# Arrêté ministériel n° 2022-331 du 13 juin 2022 portant application de l'article 23 de la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique, fixant les mesures de sécurité des systèmes d'information de l'État

| | |
|---|---|
| *Type* | Texte réglementaire |
| *Nature* | Arrêté ministériel |
| *Date du texte* | 13 juin 2022 |
| *Publication* | Journal de Monaco du 24 juin 2022[1 p.6] |
| *Thématiques* | Infractions économiques, fiscales et financières ; Nouvelles technologies et télécommunications ; Lutte contre le terrorisme et le crime organisé |

Vu la Constitution ;

Vu la loi n° 1.383 du 2 août 2011 pour une Principauté numérique, 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° 8.099 du 16 juin 2020 fixant les conditions d'application de la loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée, relative aux services de confiance ;

Vu l'Ordonnance Souveraine n° 8.504 du 18 février 2021 portant application de l'article 24 de la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique ;

Vu l'arrêté ministériel n° 2015-703 du 26 novembre 2015 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 ;

Vu l'arrêté ministériel n° 2017-56 du 1er février 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 ;

Vu l'arrêté ministériel n° 2018-281 du 4 avril 2018 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 ;

Vu la délibération du Conseil de Gouvernement en date du 1er juin 2022 ;

## Article 1er

Au sens du présent arrêté, on entend par :

- « *Administrateur réseaux et systèmes d'information* », toute personne ayant en charge le bon fonctionnement du système d'information et/ou disposant d'accès privilégiés et de droits spécifiques permettant de modifier des systèmes d'information, des réseaux, des applications, des données, des infrastructures et/ou des postes de travail. Dans la suite de l'arrêté, le terme « *administrateur* » fait référence au terme « *administrateur réseaux et systèmes d'information* » ;

- « *Autorité d'homologation* », la personne physique qui, après instruction du dossier d'homologation, prononce l'homologation de sécurité du système d'information, c'est-à-dire prend la décision d'accepter les risques résiduels identifiés sur le système d'information. L'autorité d'homologation doit être désignée à un niveau hiérarchique suffisant pour assumer toutes les responsabilités ;

- « *Commission d'homologation* », la commission chargée d'assister l'autorité d'homologation pour l'instruction de l'homologation et d'en préparer la décision. Elle est mise en place 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 et un représentant de l'Agence Monégasque de Sécurité Numérique ;

- « *Responsable de la Sécurité des Systèmes d'Information des services exécutifs de l'État* », la personne spécialisée en charge de la mise en œuvre et du respect de la Politique de Sécurité des Systèmes d'Information pour lesdits services. Dans la suite de l'arrêté, le terme « *Responsable de la Sécurité des Systèmes d'Information* » fait référence au terme « *Responsable de la Sécurité des Systèmes d'Information des services exécutifs de l'État* » ;

- « *Système d'information des services exécutifs de l'État* », 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, concourant aux missions des services exécutifs de l'État au sens de l'article 44 de la Constitution. Dans la suite de l'arrêté, le terme « *systèmes d'information* » fait référence au terme « *système d'information des services exécutifs de l'État* ».

## Article 2

La Politique de Sécurité des Systèmes d'Information de l'État (PSSI-E) contribue à assurer la continuité des activités de l'État, à prévenir la fuite d'informations et à renforcer la confiance des administrés et des entreprises dans les téléservices.

La Politique de Sécurité des Systèmes d'Information de l'État s'applique à tous les systèmes d'information des services exécutifs de l'État, y compris à ceux pilotant des systèmes industriels et aux systèmes de contrôle et d'acquisition de données pour le fonctionnement d'automates, ainsi qu'aux réseaux de communications électroniques de l'État. Elle s'impose également aux systèmes d'information traitant des informations classifiées dès lors qu'elles viennent en complément, et non en contradiction, de celles spécifiques à ces systèmes.

Les fonctionnaires et agents publics ou les préposés des services publics visés au précédent alinéa sont tenus de respecter les obligations professionnelles et les règles de sécurité énoncées dans le présent arrêté et ses annexes qui constituent la Politique de Sécurité des Systèmes d'Information de l'État (PSSI-E).

Les autres personnes publiques peuvent définir et appliquer en lieu et place de la Politique de Sécurité des Systèmes d'Information de l'État une politique de sécurité spécifique à leurs systèmes d'information et à leur contexte organisationnel. Ils en informent alors le Ministre d'État.

Les fonctionnaires et agents publics ou préposés des services publics sont tenus de respecter les dispositions des chartes, politiques et procédures prises en application du présent arrêté sous peine de sanctions conformément au régime disciplinaire applicable, sans préjudice d'une action juridictionnelle qu'elle soit de nature administrative, civile ou pénale.

### Article 3

Les systèmes d'information considérés comme sensibles, en raison de leurs besoins en disponibilité, intégrité ou confidentialité, sont hébergés sur le territoire de la Principauté.

Toutefois, des dérogations temporaires ou définitives peuvent être accordées par le Ministre d'État après avis du Directeur de l'Agence Monégasque de Sécurité Numérique. L'Agence Monégasque de Sécurité Numérique tient à jour la liste des dérogations.

### Article 4

Le Responsable de la Sécurité des Systèmes d'Information agit en toute indépendance vis-à-vis des équipes œuvrant à la mise en œuvre ou à l'opération des systèmes d'information.

Il est chargé de la mise en œuvre et du suivi de la Politique de Sécurité des Systèmes d'Information de l'État sur les systèmes d'information. À ce titre il a pour mission :

- de coordonner les actions permettant l'intégration de la sécurité dans les projets d'évolution ou de construction des systèmes d'information ;
- de mettre en œuvre et de piloter les démarches d'homologation de sécurité afin d'évaluer les risques encourus par les systèmes d'information. Pour ce faire, il coordonne la réalisation des analyses de risques et des audits de sécurité pour les systèmes d'information, assure le suivi des plans d'actions de remédiation et le renouvellement des homologations ;
- de définir et de piloter des projets visant à accélérer la mise en conformité à la Politique de Sécurité des Systèmes d'Information de l'État des systèmes d'information ;
- de réaliser des actions de contrôle du niveau de sécurité de ces systèmes d'information et demande aux services exécutifs de l'État concernés la mise en œuvre des actions correctives nécessaires ;
- de mettre en place avec l'aide des services exécutifs de l'État concernés les processus de continuité d'activité et ceux leur permettant de faire face aux alertes, aux incidents de sécurité et aux situations d'urgence des systèmes d'information ;
- de s'assurer de l'intégration des clauses contractuelles liées à la sécurité des systèmes d'information dans tout contrat ou convention signé par les services exécutifs de l'État ;
- de tenir à jour annuellement un inventaire des systèmes d'information et de la correcte évaluation de leur sensibilité ;
- de conduire des actions de sensibilisation et formation à la sécurité des systèmes d'information auprès des fonctionnaires et agents publics ou préposés des services publics.

Il a également pour mission :

- de coordonner le développement et le maintien à jour des politiques d'application déclinant la Politique de Sécurité des Systèmes d'Information de l'État, des clauses contractuelles de sécurité standards dont celles imposées aux prestataires et sous-traitants annexées au présent arrêté ;
- de contribuer à l'établissement et à la mise à jour des Chartes s'appliquant aux utilisateurs et administrateurs nécessaires à la mise en application de la Politique de Sécurité des Systèmes d'Information de l'État.

Le Responsable de la Sécurité des Systèmes d'Information peut être assisté dans ses missions par des Correspondants Sécurité des Systèmes d'Information (CSSI) désignés par les Conseillers de Gouvernement-Ministres au sein de leur département ministériel ou de leurs services. Le Responsable de la Sécurité des Systèmes d'Information et l'Agence Monégasque de Sécurité Numérique réalisent l'évaluation des compétences des personnels candidats à la fonction de Correspondant Sécurité des Systèmes d'Information. Le Responsable de la Sécurité des Systèmes d'Information tient à jour la liste des Correspondants Sécurité des Systèmes d'Information.

### Article 5

Le Correspondant Sécurité des Systèmes d'Information s'assure de la conformité des systèmes d'information à la Politique de Sécurité des Systèmes d'Information de l'État au sein du département ministériel ou du service auquel il est rattaché. Il a pour missions de :

- collecter les besoins de son service ou département en matière de sécurité des systèmes d'information ;

- piloter la mise en œuvre des plans d'actions issus des audits de sécurité et/ou des évaluations de conformité à la Politique de Sécurité des Systèmes d'Information de l'État en coordination avec les autorités concernées et avec le Responsable de la Sécurité des Systèmes d'Information ;
- assister le Responsable de la Sécurité des Systèmes d'Information dans l'exécution des actions régulières de contrôle du niveau de sécurité, et notamment dans la réalisation des revues de droits d'accès ;
- conduire les projets transverses en matière de sécurité des systèmes d'information sur son périmètre ;
- assister les services dans leurs démarches d'homologation des systèmes d'information, dans l'identification des besoins de sécurité et dans le suivi des mesures de réduction des risques ;
- contrôler la bonne mise en œuvre des politiques d'application sur son périmètre ;
- s'assurer de la mise en œuvre des clauses contractuelles de sécurité par les prestataires et sous-traitants sous la responsabilité des services concernés ;
- aider à la rédaction voire, le cas échéant réaliser le tableau d'évaluation relatif au bilan annuel prévu à l'article 7.

### Article 6

Tout système d'information fait l'objet d'une décision d'homologation préalablement à son emploi, prononcée par l'autorité d'homologation qui peut être le Ministre d'État, les Conseillers de Gouvernement-Ministres, le Secrétaire Général du Gouvernement ou leur représentant.

Une analyse de risques, permettant une prise en compte préventive de la sécurité et adaptée aux enjeux du système d'information considéré est alors nécessaire.

Le Responsable de la Sécurité des Systèmes d'Information met en place une commission d'homologation. Cette commission est composée :

- de l'autorité d'homologation ou son représentant ;
- du président de la commission d'homologation qui est responsable de la vérification *in fine* de la bonne sécurité du système ;
- de l'autorité cliente qui est responsable de l'activité métier portée par le système d'information ;
- de l'autorité d'emploi qui définit l'expression du besoin fonctionnel, le cahier des charges fonctionnel et les performances attendues ;
- de l'autorité d'exploitation qui est en charge du maintien en conditions opérationnelles et de sécurité du système d'information ;
- du responsable de la sécurité du système d'information projeté ;
- du Responsable de la Sécurité des Systèmes d'Information ou son représentant ;
- du Directeur de l'Agence Monégasque de Sécurité Numérique ou son représentant.

La décision d'homologation, proposée par le président de la commission d'homologation à l'autorité d'homologation, est prise au vu des résultats de l'analyse de risques.

La décision d'homologation intervient avant la mise en service opérationnelle du système d'information.

De façon exceptionnelle, lorsque l'urgence opérationnelle le requiert, il peut être procédé à une mise en service provisoire, sans attendre l'homologation du système d'information, en tenant compte de l'avancement de la procédure d'homologation et des risques résiduels de sécurité. Dans ce cas, l'autorité d'homologation délivre une autorisation provisoire d'emploi pour une durée courte ne pouvant dépasser 6 mois et assortie d'un plan de mise en conformité et d'un échéancier adapté.

L'autorité d'homologation, au travers de cette démarche, assume ainsi les risques résiduels mis en évidence par l'analyse de risques et est responsable de la sécurité du système d'information.

Les modalités de mise en œuvre de l'homologation et de l'analyse de risques sont annexées au présent arrêté.

### Article 7

Les services exécutifs de l'État mettant en œuvre des systèmes d'information établissent un bilan annuel, mesurant la maturité de la sécurité des systèmes d'information au vu des règles du présent arrêté et de ses annexes.

Ce bilan annuel comporte :

- un récapitulatif des actions réalisées au cours de l'année écoulée pour la mise en conformité à la politique de sécurité des systèmes d'information de l'État ;
- un récapitulatif des incidents significatifs constatés (accompagnés éventuellement de descriptifs des dispositions mises en œuvre pour les résoudre) ;

- l'état d'avancement de l'application des règles édictées par la Politique de Sécurité des Systèmes d'Information de l'État à l'aide du tableau d'évaluation du niveau de sécurité figurant en annexe 3 et, disponible et téléchargeable sur le site https://amsn.gouv.mc/OIV. Les services exécutifs de l'État y précisent pour chaque règle, si elle est :
    - documentée ou non mais non appliquée ;
    - appliquée mais non documentée ;
    - appliquée et documentée ;
    - appliquée, documentée, et contrôlée ;
    - non applicable ; dans ce cas le chef de service devra en expliquer les raisons.

Lorsqu'il y a une évolution significative par rapport à l'évaluation précédente, le service en précise les raisons.

Les documents ainsi complétés sont des documents contenant des informations soumises au secret professionnel dont la révélation est punie dans les conditions définies par l'article 308 du Code pénal.

Les services communiquent, une fois par an avant le 15 janvier de l'année suivant l'exercice faisant l'objet de l'évaluation considérée, à l'Agence Monégasque de Sécurité Numérique, le document mis à jour, selon le moyen approprié à la sensibilité des informations déclarées.

L'Agence Monégasque de Sécurité Numérique consolide l'ensemble de ces bilans à l'effet de remettre un document de synthèse au Ministre d'État et aux Conseillers de Gouvernement-Ministres concernés. Lesdits bilans ainsi que le document de synthèse sont également mis à disposition du Responsable de la Sécurité des Systèmes d'Information.

### Article 8

Les administrateurs sont individuellement désignés et dûment habilités par le chef de service responsable de l'administration du système d'information après enquête administrative conformément aux dispositions de l'arrêté ministériel n° 2016622 du 17 octobre 2016 portant application de l'article 3 de la loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale, modifié.

L'habilitation visée au précédent alinéa est renouvelée tous les trois ans dans les mêmes conditions.

Le chef de service tient à jour un registre des personnes habilitées ainsi que de leurs accès privilégiés et de leurs droits spécifiques.

### Article 9

L'Agence Monégasque de Sécurité Numérique en liaison avec le Responsable de la Sécurité des Systèmes d'Information et les chefs de service responsables de l'administration des systèmes d'information actualise, *a minima* tous les deux ans, la Politique de Sécurité des Systèmes d'Information de l'État.

### Article 10

L'arrêté ministériel n° 2017-56 du 1er février 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, est abrogé.

### Article 11

Dans les ordonnances souveraines, les arrêtés ministériels et règlements actuellement en vigueur, les termes : « *arrêté ministériel n° 2017-56 du 1er février 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* » sont remplacés par les termes : « *arrêté ministériel n° 2022-331 du 13 juin 2022 portant application de l'article 23 de la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique, fixant les mesures de sécurité des systèmes d'information de l'État* ».

### Article 12

Le Ministre d'État, le Conseiller de Gouvernement-Ministre des Affaires Sociales et de la Santé, le Conseiller de Gouvernement-Ministre de l'Équipement, de l'Environnement et de l'Urbanisme, le Conseiller de Gouvernement-Ministre de l'Intérieur, le Conseiller de Gouvernement-Ministre des Finances et de l'Économie et le Conseiller de Gouvernement-Ministre des Relations Extérieures et de la Coopération, le Secrétaire Général du Gouvernement, le Directeur de l'Agence Monégasque de Sécurité Numérique et le Responsable de la Sécurité des Systèmes d'Information sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté.

## Annexes - _

*Voir le document associé.*

## Notes

### Liens

1. Journal de Monaco du 24 juin 2022
   ^ [p.1] https://journaldemonaco.gouv.mc/Journaux/2022/Journal-8596