LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

Agence nationale de la sécurité
des systèmes d'information

Politique de la gestion de l'organisation de la sécurité de l'information

Mars 2026

Table des Matières

1 Introduction

La présente politique définit un cadre de gouvernance de la sécurité de l'information, permettant aux entités de structurer et piloter efficacement leur dispositif de sécurité. Elle expose les principes et mesures fondamentales pour guider la mise en œuvre de bonnes pratiques adaptées, renforçant ainsi leur gouvernance en matière de sécurité de l'information.

2 Périmètre, limites et exclusions

La politique couvre les aspects relatifs à la gouvernance de la sécurité de l'information. Elle s'applique à l'ensemble des systèmes d'information et des réseaux exploités par l'entité. Le périmètre précis, les limites et les éventuelles exclusions sont à définir par chaque entité en fonction de son contexte, de ses missions et de ses obligations réglementaires.

3 Définitions

L'ensemble des termes utilisés sont définis dans le Glossaire de la sécurité de l'information, maintenu par le Haut-Commissariat à la protection nationale (HCPN), dans sa fonction d'Agence nationale de la sécurité des systèmes d'information (ANSSI), et accessible via notre extranet ANSSI et notre GovSpace.

4 Gestion de la sécurité de l'information

4.1 Gouvernance et organisation de la sécurité de l'information

4.1.1 Mesures fondamentales

MF-001 L'organe de direction de l'entité devrait démontrer son engagement et sa responsabilité globale en matière de sécurité de l'information.

- ISO/IEC 27001 :2022 5.1, 5.2, 5.3, A.5.1, A.5.4
- Règlement d'exécution UE 2024/2690 1.1.1, 1.2.1
- ENISA guideline on security measures under the EECC 4th edition – SO3

MF-002 L'organe de direction de l'entité devrait désigner un Délégué à la Sécurité de l'Information (DSI) chargé de coordonner la mise en œuvre et le suivi du dispositif de sécurité de l'information.

- ISO/IEC 27001 :2022 5.3, A.5.2, A.5.3

- Règlement UE 2024/2690 : 1.2.1
- ENISA guideline on security measures under the EECC 4th edition – SO3

MF-003 L'entité devrait définir une fonction informatique, chargée d'assurer la gestion, l'exploitation et le maintien en condition opérationnelle du système d'information.

- ISO/IEC 27001 :2022 5.3, A.5.2
- Règlement d'exécution UE 2024/2690 : 1.2.1
- ENISA guideline on security measures under the EECC 4th edition – SO3

MF-004 L'entité devrait mettre en place un dispositif de pilotage afin d'organiser au mieux sa gestion de la sécurité des systèmes d'information.

- ISO/IEC 27001 :2022 5.3, A.5.2
- Règlement d'exécution UE 2024/2690 : 1.2.1
- ENISA guideline on security measures under the EECC 4th edition – SO3

4.1.2 Mesures complémentaires

MC-001 L'entité devrait participer à des initiatives de coopération et de partage d'informations en matière de cybersécurité afin de renforcer sa capacité à anticiper, détecter et répondre aux menaces susceptibles d'affecter ses systèmes d'information.

- ISO/IEC 27001 :2022 A.5.6
- Règlement d'exécution UE 2024/2690 **:** 1.2.1
- ENISA guideline on security measures under the EECC 4th edition – SO3

4.2 Cadre de gestion de la sécurité de l'information

4.2.1 Mesures fondamentales

MF-005 L'entité devrait adopter une Politique Générale de Sécurité de l'Information (PGSI).

- ISO/IEC 27001 :2022 5.2, 7.5, A.5.1
- Règlement d'exécution UE 2024/2690 : 1.1.1
- ENISA guideline on security measures under the EECC 4th edition – SO1

MF-006 L'entité devrait définir et formaliser sa vision de la sécurité de l'information à moyen et long terme, et la décliner en actions concrètes, priorisées et suivies dans le temps.

- ISO/IEC 27001 :2022 A.5.1, A5.4, A.5.36
- Règlement d'exécution UE 2024/2690 : 1.1.1
- ENISA guideline on security measures under the EECC 4th edition –SO1

MF-007 L'entité devrait établir des politiques thématiques précisant les mesures applicables à chaque domaine de la sécurité de l'information.

- ISO/IEC 27001 :2022 7.5, A.5.1
- Règlement d'exécution UE 2024/2690 : 1.1.1
- ENISA guideline on security measures under the EECC 4th edition –SO1

MF-008 L'entité devrait établir des relations avec les autorités compétentes et les équipes de réponse aux incidents de sécurité cyber afin de faciliter la coordination et la gestion des incidents affectant les réseaux et les systèmes d'information.

- ISO/IEC 27001 :2022 5.3, A.5.5
- Règlement d'exécution UE 2024/2690 : 1.2.1, 7.1
- ENISA guideline on security measures under the EECC 4th edition –SO3

4.2.2 Mesures complémentaires

MC-002 L'entité devrait décliner les politiques de sécurité de l'information en procédures, processus ou guides opérationnels permettant d'en assurer la mise en œuvre effective au sein de l'organisation.

- ISO/IEC 27001 :2022 7.5, A.5.1
- Règlement d'exécution UE 2024/2690 : 1.1.1
- ENISA guideline on security measures under the EECC 4th edition – SO1

4.3 Contrôle et amélioration continue

4.3.1 Mesures fondamentales

MF-009 L'entité devrait définir un cadre permettant de documenter, analyser et approuver les demandes de dérogation aux politiques de sécurité. Chaque demande devrait être évaluée en fonction des risques et des mesures compensatoires proposées. Toute dérogation accordée devrait faire l'objet d'une revue périodique afin de vérifier que les risques restent maîtrisés.

- ISO/IEC 27001 :2022 A.5.1 (g), Section 6.1.2, 6.1.3
- Règlement d'exécution UE 2024/2690 : 1.2.3
- ENISA guideline on security measures under the EECC 4th edition – SO1

4.3.2 Mesures complémentaires

MC-003 L'entité devrait mettre en place un dispositif de contrôle interne permettant de s'assurer du respect des règles de sécurité de l'information de l'entité.

- ISO/IEC 27001 :2022 9.1, 9.2
- Règlement d'exécution UE 2024/2690 : 7.1
- ENISA guideline on security measures under the EECC 4th edition – SO24

MC-004 L'entité devrait définir des indicateurs permettant de suivre l'évolution du niveau de sécurité de l'information, d'apprécier le niveau de maîtrise des risques et de soutenir le pilotage du dispositif de sécurité.

- ISO/IEC 27001 :2022 9.1
- Règlement d'exécution UE 2024/2690 : 7.1
- ENISA guideline on security measures under the EECC 4th edition – SO24

MC-005 L'entité devrait mettre en place un processus permettant d'améliorer en continu le dispositif de sécurité de l'information sur la base des résultats des contrôles, des audits, des incidents et de l'évolution des risques.

- ISO/IEC 27001 :2022 10.1
- Règlement d'exécution UE 2024/2690 : 7.1
- ENISA guideline on security measures under the EECC 4th edition – SO24