Arrêté Ministériel n° 2018-1053 du 8 novembre 2018 portant application de l'article 27 de la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique

Nous, Ministre d'État de la Principauté,

Vu la Constitution ;

Vu le Code pénal ;

Vu la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale ;

Vu la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique ;

Vu l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique, modifiée ;

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

Vu l'arrêté ministériel n° 2017-42 du 24 janvier 2017 portant application de l'article 26 de la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique ;

Vu l'arrêté ministériel n° 2017-625 du 16 août 2017 portant application de l'article 3 de l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique, modifiée ;

Vu l'arrêté ministériel n° 2017-835 du 29 novembre 2017 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'administration et l'administré, modifiée.

Vu la délibération du Conseil de Gouvernement en date du 24 octobre 2018 ;

ARRÊTONS :

ARTICLE PREMIER.

Les règles de sécurité prévues à l'article 27 de la loi n° 1.435 du 8 novembre 2016, susvisée, nécessaires à la protection des systèmes d'information des opérateurs d'importance vitale sont décrites à l'annexe I du présent arrêté.

À compter de l'entrée en vigueur du présent arrêté ou de sa date de désignation en tant qu'opérateur d'importance vitale, et/ou de la notification, conformément à l'article 66 du présent arrêté ministériel, des annexes V, VI et VII du présent arrêté, tout opérateur d'importance vitale applique les règles de sécurité visées au premier alinéa dans les délais figurant à l'annexe V, précitée. Ces délais peuvent être différents selon les règles de sécurité, le type de systèmes d'information concernés, l'opérateur d'importance vitale, ou la date de mise en service de ces systèmes.

ART. 2.

Dans un délai de trois mois à compter de la date d'entrée en vigueur du présent arrêté ou de sa désignation comme opérateur d'importance vitale, et/ou de la notification des annexes V, VI et VII du présent arrêté, tout opérateur adresse par courrier à l'Agence Monégasque de Sécurité Numérique la liste de ses systèmes d'information d'importance vitale, ainsi que, pour chacun d'eux, le formulaire de déclaration de l'annexe II, précitée, disponible et téléchargeable sur le site https://amsn/gouv.mc/oiv.

Pour déterminer si un système d'information doit être qualifié d'importance vitale, l'opérateur d'importance vitale mène une analyse d'impact sur ses systèmes d'information, notamment sur ceux relevant des types de système d'information mentionnés à l'annexe VI, précitée.

Lorsque, pour un type de système d'information, mentionné à l'annexe VI, précitée, l'opérateur ne déclare aucun système d'information d'importance vitale, il en précise les raisons.

ART. 3.

L'opérateur d'importance vitale communique, une fois par an à l'Agence Monégasque de Sécurité Numérique, les mises à jour de la liste mentionnée au premier alinéa de l'article précédent et de ses formulaires de déclaration.

Ledit opérateur déclare tout nouveau système d'information d'importance vitale préalablement à sa mise en service et tout système d'information qui viendrait à satisfaire aux conditions pour être qualifié d'importance vitale postérieurement à sa mise en service.

Lorsque l'opérateur d'importance vitale retire de la liste un des systèmes précédemment déclaré, il en informe sans délai l'Agence Monégasque de Sécurité Numérique en en précisant les raisons.

ART. 4.

Tout opérateur d'importance vitale déclare, à l'Agence Monégasque de Sécurité Numérique, chaque incident qui relève d'un des types d'incidents figurant à l'annexe VII du présent arrêté au moyen du formulaire de déclaration de l'annexe III, selon le moyen approprié à la sensibilité des informations déclarées.

Les informations contenues dans ledit formulaire sont couvertes par le secret professionnel et, le cas échéant, par le secret de sécurité nationale tel que prévu par la loi n° 1.430 du 13 juillet 2016, susvisée. Leur divulgation est punie des peines de l'article 308 du Code pénal et de celles prévues par l'article 19 de la loi n° 1.430 du 13 juillet 2016, précitée.

ART. 5.

Tout opérateur d'importance vitale communique à l'Agence Monégasque de Sécurité Numérique les coordonnées des personnes à habiliter au niveau Confidentiel de Sécurité Nationale, au sens de l'arrêté ministériel n° 2016-723 du 12 décembre 2016, modifié, susvisé, chargées de le représenter, dans un délai de trois mois à compter de l'entrée en vigueur du présent arrêté ou de sa désignation comme opérateur d'importance vitale.

ART. 6.

Les annexes V, VI et VII du présent arrêté sont spécifiques à chaque secteur d'importance vitale ou à chaque opérateur d'importance vitale. Par application des dispositions de l'arrêté ministériel n° 2016-723 du 12 décembre 2016, modifié, susvisé, ne donnent lieu à publication que le titre des annexes V, VI et VII, précitées. Le contenu desdites annexes est notifié aux personnes ayant le besoin d'en connaître de chaque opérateur d'importance vitale.

ART. 7.

Le Secrétaire Général du Gouvernement est chargé de l'exécution du présent arrêté.

Fait à Monaco, en l'Hôtel du Gouvernement, le huit novembre deux mille dix-huit.

Le Ministre d'État,
S. TELLE.

RÈGLES DE SÉCURITÉ NÉCESSAIRES À LA PROTECTION DES SYSTÈMES D'INFORMATION DES OPÉRATEURS D'IMPORTANCE VITALE

Annexes à l'Arrêté Ministériel n° 2018-1053 du 8 novembre 2018

SOMMAIRE

ANNEXE I

RÈGLES DE SÉCURITÉ

1. Règle relative à la politique de sécurité des systèmes d'information

L'opérateur d'importance vitale élabore, tient à jour et met en œuvre une politique de sécurité des systèmes d'information (PSSI) dont le périmètre couvre les systèmes d'information d'importance vitale (SIIV).

Ladite PSSI décrit l'ensemble des moyens organisationnels et techniques mis en œuvre par l'opérateur afin d'assurer la sécurité de ces SIIV. En particulier, elle :

- précise les objectifs et les orientations stratégiques en matière de sécurité des SIIV ;
- décrit l'organisation de la gouvernance de la sécurité et notamment les rôles et les responsabilités du personnel interne et du personnel externe (prestataires, fournisseurs, etc.) à l'égard de la sécurité des SIIV ;
- prévoit un plan de sensibilisation :
    - au respect de la législation applicable, notamment des lois n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives et n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique ainsi que des articles 308, 308-2 et 341 du Code pénal en matière de secret professionnel, de respect de la vie privée et, du secret des correspondances ;
    - à la sécurité des SIIV au profit de l'ensemble du personnel ainsi qu'un plan de formation à la sécurité des SIIV au profit des personnes en charge de l'administration et de la sécurité des SIIV et les utilisateurs disposant de droits d'accès étendus aux SIIV ; sont concernées toutes personnes ayant en charge le bon fonctionnement du SIIV ou disposant d'accès privilégiés et de droits spécifiques permettant de modifier des systèmes d'information, des réseaux, des applications, des infrastructures ou des postes de travail constituant les SIIV. Ces droits étendus, dont elles ont besoin pour réaliser leur mission au niveau organisationnel ou technique peuvent permettre d'accéder à des données liées au périmètre qu'elles administrent dans le cadre de leur mission ;
- fixe les mesures de sécurité générales, notamment en matière de contrôle du personnel interne et du personnel externe, de sécurité physique des SIIV, de gestion des ressources matérielles et logicielles des SIIV, de contrôle d'accès aux SIIV, d'exploitation, d'administration des SIIV, des ressources, des réseaux et des postes de travail connectés aux SIIV ;
- définit les procédures suivantes :
    - la procédure d'homologation de sécurité des SIIV ;
    - les procédures de contrôle et d'audit de la sécurité des SIIV ;
    - la procédure de maintien en conditions de sécurité des ressources des SIIV ;
    - la procédure de traitement des incidents de sécurité propres aux SIIV ;
    - les procédures de gestion de crises en cas d'attaques informatiques des SIIV ;
    - les plans de continuité d'activité concernant les SIIV.

Cette PSSI et ses documents d'application seront approuvés formellement par la direction de l'opérateur.

L'opérateur élabore au profit de sa direction, au moins annuellement, un rapport sur sa mise en œuvre et celle de ses documents d'application. Ce rapport, Diffusion Restreinte, précisera notamment l'état des lieux des risques, le niveau de sécurité des SIIV et les actions de sécurisation menées. La PSSI, ses documents d'application et les rapports sur leur mise en œuvre seront tenus à la disposition de l'Agence Monégasque de Sécurité Numérique.

2. Règle relative à l'homologation de sécurité

L'opérateur d'importance vitale procède à l'homologation de sécurité de chaque système d'information d'importance vitale (SIIV), en mettant en œuvre la procédure d'homologation prévue dans sa politique de sécurité des systèmes d'information (PSSI), après avoir procédé si besoin à un audit.

L'homologation d'un système est une décision formelle prise par l'opérateur qui atteste que les risques pesant sur la sécurité de ce système ont été identifiés et que les mesures nécessaires pour le protéger sont mises en œuvre. Elle atteste également que les éventuels risques résiduels ont été identifiés et acceptés par l'opérateur.

Dans le cadre de l'homologation initiale, un audit de la sécurité du SIIV doit être réalisé. Cet audit vise à vérifier l'application et l'efficacité des mesures de sécurité du SIIV et notamment le respect des règles de sécurité mentionnées dans le présent arrêté. L'audit doit aussi permettre d'évaluer le niveau de sécurité du SIIV au regard des menaces et des vulnérabilités connues. Il comporte notamment la réalisation d'un audit d'architecture, d'un audit de configuration et d'un audit organisationnel et physique.

Cet audit est réalisé dans le respect des règles fixées par le référentiel en matière d'audit de sécurité des systèmes d'information, annexé à l'arrêté ministériel n° 2017-625 du 16 août 2017 portant application de l'article 3 de l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique, modifiée. L'opérateur doit recourir pour cet audit à un Prestataire d'Audit de la Sécurité des Systèmes d'Information (PASSI) qualifié au sens de l'arrêté ministériel précité.

À l'issue de l'audit, le PASSI qualifié ayant effectué l'audit élabore un rapport d'audit qui expose les constatations sur les mesures appliquées et sur le respect des règles de sécurité prévues par le présent arrêté. Le rapport précise si le niveau de sécurité atteint est conforme aux objectifs de sécurité, compte tenu des menaces et des vulnérabilités connues. Il formule des recommandations pour remédier aux éventuelles non-conformités et vulnérabilités découvertes et l'opérateur prend les mesures nécessaires en vue de l'homologation.

L'opérateur prend la décision d'homologuer un SIIV sur la base du dossier d'homologation comportant notamment :

- l'analyse de risques et les objectifs de sécurité du SIIV ;
- les mesures de sécurité appliquées au SIIV ;
- les rapports d'audit de la sécurité du SIIV ;
- les risques résiduels et les raisons justifiant leur acceptation.

L'homologation est valable pour une durée maximale de trois ans et est renouvelée au terme de cette période.

Toutefois, la validité de l'homologation est réexaminée par l'opérateur lors de chaque événement ou évolution de nature à modifier le contexte décrit dans le dossier d'homologation.

Lors du renouvellement de l'homologation, la réalisation d'un audit est laissée à l'appréciation de l'opérateur. Cependant un audit réalisé par un PASSI qualifié doit être effectué sur le SIIV tous les 6 ans à compter de l'audit PASSI initial.

L'opérateur tient à la disposition de l'Agence Monégasque de Sécurité Numérique les décisions et dossiers d'homologation, notamment les rapports d'audit. Ces documents sont susceptibles de contenir des informations soumises au secret professionnel dont la divulgation est réprimée par les dispositions de l'article 308 du Code pénal. Ils sont, le cas échéant, couverts par le secret de sécurité nationale tel que prévu par l'article 18 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale.

3. Règle relative à la cartographie

L'opérateur d'importance vitale tient à la disposition de l'Agence Monégasque de Sécurité Numérique, pour chaque système d'information d'importance vitale (SIIV), les éléments de cartographie suivants :

- les noms et les fonctions des applications, supportant les activités de l'opérateur pour les missions d'intérêt vital, installées sur le SIIV ;
- le cas échéant, les plages d'adresses IP de sortie du SIIV vers internet ou un réseau tiers, ou accessibles depuis ces réseaux ;
- le cas échéant, les plages d'adresses IP associées aux différents sous-réseaux composant le SIIV ;
- la description fonctionnelle et les localisations géographiques d'installation du SIIV et de ses différents sous-réseaux ;
- la description fonctionnelle des points d'interconnexion du SIIV et de ses différents sous-réseaux avec des réseaux tiers, notamment la description des équipements et des fonctions de filtrage et de protection mis en œuvre au niveau de ces interconnexions ;
- l'inventaire et l'architecture des dispositifs d'administration du SIIV permettant de réaliser notamment les opérations d'installation à distance, de mise à jour, de supervision, de gestion des configurations, d'authentification ainsi que de gestion des comptes et des droits d'accès ;
- la liste des comptes disposant de droits d'accès privilégiés (appelés « comptes privilégiés ») au SIIV. Cette liste précise pour chaque compte le niveau et le périmètre des droits d'accès associés, notamment les comptes sur lesquels portent ces droits (comptes d'utilisateurs, comptes de messagerie, comptes de processus, etc.) ;
- l'inventaire, l'architecture et le positionnement des services de résolution de noms d'hôte, de messagerie, de relais internet et d'accès distant mis en œuvre par le SIIV.

Les éléments de cartographie ainsi réunis sont des documents susceptibles de contenir des informations soumises au secret professionnel dont la divulgation est réprimée par les dispositions de l'article 308 du Code pénal. Ils sont, le cas échéant, couverts par le secret de sécurité nationale tel que prévu par l'article 18 de la loi n° 1.430 du 13 juillet 2016, précitée.

Sur demande de l'Agence Monégasque de Sécurité Numérique, l'opérateur lui communique les éléments de cartographie mis à jour sur un support électronique, dans un format qui peut être lu par les principaux logiciels bureautiques accessibles au public.

4. Règle relative au maintien en conditions de sécurité

L'opérateur d'importance vitale élabore, tient à jour et met en œuvre une procédure de maintien en conditions de sécurité des ressources matérielles et logicielles de ses systèmes d'information d'importance vitale (SIIV), conformément à sa politique de sécurité des systèmes d'information.

Cette procédure définit les conditions permettant de maintenir le niveau de sécurité des ressources des SIIV en fonction de l'évolution des vulnérabilités et des menaces et notamment la politique d'installation de toute nouvelle version et mesure correctrice de sécurité d'une ressource et les vérifications à effectuer avant l'installation. Elle prévoit que :

- l'opérateur se tient informé des vulnérabilités et des mesures correctrices de sécurité susceptibles de concerner les ressources matérielles et logicielles de ses SIIV qui sont diffusées notamment par les fournisseurs ou les fabricants de ces ressources ou par des centres de prévention et d'alerte, en matière de cyber sécurité tels que le CERT-MC (amsn.gouv.mc) ;
- sauf en cas de difficultés techniques ou opérationnelles justifiées, l'opérateur installe et maintient toutes les ressources matérielles et logicielles de ses SIIV dans des versions supportées par leurs fournisseurs ou leurs fabricants et mises à jour du point de vue de la sécurité ; en cas de difficultés techniques ou opérationnelles les mesures nécessaires devront être prises afin de maintenir le niveau de sécurité décrit dans l'homologation courante ;
- préalablement à l'installation de toute nouvelle version, l'opérateur s'assure de l'origine de cette version et de son intégrité, et analyse l'impact de cette version sur le SIIV concerné d'un point de vue technique et opérationnel ;
- dès qu'il a connaissance d'une mesure correctrice de sécurité concernant une de ses ressources, et sauf en cas de difficultés techniques ou opérationnelles justifiées, l'opérateur en planifie l'installation après avoir effectué les vérifications mentionnées à l'alinéa précédent, et procède à cette installation dans les délais prévus par cette procédure ;
- lorsque des raisons techniques ou opérationnelles le justifient, l'opérateur peut décider, pour certaines ressources de ses SIIV, de ne pas installer une version supportée par le fournisseur ou le fabricant de la ressource concernée ou de ne pas installer une mesure correctrice de sécurité. Dans ce cas, l'opérateur :
    - met en œuvre des mesures techniques ou organisationnelles prévues par cette procédure pour réduire les risques liés à l'utilisation d'une version obsolète ou comportant des vulnérabilités connues ;
    - décrit dans le dossier d'homologation du SIIV concerné ces mesures de réduction des risques et les raisons techniques ou opérationnelles ayant empêché l'installation d'une version supportée ou d'une mesure correctrice de sécurité.

5. Règle relative à la journalisation

L'opérateur d'importance vitale met en œuvre sur chaque système d'information d'importance vitale (SIIV) un système de journalisation qui enregistre les événements relatifs à l'authentification des utilisateurs, à la gestion des comptes et des droits d'accès, à l'accès aux ressources, aux modifications des règles de sécurité du SIIV ainsi qu'au fonctionnement du SIIV.

Le système de journalisation porte sur les équipements suivants lorsqu'ils génèrent les événements mentionnés au 1er alinéa :

- les serveurs applicatifs supportant les activités d'importance vitale ;
- les serveurs d'infrastructure système ;
- les serveurs d'infrastructure réseau ;
- les équipements de sécurité ;
- les postes d'exploitation et de maintenance des systèmes industriels ;
- les équipements réseau ;

- les postes d'administration.

Les événements enregistrés par le système de journalisation sont horodatés au moyen de sources de temps synchronisées. Ils sont, pour chaque SIIV, centralisés et archivés pendant une durée d'un an.

Le format d'archivage des événements permet de réaliser des recherches automatisées sur ces événements.

6. Règle relative à la corrélation et l'analyse de journaux

L'opérateur d'importance vitale met en œuvre un système de corrélation et d'analyse de journaux qui exploite les événements enregistrés par le système de journalisation installé sur chacun des systèmes d'information d'importance vitale (SIIV), afin de détecter des événements susceptibles d'affecter la sécurité des SIIV.

Le système de corrélation et d'analyse de journaux est installé et exploité sur un système d'information mis en place exclusivement à des fins de détection d'événements susceptibles d'affecter la sécurité des systèmes d'information d'importance vitale (SIIV).

Si l'opérateur souhaite mettre en œuvre lui-même un système de corrélation, il doit respecter les règles définies par arrêté ministériel.

L'opérateur peut mandater l'AMSN pour opérer le système de corrélation. Les modalités de mise en œuvre sont définies par arrêté ministériel.

7. Règle relative à la détection

L'opérateur d'importance vitale met en œuvre un système de détection qualifié, en application de l'article 27 de la loi n° 1.435 du 8 novembre 2016, précitée.

Les systèmes de détection qualifiés analysent les flux de données transitant par ceux-ci afin de rechercher des événements susceptibles d'affecter la sécurité des systèmes d'information d'importance vitale (SIIV). Ils sont positionnés de manière à pouvoir analyser l'ensemble des flux échangés entre les SIIV et les systèmes d'information tiers à ceux de l'opérateur.

Les systèmes de détection qualifiés sont choisis parmi ceux figurant sur la liste disponible auprès de l'Agence Monégasque de Sécurité Numérique.

Si l'opérateur souhaite mettre en œuvre lui-même un système de détection qualifié, il doit respecter les règles définies par arrêté ministériel.

L'opérateur peut mandater l'AMSN pour opérer le système de détection qualifié. Les modalités de mise en œuvre sont définies par arrêté ministériel.

8. Règle relative au traitement des attaques par déni de service distribué

L'opérateur met en œuvre un système de détection et de traitement des attaques par déni de service distribué afin de protéger les SIIV concernés par ce type d'attaque.

L'opérateur peut mandater à cet effet un prestataire ad hoc.

9. Règle relative au traitement des incidents de sécurité

L'opérateur d'importance vitale élabore, tient à jour et met en œuvre une procédure de traitement des incidents affectant le fonctionnement ou la sécurité de ses systèmes d'information d'importance vitale (SIIV), conformément à sa politique de sécurité des systèmes d'information.

L'opérateur ou le prestataire mandaté à cet effet procède au traitement des incidents en s'appuyant sur les recommandations publiées par l'Agence Monégasque de Sécurité Numérique.

Un système d'information spécifique, isolé d'internet, doit être mis en place pour traiter les incidents, notamment pour stocker les relevés techniques relatifs aux analyses des incidents. Ce système spécifique de traitement des incidents est cloisonné vis-à-vis du SIIV concerné par l'incident.

L'opérateur conserve les relevés techniques relatifs aux analyses des incidents pendant une durée d'un an. Il tient ces relevés techniques à la disposition de l'Agence Monégasque de Sécurité Numérique.

Les relevés techniques ainsi réunis sont des documents susceptibles de contenir des informations soumises au secret professionnel dont la divulgation est réprimée par les dispositions de l'article 308 du Code pénal. Ils sont, le cas échéant, couverts par le secret de sécurité nationale tel que prévu par la loi n° 1.430 du 13 juillet 2016, précitée.

10. Règle relative au traitement des alertes

L'opérateur d'importance vitale met en place une astreinte lui permettant de prendre connaissance, à tout moment et sans délai, d'informations transmises par l'Agence Monégasque de Sécurité Numérique relatives à des incidents, des vulnérabilités et des menaces. Il met en œuvre une procédure pour traiter les informations ainsi reçues et le cas échéant prendre les mesures de sécurité nécessaires à la protection de ses systèmes d'information d'importance vitale (SIIV).

L'opérateur communique à l'Agence Monégasque de Sécurité Numérique les coordonnées (nom du service, numéro de téléphone, numéro de fax, et adresse électronique) tenues à jour de l'astreinte prévue à l'alinéa précédent.

11. Règle relative à la gestion de crises

L'opérateur d'importance vitale élabore, tient à jour et met en œuvre un plan et des procédures de gestion de crises, conformément à sa politique de sécurité des systèmes d'information, en cas d'attaques informatiques d'un type figurant à l'annexe VII.

Ce plan et ces procédures décrivent les moyens techniques et organisationnels dont dispose l'opérateur pour mettre en œuvre les mesures décidées par le Ministre d'État en cas de crises, notamment les mesures suivantes :

- appliquer une configuration système afin d'éviter les attaques ou d'en limiter les effets. Cette configuration peut viser notamment :
    - à proscrire l'utilisation de supports de stockage amovibles ou la connexion d'équipements nomades aux SIIV de l'opérateur ;
    - à installer une mesure correctrice de sécurité sur un SIIV ;
    - à imposer un protocole de routage ;
- mettre en place des règles de filtrage sur les réseaux ou des configurations particulières sur les SIIV. Cette mesure peut viser notamment :

  - à effectuer des restrictions d'accès sous forme de listes blanches et de listes noires d'utilisateurs ;
  - à bloquer les échanges de fichiers d'un type particulier ;
  - à isoler des sites internet, des applications, ou des équipements informatiques de l'opérateur ;
- isoler du réseau internet les systèmes d'information de l'opérateur. Cette mesure impose de déconnecter physiquement ou logiquement les interfaces réseau des systèmes d'information concernés.

La procédure précise les conditions dans lesquelles ces mesures peuvent être appliquées compte tenu des contraintes notamment techniques ou organisationnelles de mise en œuvre.

12. Règle relative à l'identification

L'opérateur d'importance vitale crée des comptes individuels pour les utilisateurs et pour les processus automatiques accédant aux ressources de ses systèmes d'information d'importance vitale (SIIV).

Lorsque des raisons techniques ou opérationnelles ne permettent pas de créer de comptes individuels pour les utilisateurs ou pour les processus automatiques, l'opérateur met en place des mesures permettant de réduire le risque lié à l'utilisation de comptes partagés et d'assurer la traçabilité de l'utilisation de ces comptes.

Dans ce cas, l'opérateur décrit ces mesures dans le dossier d'homologation du SIIV concerné et les raisons justifiant le recours à des comptes partagés.

L'opérateur désactive sans délai les comptes qui ne sont plus nécessaires dans les limites légales et réglementaires applicables à ce type de données.

13. Règle relative à l'authentification

L'opérateur d'importance vitale protège les accès aux ressources de ses systèmes d'information d'importance vitale (SIIV), que ce soit par un utilisateur ou par un processus automatique, au moyen d'un mécanisme d'authentification basé sur un élément secret.

L'opérateur définit, conformément à sa politique de sécurité des systèmes d'information, les règles de gestion des éléments secrets d'authentification mis en œuvre dans ses SIIV.

Lorsque la ressource le permet techniquement, les éléments secrets d'authentification doivent pouvoir être modifiés par l'opérateur chaque fois que cela est nécessaire. Dans ce cas, l'opérateur respecte les règles suivantes :

- l'opérateur doit modifier les éléments secrets d'authentification lorsqu'ils ont été installés par le fabricant ou le fournisseur de la ressource, avant sa mise en service. À cet effet, l'opérateur s'assure auprès du fabricant ou du fournisseur qu'il dispose des moyens et des droits permettant de réaliser ces opérations ;
- l'élément secret d'authentification d'un compte partagé doit être renouvelé régulièrement et à chaque retrait d'un utilisateur de ce compte ;
- les utilisateurs qui n'en ont pas la responsabilité, ne peuvent pas modifier les éléments secrets d'authentification. Ils ne peuvent pas non plus accéder à ces éléments en clair ;

- lorsque les éléments secrets d'authentification sont des mots de passe, les utilisateurs ne doivent pas les réutiliser entre comptes privilégiés ou entre un compte privilégié et un compte non privilégié ;
- lorsque les éléments secrets d'authentification sont des mots de passe, ceux-ci sont conformes aux règles de l'art telles que celles préconisées par l'Agence Monégasque de Sécurité Numérique, en matière de complexité (longueur du mot de passe et types de caractères), en tenant compte du niveau de complexité maximal permis par la ressource concernée, et en matière de renouvellement.

Lorsque la ressource ne permet pas techniquement de modifier l'élément secret d'authentification, l'opérateur met en place un contrôle d'accès physique à la ressource concernée ainsi que des mesures de traçabilité des accès et de réduction du risque lié à l'utilisation d'un élément secret d'authentification fixe.

L'opérateur décrit dans le dossier d'homologation du SIIV concerné ces mesures et les raisons techniques ayant empêché la modification de l'élément secret d'authentification.

14. Règle relative aux droits d'accès

L'opérateur d'importance vitale définit, conformément à sa politique de sécurité des systèmes d'information, les règles de gestion (ajout, suppression, suspension, délégation, modification, etc.) et d'attribution des droits d'accès aux ressources de ses systèmes d'information d'importance vitale (SIIV), et respecte les règles suivantes :

- l'opérateur n'attribue à un utilisateur ou à un processus automatique les droits d'accès à une ressource que si cet accès est strictement nécessaire à l'exercice des missions de l'utilisateur ou au fonctionnement du processus automatique ;
- l'opérateur définit les accès aux différentes fonctionnalités de cette ressource et en attribue les droits uniquement aux utilisateurs et aux processus automatiques qui en ont strictement le besoin ;
- les droits d'accès sont révisés périodiquement, au moins tous les ans et à chaque modification significative des droits d'accès liés à la mission du ou des bénéficiaires de ces droits. Cette révision porte sur les liens entre les comptes, les droits d'accès associés et les ressources ou les fonctionnalités qui en font l'objet ;
- l'opérateur établit et tient à jour la liste des comptes privilégiés. Toute modification d'un compte privilégié (ajout, suppression, suspension ou modification des droits associés) fait l'objet d'un contrôle formel de l'opérateur destiné à vérifier que les droits d'accès, aux ressources et fonctionnalités sont attribués selon le principe du moindre privilège (seuls les droits strictement nécessaires sont accordés) et en cohérence avec les besoins d'utilisation du compte.

15. Règle relative aux comptes d'administration

L'opérateur d'importance vitale crée des comptes (appelés « comptes d'administration ») destinés aux seules personnes (appelées administrateurs) chargées d'effectuer les opérations d'administration (installation, configuration, gestion, maintenance, supervision, etc.) des ressources de ses systèmes d'information d'importance vitale (SIIV).

L'opérateur définit, conformément à sa politique de sécurité des systèmes d'information, les règles de gestion et d'attribution des comptes d'administration de ses SIIV, et respecte les règles suivantes :

- - l'attribution des droits aux administrateurs respecte le principe du moindre privilège. En particulier, afin de limiter la portée de ces droits individuels, ils sont attribués à chaque administrateur en les restreignant autant que possible au périmètre fonctionnel et technique dont cet administrateur est responsable ;
- un compte d'administration est utilisé exclusivement pour se connecter à un système d'information d'administration (système d'information utilisé pour les opérations d'administration des ressources) ou à une ressource administrée ;
- les opérations d'administration sont effectuées exclusivement à partir de comptes d'administration, et inversement, les comptes d'administration sont utilisés exclusivement pour les opérations d'administration ;
- lorsque l'administration d'une ressource ne peut pas techniquement être effectuée à partir d'un compte spécifique d'administration, l'opérateur met en place des mesures permettant d'assurer la traçabilité et le contrôle des opérations d'administration réalisées sur cette ressource et des mesures de réduction du risque lié à l'utilisation d'un compte non spécifique à l'administration. Il décrit dans le dossier d'homologation du SIIV concerné ces mesures ainsi que les raisons techniques ayant empêché l'utilisation d'un compte d'administration ;
- l'opérateur établit et tient à jour la liste des comptes d'administration de ses SIIV et les gère en tant que comptes privilégiés.

16. Règle relative aux systèmes d'information d'administration

L'opérateur d'importance vitale applique les règles suivantes aux systèmes d'information utilisés pour effectuer l'administration de ses systèmes d'information d'importance vitale (SIIV), qui sont appelés « systèmes d'information d'administration » :

- les ressources matérielles et logicielles des systèmes d'information d'administration sont gérées et configurées par l'opérateur ou, le cas échéant, par le prestataire qu'il a mandaté pour réaliser les opérations d'administration ;
- les ressources matérielles et logicielles des systèmes d'information d'administration sont utilisées exclusivement pour réaliser des opérations d'administration. Cependant, lorsque des raisons techniques ou organisationnelles le justifient, le poste de travail physique de l'administrateur peut être utilisé pour réaliser des opérations autres que des opérations d'administration. Dans ce cas, des mécanismes de durcissement du système d'exploitation du poste de travail et de cloisonnement doivent être mis en place pour permettre d'isoler l'environnement logiciel utilisé pour ces autres opérations de l'environnement logiciel utilisé pour les opérations d'administration ;
- un environnement logiciel utilisé pour effectuer des opérations d'administration ne doit pas être utilisé à d'autres fins. Il ne doit, en aucun cas, être utilisé pour accéder à des sites ou serveurs de messagerie sur internet ;
- un utilisateur ne doit pas se connecter à un système d'information d'administration au moyen d'un environnement logiciel utilisé pour d'autres fonctions que des opérations d'administration ;
- les flux de données associés à des opérations autres que des opérations d'administration doivent, lorsqu'ils transitent sur les systèmes d'information d'administration, être cloisonnés au moyen de mécanismes de chiffrement et d'authentification conformes aux règles définies dans le Référentiel Général de Sécurité annexé à l'arrêté ministériel n° 2017-835 du 29 novembre 2017 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du

29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée ;

- les systèmes d'information d'administration sont connectés aux ressources à administrer au travers d'une liaison réseau physique utilisée exclusivement pour les opérations d'administration. Ces ressources sont administrées au travers de leur interface d'administration physique. L'opérateur peut administrer une ressource au travers d'une liaison réseau logique ou de son interface d'administration logique, à la condition de mettre en œuvre des mesures de réduction du risque. Dans ce cas, il décrit ces mesures et leur justification dans le dossier d'homologation du SIIV concerné ;
- lorsqu'ils ne circulent pas dans le système d'information d'administration, les flux d'administration sont protégés par des mécanismes de chiffrement et d'authentification conformes aux règles définies dans le Référentiel Général de Sécurité annexé à l'arrêté ministériel n° 2017-835 du 29 novembre 2017, précité. Si le chiffrement et l'authentification de ces flux ne sont pas possibles pour des raisons techniques, l'opérateur met en œuvre des mesures permettant de protéger ces flux en confidentialité et en intégrité et de renforcer le contrôle et la traçabilité des opérations d'administration. Dans ce cas, il décrit ces mesures et leur justification dans le dossier d'homologation du SIIV concerné ;
- les journaux enregistrant les événements générés par les ressources utilisées par les administrateurs ne contiennent aucun mot de passe en clair ou sous forme de condensat.

17. Règle relative au cloisonnement

L'opérateur d'importance vitale procède au cloisonnement de ses systèmes d'information d'importance vitale (SIIV) afin de limiter la propagation des attaques informatiques au sein de ses systèmes ou ses sous-systèmes. Il respecte les règles suivantes :

- chaque SIIV est cloisonné physiquement ou logiquement vis-à-vis des autres systèmes de l'opérateur ou des systèmes tiers ;
- lorsqu'un SIIV est lui-même constitué de sous-systèmes, ceux-ci sont cloisonnés entre eux physiquement ou logiquement. Un sous-système peut être constitué pour assurer une fonctionnalité ou un ensemble homogène de fonctionnalités d'un SIIV ou encore pour isoler des ressources d'un SIIV nécessitant un même besoin de sécurité ;
- seules les interconnexions strictement nécessaires au bon fonctionnement et à la sécurité d'un SIIV sont mises en place entre le SIIV et les autres systèmes ou entre les sous-systèmes du SIIV.

L'opérateur décrit dans le dossier d'homologation de chaque SIIV les mécanismes de cloisonnement qu'il met en place.

18. Règle relative au filtrage

L'opérateur d'importance vitale met en place des mécanismes de filtrage des flux de données circulant dans ses systèmes d'information d'importance vitale (SIIV) afin de bloquer la circulation des flux inutiles au fonctionnement de ses systèmes et susceptibles de faciliter des attaques informatiques. Il respecte les règles suivantes :

- l'opérateur définit les règles de filtrage des flux de données (filtrage sur adresse réseau, sur protocole, sur numéro de port, etc.) permettant de limiter autant que possible la circulation des flux aux seuls flux de données nécessaires au fonctionnement et à la sécurité de ses SIIV ;

- les flux entrants et sortants des SIIV ainsi que les flux entre sous-systèmes des SIIV sont filtrés au niveau de leurs interconnexions de manière à ne permettre que la circulation des seuls flux strictement nécessaires au fonctionnement et à la sécurité des SIIV. Les flux qui ne sont pas conformes aux règles de filtrage sont bloqués ;
- l'opérateur établit et tient à jour une liste des règles de filtrage mentionnant l'ensemble des règles en vigueur ou supprimées depuis moins d'un an. Cette liste précise pour chaque règle :
    - le motif et la date de la mise en œuvre, de la modification ou de la suppression de la règle ;
    - les modalités techniques de mise en œuvre de la règle.

L'opérateur décrit dans le dossier d'homologation de chaque SIIV les mécanismes de filtrage qu'il met en place.

19. Règle relative aux accès à distance

L'opérateur d'importance vitale protège les accès à ses systèmes d'information d'importance vitale (SIIV) effectués à travers des réseaux tiers. En particulier, lorsque l'opérateur ou un prestataire qu'il a mandaté à cet effet accède à un SIIV à travers un réseau tiers à ceux de l'opérateur ou du prestataire, l'opérateur applique ou fait appliquer à son prestataire les règles suivantes :

- l'accès au SIIV est protégé par des mécanismes de chiffrement et d'authentification conformes aux règles définies dans le Référentiel Général de Sécurité, annexé à l'arrêté ministériel n° 2017‑835 du 29 novembre 2017, précité ;
- le mécanisme d'authentification utilisé est renforcé en mettant en œuvre une authentification à double facteur (authentification basée à la fois sur un élément secret et un autre élément propre à l'utilisateur) ;
- les équipements utilisés pour accéder au SIIV sont gérés et configurés par l'opérateur ou, le cas échéant, par le prestataire. Les mémoires de masse de ces équipements sont en permanence protégées par des mécanismes de chiffrement et d'authentification conformes aux règles définies dans le Référentiel Général de Sécurité, annexé à l'arrêté ministériel n° 2017-835 du 29 novembre 2017, précité.

20. Règle relative à l'installation de services et d'équipements

L'opérateur d'importance vitale respecte les règles suivantes lorsqu'il installe des services et des équipements sur ses systèmes d'information d'importance vitale (SIIV) :

- l'opérateur installe sur ses SIIV les seuls services et fonctionnalités qui sont indispensables au fonctionnement ou à la sécurité de ses SIIV. L'opérateur désactive les services et les fonctionnalités qui ne sont pas indispensables, notamment ceux installés par défaut, et les désinstalle si cela est possible. Lorsque la désinstallation n'est pas possible, l'opérateur le mentionne dans le dossier d'homologation du SIIV concerné en précisant les services et fonctionnalités concernés et les mesures de réduction du risque mises en œuvre ;
- l'opérateur ne connecte à ses SIIV que des équipements, matériels périphériques et supports amovibles qu'il a dûment répertoriés et qui sont indispensables au fonctionnement ou à la sécurité de ses SIIV ;
- les supports amovibles inscriptibles connectés aux SIIV sont utilisés exclusivement pour les besoins de ces SIIV ;

- l'opérateur procède, avant chaque utilisation de supports amovibles, à l'analyse de leur contenu, notamment à la recherche de code malveillant. L'opérateur met en place, sur les équipements auxquels sont connectés ces supports amovibles, des mécanismes de protection contre les risques d'exécution de code malveillant provenant de ces supports.

21. Règle relative aux indicateurs

L'opérateur d'importance vitale évalue le niveau de sécurité de ses SIIV à l'aide du document de l'annexe IV disponible et téléchargeable sur le site https://amsn.gouv.mc/oiv.

L'opérateur précise pour chaque indicateur, s'il est :

- Documenté ou non mais non appliqué ;
- Appliqué mais non documenté ;
- Appliqué documenté ;
- Appliqué, documenté, et contrôlé ;
- Non applicable ; dans ce cas l'opérateur devra en expliquer les raisons.

Lorsqu'un indicateur évolue de façon significative par rapport à l'évaluation précédente, l'opérateur en précise les raisons.

Les indicateurs ainsi réunis sont des documents susceptibles de contenir des informations soumises au secret professionnel dont la divulgation est réprimée par les dispositions de l'article 308 du Code pénal. Ils sont, le cas échéant, couverts par le secret de sécurité nationale tel que prévu par la loi n° 1.430 du 13 juillet 2016, précitée.

L'opérateur communique, une fois par an, à l'Agence Monégasque de Sécurité Numérique, ces indicateurs mis à jour, selon le moyen approprié à la sensibilité des informations déclarées.

ANNEXE II

FORMULAIRE DE DÉCLARATION D'UN SYSTÈME D'INFORMATION D'IMPORTANCE VITALE

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

ANNEXE III

FORMULAIRE DE DÉCLARATION D'UN INCIDENT DE SÉCURITÉ

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

ANNEXE IV

TABLEAU D'ÉVALUATION DU NIVEAU DE SÉCURITÉ DES SYSTÈMES D'INFORMATION D'IMPORTANCE VITALE

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

ANNEXE V

DÉLAIS D'APPLICATION DES RÈGLES DE SÉCURITÉ

Conformément aux dispositions de l'article 6 de l'arrêté ministériel n° 2018-1053 du 8 novembre 2018 portant application de l'article 27 de la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique, le contenu de cette annexe est notifié aux personnes ayant besoin d'en connaître de chaque opérateur d'importance vitale.

n°	RÈGLES DE SÉCURITÉ	DÉLAIS D'APPLICATION
1	Règle relative à la politique de sécurité des systèmes d'information	
2	Règle relative à l'homologation de sécurité	
3	Règle relative à la cartographie	
4	Règle relative au maintien en conditions de sécurité	
5	Règle relative à la journalisation	
6	Règle relative à la corrélation et l'analyse de journaux	
7	Règle relative à la détection	
8	Règle relative au traitement des attaques par déni de service distribué	
9	Règle relative au traitement des incidents de sécurité	
10	Règle relative au traitement des alertes	
11	Règle relative à la gestion de crises	
12	Règle relative à l'identification	
13	Règle relative à l'authentification	
14	Règle relative aux droits d'accès	
15	Règle relative aux comptes d'administration	
16	Règle relative aux systèmes d'information d'administration	

17	Règle relative au cloisonnement	
18	Règle relative au filtrage	
19	Règle relative aux accès à distance	
20	Règle relative à l’installation de services et d’équipements	
21	Règle relative aux indicateurs	

ANNEXE VI

TYPES DE SYSTÈME D'INFORMATION D'IMPORTANCE VITALE

Conformément aux dispositions de l'article 6 de l'arrêté ministériel n° 2018-1053 du 8 novembre 2018 portant application de l'article 27 de la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique, le contenu de cette annexe est notifié aux personnes ayant besoin d'en connaître de chaque opérateur d'importance vitale.

ANNEXE VII

TYPES D'INCIDENT

Conformément aux dispositions de l'article 6 de l'arrêté ministériel n° 2018-1053 du 8 novembre 2018 portant application de l'article 27 de la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique, le contenu de cette annexe est notifié aux personnes ayant besoin d'en connaître de chaque opérateur d'importance vitale.