : Ressources Humaines : faire des personnes les maillons forts des systèmes d'information des services concernés.

2.3- Gestion des biens

Objectif 3 : Cartographie des systèmes d'information : tenir à jour une cartographie détaillée et complète des systèmes d'information.

Objectif 4 : Qualification et protection de l'information : qualifier l'information de façon à adapter les mesures de Protection.

2.4- Intégration de la sécurité des systèmes d'information dans le cycle de vie des systèmes d'information

Objectif 5 : Risques : apprécier, traiter, et communiquer sur les risques relatifs à la sécurité des systèmes d'information.

Objectif 6 : Maintien en condition de sécurité : gérer dynamiquement les mesures de protection, tout au long de la vie du système d'information.

Objectif 7 : Produits et services qualifiés ou certifiés : 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.

Objectif 8 : Maîtrise des prestations : veiller aux exigences de sécurité lorsqu'il est fait appel à de la prestation par des tiers.

2.5- Sécurité physique

Objectif 9 : Sécurité physique des locaux abritant les systèmes d'information : inscrire la sécurisation physique des systèmes d'information dans la sécurisation physique des locaux et dans les processus associés.

2.6- Sécurité physique des centres informatiques

Objectif 10 : 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.

Objectif 11 : Sécurité du 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.

2.7- Sécurité des réseaux

Objectif 12 : Usage sécurisé des réseaux nationaux : utiliser les infrastructures nationales, en respectant les règles de sécurité qui leur sont attachées.

Objectif 13 : Usage sécurisé des réseaux locaux : maîtriser les interconnexions de réseaux locaux. Configurer de manière adéquate les équipements de réseau actifs.

Objectif 14 : Accès spécifiques : ne pas porter atteinte à la sécurité du système d'information par le déploiement d'accès non supervisés.

Objectif 15 : Usage sécurisé des réseaux sans fil : maîtriser le déploiement, la configuration et l'usage des réseaux sans fil.

Objectif 16 : Sécurité des mécanismes de commutation et de routage : configurer les mécanismes de commutation et de routage pour se protéger des attaques.

Objectif 17 : Cartographie réseau : tenir à jour une cartographie détaillée et complète des réseaux et des interconnexions.

Objectif 18 : Architecture sécurisée des centres informatiques : appliquer les principes de défense en profondeur à l'architecture matérielle et logicielle des centres informatiques.

2.8- Exploitation des systèmes d'information

Objectif 19 : Protection des informations sensibles : définir et mettre en œuvre des mesures de protection renforcées pour les informations sensibles.

Objectif 20 : Surveillance et configuration des ressources informatiques : durcir les configurations des ressources informatiques, et surveiller les interventions opérées sur celles-ci.

Objectif 21 : Autorisations et contrôles d'accès : authentifier les usagers et contrôler leurs accès aux ressources des systèmes d'information de la Commune, en fonction d'une politique explicite d'autorisations.

Objectif 22 : Sécurisation de l'exploitation : fournir aux administrateurs les outils nécessaires à l'exercice des tâches de sécurité des systèmes d'information et configurer ces outils de manière sécurisée.

Objectif 23 : Défense des systèmes d'information : défendre les systèmes d'information nécessite une vigilance de tous, et des actions permanentes.

Objectif 24 : Exploitation sécurisée des centres informatiques : exploiter de manière sécurisée les centres informatiques en s'appuyant sur des procédures adaptées et sur la maîtrise des outils de supervision.

2.9- Sécurité du poste de travail

Objectif 25 : Sécurisation des postes de travail : durcir les configurations des postes de travail en protégeant les utilisateurs.

Objectif 26 : Sécurisation des copieurs multifonctions : paramétrer les imprimantes et copieurs multifonctions afin de diminuer leur surface d'attaque.

Objectif 27 : Sécurisation de la téléphonie : sécuriser la téléphonie pour protéger les utilisateurs contre des attaques malveillantes.

Objectif 28 : Contrôles de la conformité des postes de travail : contrôler régulièrement la conformité des paramétrages de sécurité appliqués aux postes de travail.

2.10- Sécurité du développement des systèmes

Objectif 29 : Prise en compte de la sécurité dans le développement des systèmes d'information : reconnaître la sécurité comme une fonction essentielle, et la prendre en compte dès la conception des projets.

Objectif 30 : Prise en compte de la sécurité dans le développement des logiciels : mener les développements logiciels selon une méthodologie de sécurisation du code produit.

Objectif 31 : Sécurisation des applications à risques : accompagner le développement sécurisé d'applications à risques par des contre-mesures minimisant l'impact d'attaques nouvelles.

2.11- Traitement des incidents

Objectif 32 : Chaînes opérationnelles : partager l'information (alertes, incidents) dans le respect des règles de prudence et mutualiser les opérations de remise en entreprise, de façon à lutter efficacement contre les attaques.

2.12- Continuité d'activités

Objectif 33 : Gestion de la continuité d'activité : se doter de plans de continuité d'activité, et les tester.

2.13- Contrôles

Objectif 34 : Contrôles réguliers : effectuer des contrôles (audits, inspections) et des exercices réguliers de façon à mesurer les progrès accomplis et corriger les manquements.

3. TROISIÈME PARTIE :

RÈGLES APPLICABLES

Sont regardées comme prioritaires, les mentions figurant sous les numéros : 3.1.1. ; 3.1.2. ; 3.2.1. ; 3.2.3. ; 3.2.4. ; 3.2.5. ; 3.3.1. ; 3.3.2. ; 3.3.3. ; 3.3.4. ; 3.4.1. ; 3.4.2. ; 3.4.4. ; 3.4.5. ; 3.4.8. ; 3.5.1. ; 3.5.4. ; 3.6.1. ; 3.6.4. ; 3.6.6. ; 3.7.1. ; 3.8.1. ; 3.8.2. ; 3.8.3. ; 3.8.4. ; 3.8.8. ; 3.8.9. ; 3.8.14. ; 3.8.15. ; 3.8.16. ; 3.9.1. ; 3.9.3. ; 3.10.1. ; 3.10.2. ; 3.10.5. ; 3.10.8. ; 3.10.9. ; 3.10.10. ; 3.10.11. ; 3.10.13. ; 3.10.14. ; 3.10.16. ; 3.10.17. ; 3.10.18. ; 3.10.19. ; 3.10.21. ; 3.10.22. ; 3.10.26. ; 3.10.31. ; 3.10.35. ; 3.10.37. ; 3.10.38. ; 3.10.39. ; 3.10.41. ; 3.10.42. ; 3.10.43. ; 3.10.44. ; 3.10.45 ; 3.10.46. ; 3.10.55. ; 3.10.56. ; 3.10.57. ; 3.10.58. ; 3.11.1. ; 3.11.2. ; 3.11.3. ; 3.11.5. ; 3.11.6. ; 3.11.7. ; 3.11.13. ; 3.11.14. ; 3.11.20. ; 3.12.1. ; 3.12.2. ; 3.12.4. ; 3.12.7. ; 3.13.2. ; 3.14.1. ; 3.14.4. ; 3.14.5. ; ci-après énoncés.

3.1- Politique, organisation, gouvernance

Organisation de la sécurité des systèmes d'information

Objectif 1 : organisation de la sécurité du système d'information : mettre en place une organisation adéquate, garantissant la prise en compte préventive et réactive de la sécurité.

Organisation de la sécurité des systèmes d'information

3.1.1 ORG-SSI : une organisation pour la sécurité du système d'information est définie au sein de la Commune voire au sein de chaque service concerné. Cette organisation identifie les acteurs, définit les responsabilités internes et à l'égard des tiers, les modalités si nécessaires de coordination avec les autorités et l'Agence Monégasque de Sécurité Numérique, ainsi que les modalités d'application des mesures de protection. Des procédures d'applications sont écrites et portées à la connaissance de tous.

Responsabilités internes

3.1.2 ORG-RSSI : désignation du responsable de la sécurité des systèmes d'information (RSSI) qui :

- fait valider les mesures d'application de la Politique de Sécurité des Systèmes d'Information de la Commune par le Maire et le Secrétaire Général ;

- coordonne les actions permettant l'intégration des clauses liées à la sécurité des systèmes d'information dans tout contrat ou convention ;

- planifie les actions de mise en application de la Politique de Sécurité des Systèmes d'Information de la Commune ;

- rend compte régulièrement de la mise en application des mesures de sécurité auprès du Maire et du Secrétaire Général ;

- formalise et tient à jour les documents d'application de la Politique de Sécurité des Systèmes d'Information de la Commune sur son périmètre.

3.2- Ressources Humaines

Objectif 2 : ressources Humaines : faire des personnes les maillons forts des systèmes d'information de la Commune.

Utilisateurs

3.2.1 RH-SSI : une charte d'application de la Politique de Sécurité des Systèmes d'Information, récapitulant les mesures pratiques d'utilisation sécurisée des ressources informatiques est communiquée à l'ensemble des élus, des fonctionnaires et agents non titulaires de la Commune. Le personnel non permanent (stagiaires, intérimaires, prestataires…) est informé de ses devoirs dans le cadre de son usage des systèmes d'information de la Commune.

Personnel permanent

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

3.2.3 RH-UTIL : sensibilisation des utilisateurs des systèmes d'information. Chaque utilisateur doit être régulièrement informé des exigences de sécurité le concernant, et motivé à leur respect. Il doit être formé à l'utilisation des outils de travail conformément aux règles de la sécurité des systèmes d'information.

Mouvement de personnel

3.2.4 RH-MOUV : gestion des arrivées, des mutations et des départs. 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.

Personnel non permanent

3.2.5 RH-NPERM : gestion du personnel non permanent (stagiaires, intérimaires, prestataires…). Les règles de la Politique de Sécurité des Systèmes d'Information de la Commune s'appliquent à tout personnel non permanent utilisateur d'un système d'information de la Commune. 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.

3.3- Gestion des biens

Objectif 3 : cartographie des systèmes d'information : tenir à jour une cartographie détaillée et complète des systèmes d'information.

3.3.1 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 au RSSI pour les besoins de coordination opérationnelle. Il comprend la liste des « briques » matérielles et logicielles utilisées, ainsi que leurs versions exactes.

3.3.2 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 fournie au RSSI, et à l'Agence Monégasque de Sécurité Numérique sur sa demande.

Objectif 4 : qualification et protection de l'information. Qualifier l'information de façon à adapter les mesures de protection.

3.3.3 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 arrêtés d'application de la loi n° 1.430 du 13 juillet 2016.

3.3.4 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.

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

Gestion des risques et homologation de sécurité

Objectif 5 : gestion des risques et homologation de sécurité. Apprécier, traiter, et communiquer sur les risques relatifs à la sécurité des systèmes d'information.

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

Maintien en condition de sécurité des systèmes d'information

Objectif 6 : maintien en condition de sécurité des systèmes d'information. Gérer dynamiquement les mesures de protection, tout au long de la vie du système d'information.

3.4.2 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.

3.4.3 INT-QUOT-SSI : mise en œuvre au quotidien de la sécurité des systèmes d'information. 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.

Produits et services labellisés

Objectif 7 : produits et services qualifiés ou certifiés. Utiliser si possible et disponible, 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.

3.4.4 INT-AQ-PSL : acquisition de produits et services de confiance. Lorsqu'ils sont disponibles, des produits ou des services de sécurité labellisés par l'Agence Monégasque de Sécurité Numérique doivent être utilisés.

Gestion des prestataires

Objectif 8 : maîtrise des prestations. Veiller aux exigences de sécurité lorsqu'il est fait appel à de la prestation par des tiers.

3.4.5 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.

3.4.6 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 un prestataire d'audit qualifié, 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.

3.4.7 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.

3.4.8 INT-REX-HB : hébergement. L'hébergement des données de l'Administration sur le territoire national est obligatoire, sauf accord du Maire, et dérogation dûment motivée et précisée dans la décision d'homologation[2].

3.4.9 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.).

3.5- Sécurité physique

Sécurité physique des locaux abritant les systèmes d'information

Règles générales

Objectif 9 : sécurité physique des locaux abritant les systèmes d'information. Inscrire la sécurisation physique des systèmes d'information dans la sécurisation physique des locaux et dans les processus associés.

3.5.1 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 et de l'Agence Monégasque de Sécurité Numérique si besoin. Pour chaque zone de sécurité, des critères précis d'autorisation d'accès sont établis.

Règles de sécurité s'appliquant aux zones d'accueil du public

3.5.2 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.

---

2 L'autorité d'homologation met en place une commission d'homologation, pilotée par le RSSI, chargée de l'assister et de préparer la décision d'homologation. Une telle commission comprend notamment le RSSI, des représentants des utilisateurs du système, et des responsables de l'exploitation et de la sécurité du système. La décision est soumise pour avis à l'Agence Monégasque de Sécurité Numérique.

3.5.3 PHY-SENS : protection des informations sensibles au sein des zones d'accueil. 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.

Règles de sécurité complémentaires s'appliquant aux locaux techniques

3.5.4 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.

3.5.5 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.

3.5.6 PHY-CTRL : contrôles anti-piégeages. Sur les systèmes d'information particulièrement sensibles, il convient de mener des contrôles anti-piégeages réguliers, effectués par du personnel formé. Il peut être fait appel à des services spécialisés (opérations dites de « dépoussiérage »).

3.6- Sécurité physique des centres informatiques

Objectif 10 : 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.

Règles générales

3.6.1 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 service concerné.

Règles de sécurité complémentaires s'appliquant aux zones internes et restreintes

3.6.2 PHY-CI-CTRLACC : contrôle d'accès physique. 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.

3.6.3 PHY-CI-MOYENS : délivrance des moyens d'accès physique. 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.

3.6.4 PHY-CI-TRACE : traçabilité des accès. 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.

Règles de sécurité complémentaires s'appliquant aux salles informatiques et aux locaux techniques

3.6.5 PHY-CI-ENERGIE : local énergie. L'alimentation secteur des équipements devra être conforme aux règles de l'art, de façon à se prémunir des atteintes à la sécurité des personnes et équipements liées à un défaut électrique.

3.6.6 PHY-CI-CLIM : 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.

3.6.7 PHY-CI-INC : 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.

3.6.8 PHY-CI-EAU : 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.

3.7- Système d'information de sûreté

Objectif 11 : sécurité du 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 support 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 vidéo-surveillance (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.

3.7.1 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. Un système de gestion de la sécurité du système d'information de sûreté (s'inspirant de la norme ISO 27001) assure le maintien en condition de sécurité. L'emploi de produits labellisés, quand ils existent, est fortement recommandé.

3.8- Sécurité des réseaux

Sécurité des réseaux

Objectif 12 : usage sécurisé des réseaux. Utiliser les infrastructures nationales, en respectant les règles de sécurité qui leur sont attachées.

3.8.1 RES-MAITRISE : systèmes autorisés sur le réseau. Seuls les équipements gérés et configurés par les équipes informatiques habilitées peuvent être connectés au réseau d'un service concerné.

3.8.2 RES-INTERCO : interconnexion avec des réseaux externes. Toute interconnexion entre les réseaux de la Commune et un réseau externe (réseau d'un tiers, Internet, etc.) doit être réalisée via des infrastructures maîtrisées. La décision d'interconnexion doit être motivée et validée par le Maire et le Secrétaire Général.

3.8.3 RES-ENTSOR : mettre en place un 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.

3.8.4 RES-PROT : protection des informations. Les accès à Internet passent obligatoirement à travers les passerelles nationales. Dès lors que des informations sensibles doivent transiter sur des réseaux non maîtrisés, il convient de les protéger spécifiquement par chiffrement adapté.

Sécurité des réseaux locaux

Objectif 13 : usage sécurisé des réseaux locaux. Maîtriser les interconnexions de réseaux locaux. Configurer de manière adéquate les équipements de réseau actifs.

3.8.5 RES-CLOIS : cloisonner le système d'information 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.

3.8.6 RES-INTERCOGEO : interconnexion des sites géographiques de la Commune. L'interconnexion au niveau local de réseaux locaux des services concernés 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 par le RSSI.

3.8.7 RES-RESS : cloisonnement des ressources en cas de partage de locaux. Dans le cas où un service concerné 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 par le RSSI.

Accès spécifiques

Objectif 14 : accès spécifiques. Ne pas porter atteinte à la sécurité du système d'information par le déploiement d'accès non supervisés.

3.8.8 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.

Sécurité des réseaux sans fil

Objectif 15 : usage sécurisé des réseaux sans fil. Maîtriser le déploiement, la configuration et l'usage des réseaux sans fil.

3.8.9 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 par le RSSI, 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.

Sécurisation des mécanismes de commutation et de routage

Objectif 16 : sécurité des mécanismes de commutation et de routage. Configurer les mécanismes de commutation et de routage pour se protéger des attaques.

3.8.10 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 » (A.R.P.).

3.8.11 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.

3.8.12 RES-ROUTDYN-IGP : configurer le protocole « Interior Gateway Protocol » (I.G.P.) de manière sécurisée. Le protocole de routage dynamique de type I.G.P. 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.

3.8.13 RES-ROUTDYN-EGP : sécuriser les sessions Exterior Gateway Protocol » (E.G.P.). Lors de la mise en place d'une session E.G.P. avec un pair extérieur sur un média partagé, cette session doit s'accompagner d'un mot de passe de type MESSAGE-DIGEST-KEY.

3.8.14 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.

3.8.15 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.

Cartographie réseau

Objectif 17 : cartographie réseau. Tenir à jour une cartographie détaillée et complète des réseaux et des interconnexions.

3.8.16 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.

3.9- Architecture des systèmes d'information

Architecture des centres informatiques

Objectif 18 : architecture sécurisée des centres informatiques. Appliquer les principes de défense en profondeur à l'architecture matérielle et logicielle des centres informatiques.

3.9.1 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 (V.L.A.N.) appropriés, d'un filtrage strict des flux applicatifs et d'administration.

3.9.2 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.

3.9.3 ARCHI-PASS : passerelle Internet. Les interconnexions Internet passent obligatoirement par les passerelles homologuées de la Commune.

3.10- Exploitation des systèmes d'information

Protection des informations sensibles

Objectif 19 : protection des informations sensibles. Définir et mettre en œuvre des mesures de protection renforcées pour les informations sensibles.

3.10.1 EXP-PROT-INF : protection des informations sensibles en confidentialité et 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.

Sécurité des ressources informatiques

Objectif 20 : surveillance et configuration des ressources informatiques. Durcir les configurations des ressources informatiques, et surveiller les interventions opérées sur celles-ci.

3.10.2 EXP-TRAC : traçabilité des interventions sur le système. Les interventions de maintenance sur les ressources informatiques de la Commune doivent être tracées par le service informatique, et ces traces doivent être accessibles durant au moins un an.

3.10.3 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.

3.10.4 EXP-DOC-CONFIG : documentation des configurations. La configuration standard des ressources informatiques doit être documentée et mise à jour à chaque changement notable.

Gestion des autorisations et contrôle d'accès logique aux ressources

Objectif 21 : autorisations et contrôles d'accès. Authentifier les usagers et contrôler leurs accès aux ressources des systèmes d'information de la Commune, en fonction d'une politique explicite d'autorisations.

Contrôle des accès logiques

3.10.5 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. À 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.

3.10.6 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 minimum de privilèges lui permettant de conduire les actions explicitement autorisées pour lui).

3.10.7 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.

Processus d'autorisation

3.10.8 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.

3.10.9 EXP-REVUE-AUTH : revue des autorisations d'accès. Une revue des autorisations d'accès doit être réalisée annuellement sous le contrôle du RSSI, le cas échéant avec l'appui de l'Agence Monégasque de Sécurité Numérique.

Gestion des authentifiants

3.10.10 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.

3.10.11 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.

3.10.12 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.

3.10.13 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 service concerné. Les recommandations de l'Agence Monégasque de Sécurité Numérique doivent être appliquées pour tous les comptes.

3.10.14 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.

Gestion des authentifiants d'administration des systèmes d'information

3.10.15 EXP-SEQ-ADMIN : séquestre des authentifiants « administrateur ». Les authentifiants 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.

3.10.16 EXP-POL-ADMIN : politique de mots de passe « administrateurs ». Chaque administrateur doit disposer d'un mot de passe propre et destiné à l'administration.

3.10.17 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).

Exploitation sécurisée des ressources informatiques

Objectif 22 : sécurisation de l'exploitation. Fournir aux administrateurs les outils nécessaires à l'exercice des tâches de sécurité des systèmes d'information et configurer ces outils de manière sécurisée.

Entreprise des systèmes

3.10.18 EXP-RESTR-DROITS : restriction des droits. Sauf exception dûment motivée et validée par le RSSI, les utilisateurs n'ont pas de droits d'administration.

3.10.19 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.

3.10.20 EXP-HABILIT-ADMIN : habilitation des administrateurs. L'habilitation des administrateurs s'effectue selon une procédure validée par l'autorité d'homologation. Le nombre de personnes habilitées pour des opérations d'administration doit être connu et validé par l'autorité d'homologation.

3.10.21 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.

3.10.22 EXP-SEC-FLUXADMIN : sécurisation des flux d'administration. Les opérations d'administration sur les ressources d'une entité 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.

3.10.23 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.

3.10.24 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 agents autorisés par l'équipe chargée des systèmes d'information, sur les ressources informatiques de leur périmètre. Des mesures de sécurité spécifiques doivent être définies et respectées.

Entreprise des domaines

3.10.25 EXP-DOM-POL : définir une politique de gestion des comptes du domaine. Une politique explicite de gestion des comptes du domaine doit être documentée.

3.10.26 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.

3.10.27 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.

3.10.28 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.

3.10.29 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.

3.10.30 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.

3.10.31 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.

3.10.32 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.

Envoi en maintenance et mise au rebut

3.10.33 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 qualifiés. L'effacement des données sensibles doit s'appuyer sur des produits qualifiés, ou respecter des procédures établies en concertation avec le RSSI.

3.10.34 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, ou respecter des procédures établies en concertation avec le RSSI.

Lutte contre les codes malveillants

3.10.35 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.

3.10.36 EXP-GES-ANTIVIR : gestion des événements de sécurité de l'antivirus. Les événements de sécurité de l'antivirus doivent être remontés sur un serveur pour analyse statistique et gestion des problèmes a posteriori (exemples : serveur constamment infecté, virus détecté et non éradiqué par l'antivirus, etc.).

3.10.37 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.

3.10.38 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 doit être configuré de manière sécurisée (désactivation des services inutiles, nettoyage du magasin de certificats, etc.).

Mise à jour des systèmes et des logiciels

3.10.39 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.

3.10.40 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 les préconisations de l'Agence Monégasque de Sécurité Numérique et des outils labellisés si possible.

3.10.41 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.

3.10.42 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 système d'information) et des applications (pas de ressources partagées avec le reste du système d'information).

Journalisation

3.10.43 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.

3.10.44 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 de traces des événements de sécurité est définie par le RSSI, validée par l'autorité d'homologation et mise en œuvre. Le niveau de sécurité d'un système d'information dépend en grande partie de la capacité de ses exploitants et administrateurs à détecter les erreurs, dysfonctionnements et tentatives d'accès illicites survenant sur les éléments qui le composent.

3.10.45 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.

Défense des systèmes d'information

Objectif 23 : défense des systèmes d'information. Défendre les systèmes d'information nécessite une vigilance de tous, et des actions permanentes.

3.10.46 EXP-GES-DYN : gestion dynamique de la sécurité. L'équipe en charge d'exploitation du système 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.

Gestion des matériels informatiques fournis à l'utilisateur

3.10.47 EXP-MAIT-MAT : maîtrise des matériels. Les postes de travail - y compris dans le cas d'une location - sont fournis à l'utilisateur par la Commune, gérés et configurés sous la responsabilité de la Commune. 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.

3.10.48 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 Politique de Sécurité des Systèmes d'Information de la Commune. Chaque utilisateur doit veiller à la sécurité des supports amovibles (clés USB et disques amovibles), notamment en les conservant dans un endroit sûr. Il est recommandé de chiffrer les données contenues sur ces supports. Les supports contenant des données sensibles doivent être stockés dans des meubles fermant à clef.

3.10.49 EXP-DECLAR-VOL : déclarer les pertes et vols. Toute perte ou vol d'une ressource d'un système d'information doit être déclarée au RSSI, au Maire et au Secrétaire Général, et éventuellement à l'Agence Monégasque de Sécurité Numérique.

3.10.50 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.

Nomadisme

3.10.51 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.

3.10.52 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 selon une procédure définie.

Sécurisation des imprimantes et copieurs multifonctions manipulant des informations sensibles

3.10.53 EXP-IMP-SENS : impression des informations sensibles. Les impressions d'informations sensibles doivent être effectuées selon une procédure prédéfinie, garantissant le contrôle par l'utilisateur, du déclenchement de l'impression jusqu'à la récupération du support imprimé.

3.10.54 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.

Exploitation des centres informatiques

Objectif 24 : exploitation sécurisée des centres informatiques. Exploiter de manière sécurisée les centres informatiques en s'appuyant sur des procédures adaptées et sur la maîtrise des outils de supervision.

Sécurité des ressources informatiques

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

3.10.55 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.

3.10.56 EXP-CI-PROTFIC : passerelle d'échange de fichiers. Les échanges de fichiers entre applications doivent privilégier les protocoles sécurisés (SSL/TLS, FTPS...).

3.10.57 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.

3.10.58 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 deux types de flux d'administration doivent être dans la mesure du possible cloisonnés.

3.10.59 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, on utilisera les extensions sécurisées DNSSEC.

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

3.10.61 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).

3.10.62 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.

3.11- Sécurité du poste de travail

Sécurisation des postes de travail

Objectif 25 : sécurisation des postes de travail. Durcir les configurations des postes de travail en protégeant les utilisateurs.

Mise à disposition du poste

3.11.1 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 systèmes d'information.

Sécurité physique des postes de travail

3.11.2 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).

3.11.3 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.

Réaffectation du poste et récupération d'informations

3.11.4 PDT-REAFFECT : réaffectation du poste de travail. Une procédure de sécurité des systèmes d'information définit les règles concernant le traitement à appliquer aux informations ayant été stockées où manipulées sur les postes réaffectés.

Gestion des privilèges sur les postes de travail

3.11.5 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.

3.11.6 PDT-PRIV : utilisation des privilèges d'accès « administrateur ». Les privilèges d'accès « administrateur » doivent être utilisés uniquement pour les actions d'administration le nécessitant.

3.11.7 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.

Protection des informations

3.11.8 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.

3.11.9 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.

3.11.10 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.

3.11.11 PDT-CHIFF-SENS : chiffrement des données sensibles. Une solution de chiffrement labellisée 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.

3.11.12 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 Service Informatique.

Nomadisme

3.11.13 PDT-NOMAD-ACCESS : accès à distance aux Systèmes d'Information de la Commune. Les accès à distance aux systèmes d'information de la Commune (accès dits « nomades ») doivent être réalisés via les infrastructures communales. Lorsque l'accès à distance utilise d'autres infrastructures, l'usage de réseaux privés virtuels (VPN) de confiance est nécessaire.

3.11.14 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.

3.11.15 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.

3.11.16 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.

3.11.17 PDT-NOMAD-DESACTIV : désactivation des interfaces de connexion sans fil. Des règles de configuration des interfaces de connexion sans fil (Wifi, Bluetooth, 4G…), 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.

Sécurisation des imprimantes et copieurs multifonctions

Objectif 26 : sécurisation des copieurs multifonctions. Paramétrer les imprimantes et copieurs multifonctions afin de diminuer leur surface d'attaque.

3.11.18 PDT-MUL-DURCISS : durcissement des imprimantes et copieurs multifonctions. Les imprimantes et copieurs multifonctions hébergés localement dans un service concerné 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.

3.11.19 PDT-MUL-SECNUM : sécurisation de la fonction de numérisation. Lorsqu'elle est activée, la fonction de numérisation sur les copieurs multifonctions hébergés dans un service concerné 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 la Commune, envoi uniquement à une seule adresse de messagerie.

Sécurisation de la téléphonie

Objectif 27 : sécurisation de la téléphonie. Sécuriser la téléphonie pour protéger les utilisateurs contre des attaques malveillantes.

3.11.20 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.

3.11.21 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.

3.11.22 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.

Contrôles de conformité

Objectif 28 : contrôles de la conformité des postes de travail. Contrôler régulièrement la conformité des paramétrages de sécurité appliqués aux postes de travail.

3.11.23 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.

3.12- Sécurité du développement des systèmes

Développement des systèmes

Objectif 29 : prise en compte de la sécurité dans le développement des systèmes d'information. Reconnaître la sécurité comme une fonction essentielle, et la prendre en compte dès la conception des projets.

3.12.1 DEV-INTEGR-SECLOC : intégrer la sécurité dans les développements. Toute initiative de développement informatique doit respecter les exigences de la Commune 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 si besoin de l'application du référentiel général de sécurité, et de l'application d'une démarche d'homologation du système.

3.12.2 DEV-SOUS-TRAIT : intégrer des clauses de sécurité des systèmes d'information 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.

Développements logiciels et sécurité

Objectif 30 : prise en compte de la sécurité dans le développement des logiciels. Mener les développements logiciels selon une méthodologie de sécurisation du code produit.

3.12.3 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.

3.12.4 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.

3.12.5 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.

3.12.6 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.

3.12.7 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 REGLES 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.).

3.12.8 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.

Applications à risques

Objectif 31 : sécurisation des applications à risques. Accompagner le développement sécurisé d'applications à risques par des contre-mesures minimisant l'impact d'attaques nouvelles.

3.12.9 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.

3.13- Traitement des incidents

Chaînes opérationnelles

Objectif 32 : chaînes opérationnelles. 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.

3.13.1 TI-OPS-SSI : chaînes opérationnelles de sécurité des systèmes d'information. Les chaînes opérationnelles de la Commune concourent à l'effort de cyber sécurité. Les alertes et les incidents sont gérés selon des procédures testées lors d'exercices. La coordination des compétences est organisée à l'échelon de la Commune. Les situations d'urgences peuvent faire appel à des mesures définies préalablement.

Traitement des alertes de sécurité émises par les instances nationales (Agence Monégasque de Sécurité Numérique)

3.13.2 TI-MOB : mobilisation en cas d'alerte. En cas d'alerte de sécurité identifiée au niveau national, le RSSI s'assure de la bonne application des exigences formulées par les instances nationales, dans les meilleurs délais.

Remontée des incidents de sécurité rencontrés

3.13.3 TI-QUAL-TRAIT : qualification et traitement des incidents. Le RSSI et la chaine hiérarchique sont informés de tout incident de sécurité. Le RSSI assure la qualification de l'incident et le pilotage de son traitement. Si nécessaire il alerte le Maire, le Secrétaire Général et l'Agence Monégasque de Sécurité Numérique.

3.13.4 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, fait l'objet d'un compte-rendu au RSSI qui si besoin alertera le Maire, le Secrétaire Général et le Centre opérationnel de la sécurité des systèmes d'information (CERT-MC) de l'Agence Monégasque de Sécurité Numérique.

Cette remontée est immédiate pour les incidents dont la portée est susceptible de dépasser à court terme le périmètre de la Commune, et pour les incidents correspondant à des signalements spécifiques, notamment de la part de l'Agence Monégasque de Sécurité Numérique.

Le RSSI 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.

3.14- Continuité d'activité

Gestion de la continuité d'activité des systèmes d'information

Objectif 33 : gestion de la continuité d'activité. Se doter de plans de continuité d'activité, et les tester.

3.14.1 PCA-DEP : définition du plan de continuité d'activité des systèmes d'information. Chaque service concerné définit 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.

Mise en œuvre du plan de continuité d'activité des systèmes d'information

3.14.2 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.

3.14.3 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.

3.14.4 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.

3.14.5 PCA-PROT : protection de la confidentialité des sauvegardes. Les sauvegardes doivent être traitées de manière à garantir leur confidentialité et leur intégrité.

Maintien en conditions opérationnelles du plan de continuité d'activité des systèmes d'information

3.14.6 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.

3.14.7 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.

3.15- Conformité, audit, inspection, contrôle

Contrôles

Objectif 34 : contrôles réguliers. Effectuer des contrôles (audits, inspections) et des exercices réguliers de façon à mesurer les progrès accomplis et corriger les manquements.

3.15.1 CONTR-SSI : contrôles locaux. La conformité à la Politique de Sécurité des Systèmes d'Information de la Commune est vérifiée par des contrôles réguliers. Le RSSI conduit des actions d'évaluation de la conformité à la Politique de Sécurité des Systèmes d'Information de la Commune et contribuent à la consolidation de l'état d'avancement de sa mise en œuvre.

3.15.2 CONTR-BILAN-SSI : bilan annuel. Chaque service concerné établit un bilan annuel mesurant la maturité de sécurité des systèmes d'information globale. Le RSSI consolide l'ensemble de ces bilans. Le document de synthèse est soumis au Maire et au Secrétaire Général.

Date d'entrée en vigueur :

La Politique de Sécurité des Systèmes d'Information de la Commune figure en annexe de l'arrêté municipal n° 2019-561 du 14 février 2019 et entre en vigueur à compter du lendemain de la publication au Journal de Monaco dudit arrêté municipal.

Dispositions transitoires

La mise en application de la Politique de Sécurité des Systèmes d'Information s'effectue selon les règles suivantes :

✓ les systèmes d'informations de la Commune devront être en conformité totale dans les 3 ans suivant la publication de la Politique de Sécurité des Systèmes d'Information ;

✓ la Commune devra, au 1er septembre 2019, avoir mis en conformité sa politique de sécurité des systèmes d'information de la Commune et défini un plan d'action. Celui-ci tiendra compte des impacts sur les activités ainsi que des moyens financiers et humains à mettre en œuvre. Il sera établi un calendrier de mise en conformité indiquant les mesures à prendre dans l'immédiat puis à court et à long terme.

imprimé sur papier PEFC

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