Arrêté Ministériel n° 2019-791 du 17 septembre 2019 portant application de l'article 2, a) de l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique, modifiée

Nous, Ministre d'État de la Principauté,

Vu la Constitution ;

Vu la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée ;

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° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'administration et l'administré, modifiée ;

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, susvisée, modifié ;

Vu 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, susvisée ;

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, modifiée, susvisée ;

Vu l'arrêté ministériel n° 2017-625 du 16 août 2017 portant application de l'article 3 c) de l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015, modifiée, susvisée ;

Vu l'arrêté ministériel n° 2018-1108 du 28 novembre 2018 portant application de l'article 3 f) de l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015, modifiée, susvisée ;

Vu la délibération du Conseil de Gouvernement en date du 4 septembre 2019 ;

ARRÊTONS :

ARTICLE PREMIER.

Les systèmes d'information sensibles sont ceux qui traitent d'informations dont la compromission, l'endommagement, l'effacement, la détérioration, la modification, l'altération, ou la divulgation à des personnes non autorisées, est de nature à nuire à la continuité du fonctionnement des entités publiques ou privées mettant en œuvre de tels systèmes d'information.

Chaque entité publique ou privée détermine la classification des informations sensibles selon les critères qu'elle fixe en fonction des composantes suivantes : disponibilité, intégrité, confidentialité et traçabilité, et les marque par les moyens de son choix.

ART. 2.

Les règles destinées à garantir la sécurité des systèmes d'information sensibles sont annexées au présent arrêté.

Des dérogations auxdites règles peuvent être accordées, au cas par cas et pour une durée déterminée, par le Directeur de l'Agence Monégasque de Sécurité Numérique, sur la base de l'analyse de risque réalisée par l'entité concernée.

ART. 3.

Les entités publiques ou privées, ayant mis en service un système d'informations sensibles avant la date d'entrée en vigueur du présent arrêté ou dans les six mois suivant cette date, disposent, à compter de celle-ci, d'un délai de trois ans pour mettre leur système d'informations sensibles en conformité avec ces dispositions.

Durant ce délai, les entités établissent et tiennent à la disposition de l'Agence Monégasque de Sécurité Numérique la liste des manquements aux règles prévues par l'annexe au présent arrêté.

ART. 4.

Le Ministre d'État est chargé de l’exécution du présent arrêté.

Fait à Monaco, en l’Hôtel du Gouvernement, le dix-sept septembre deux mille dix-neuf.

Le Ministre d’État,
S. TELLE.

DISPOSITIONS RELATIVES À LA PROTECTION DES SYSTÈMES D'INFORMATION SENSIBLES

Annexe à l'arrêté ministériel n° 2019-791 du 17 septembre 2019

SOMMAIRE

1. Objet de la présente annexe

La présente annexe définit les règles relatives à la protection des systèmes d'information dits sensibles traitant des informations sensibles Elle s'adresse à l'ensemble des personnes physiques ou morales intervenant sur ces systèmes d'information.

Le respect des règles précitées contribue à prévenir la sécurité des informations sensibles.

2. Définition et périmètre

2.1. Détermination de la sensibilité des informations

Chaque entité publique ou privée mettant en œuvre un système d'information sensible :

- identifie les informations sensibles qu'elle met en œuvre conformément à l'article 2 de l'arrêté ministériel n° 2019-791 du 17 septembre 2019 ;
- définit le marquage de ces informations ;
- marque cette information selon les modèles définis par l'entité ;
- applique des mesures de protection décrites ci-après.

Lorsque les informations sensibles transitent entre plusieurs entités, leur niveau de sensibilité est explicitement mentionné par l'entité émettrice afin qu'elles soient protégées en conséquence par l'entité destinataire en termes de disponibilité, d'intégrité, de confidentialité et de traçabilité, pendant et après leur transit.

2.2. Principes appliqués

Les règles décrites dans la présente annexe s'appuient sur cinq principes :

- mettre en place une organisation consacrée à la sécurité des systèmes d'information incluant des volets préventifs et défensifs et reposant sur des moyens humains, matériels et financiers identifiés ;
- évaluer les risques périodiquement dans une démarche d'amélioration continue de la sécurité de chaque système pendant sa durée de vie ;
- défendre en profondeur avec plusieurs dispositifs successifs de sécurité, en s'assurant dès la conception que si l'une des mesures de sécurité est compromise ou défaillante, d'autres mesures assurent la protection des informations sensibles ;
- respecter les règles élémentaires d'hygiène informatique[1] mises en œuvre par des administrateurs de systèmes d'information formés à cet effet ;
- recourir :
  - à, quand ils existent, des produits de sécurité qualifiés[2] au sens du Référentiel Général de Sécurité[3], 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 ;
  - à des prestataires de services de confiance qualifiés par l'Agence Monégasque de Sécurité Numérique ;

[1] https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf
[2] https://www.ssi.gouv.fr/administration/visa-de-securite/visasde-securite-le-catalogue/
[3] RGS annexé à l'arrêté ministériel n° 2017-835 du 29 novembre 2017

- ainsi qu'aux référentiels et guides relatifs à la sécurité des systèmes d'information édités par ladite Agence.

3. Application des règles aux systèmes d'information sensibles

Les entités publiques qui mettent en œuvre des systèmes d'information sensibles appliquent à ces systèmes d'information :

- la politique de sécurité des systèmes d'information de l'État (PSSI-E)[4] en intégralité, sauf dérogation formelle accordée par le Directeur de l'Agence Monégasque de Sécurité Numérique ;
- les règles annexées à 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.

Les entités privées hors du champ d'application de la PSSI-E, qui mettent en œuvre des systèmes d'information sensibles, appliquent les mêmes règles que celles prévues dans la PSSI-E, en les adaptant à leur PSSI ainsi que les règles prévues au paragraphe 4 ci-après. Toutes les adaptations ou les non-applications des règles de la PSSI-E doivent être clairement identifiées, tracées et expliquées dans un document visé par l'autorité d'homologation de ladite entité.

4. Protection des systèmes d'information sensibles

4.1. Traitement des informations sensibles

Le traitement des informations sensibles, notamment leur stockage et leur diffusion, s'effectue sur des réseaux homologués et protégés par des matériels qualifiés par l'Agence Monégasque de Sécurité Numérique.

Les informations sensibles sont chiffrées à l'aide de moyens qualifiés par l'Agence Monégasque de Sécurité Numérique, dès lors qu'elles transitent ou sont stockées en dehors d'une zone physiquement protégée dans les conditions prévues au paragraphe 4.2 (en particulier sur Internet). En effet, toute connexion à un réseau public constitue en elle-même une vulnérabilité qui peut facilement conduire à la compromission d'informations.

4.2. Protection physique des locaux

Les mesures de sécurité physique sont fixées en proportion des menaces déterminées par « l'analyse des risques » effectuée pour l'homologation. Elles ont pour objectif à la fois de prévenir la perte, l'altération ou la détérioration des systèmes d'information sensibles en :

- défendant par une barrière périmétrique physique les limites de la zone à protéger où se trouve le système d'information sensible ;
- dissuadant l'accès non autorisé par toute mesure physique appropriée ;
- contrôlant l'accès des locaux de façon électronique, électromécanique ou humaine ;
- conservant la traçabilité des accès ;
- protégeant des intrusions par un système de détection (ce système peut remplacer une barrière périmétrique ou la compléter pour renforcer le niveau de sécurité) ;

[4] PSSI-E : annexée à l'arrêté ministériel n° 2017-56 du 01/02/2017 portant application 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.

- mettant en place les moyens d'éviter et de détecter les incidents physiques tels que les défauts d'alimentation ou de climatisation, les incendies et les dégâts des eaux.

4.3. Externalisation

En cas d'externalisation d'une prestation concernant un système d'information sensible, le contrat qui lie le commanditaire et le prestataire :

- intègre un plan d'assurance sécurité[5] ;
- fait appliquer aux prestataires les règles prévues dans l'arrêté ministériel n° 2019-791 du 17 septembre 2019 et la présente annexe.

Dans le cas d'une prestation d'hébergement informatique, l'entité doit, sauf dérogation, faire appel à un Prestataire d'Informatique en Nuage et d'Hébergement (PINH), qualifié, dont le référentiel est annexé à l'arrêté ministériel n° 2018-1108 du 26 novembre 2018.

4.4. Utilisation en milieu non maîtrisé

Les accès aux systèmes d'information sensibles par des dispositifs nomades (ordinateurs portables, média amovibles, téléphones, etc.) sont chiffrées par des moyens validés par l'Agence Monégasque de Sécurité Numérique.

Les moyens de stockage des dispositifs nomades pouvant se connecter aux systèmes d'information sensibles, doivent être chiffrés et permettre l'effacement à distance, afin de limiter le risque de divulgation en cas de perte ou de vol, par des moyens validés par l'Agence Monégasque de Sécurité Numérique.

La consultation de documents électroniques sur les systèmes d'information sensibles dans les lieux publics est entourée de précautions particulières :

- utilisation obligatoire d'un filtre de confidentialité sur l'écran ;
- surveillance continuelle du poste nomade lui-même.

La connexion d'équipements personnels à un système d'information sensible est proscrite en l'absence d'un système de gestion des terminaux mobiles mis en œuvre par l'administrateur du système d'information sensible.

4.5. Supports audiovisuels

Avant de diffuser des informations sensibles, portant une marque de confidentialité destinée :

- à restreindre leur diffusion à un domaine spécifique ou à un groupe de personne spécifique et précisée par une mention particulière,
- ou à garantir leur protection, avec un support audiovisuel (vidéo projecteur, vidéo conférence, …), le responsable de la diffusion vérifie le besoin d'en connaître des participants.

À cette occasion, les éventuelles captations photographiques, vidéo ou audio des informations font l'objet d'une attention particulière. Le cas échéant, ces captations sont interdites.

[5] https://amsn.gouv.mc/Informations-pratiques/Guidespratiques/Risques-de-l-infogerance/

4.6. Interconnexion d'un système d'information sensible à d'autres réseaux

Toute interconnexion d'un système d'information sensible à un autre système d'information doit être effectuée à l'aide de matériels qualifiés par l'Agence Monégasque de Sécurité Numérique.

Pour une interconnexion à un système moins protégé ou si les données transitent sur des réseaux d'une moindre protection (Internet par exemple), les données sensibles doivent être chiffrées par un moyen qualifié par l'Agence Monégasque de Sécurité Numérique, permettant de garantir que les données seront protégées en confidentialité et en intégrité de l'origine à la destination.

L'interconnexion à un réseau Confidentiel de Sécurité Nationale (CSN) est interdite.

5. Exemples d'informations sensibles permettant de qualifier les systèmes d'information de « systèmes d'information sensibles »

Disponibles et téléchargeables sur https://amsn.gouv.mc/Informations-pratiques/Guides-pratiques

6. Exemples de modèles de marquage d'informations sensibles

Disponibles et téléchargeables sur https://amsn.gouv.mc/Informations-pratiques/Guides-pratiques