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

Agence nationale de la sécurité
des systèmes d'information

Lignes directrices pour la gestion de l'organisation de la sécurité de l'information

Avril 2026

1 Table des Matières

2 Introduction

L'objectif de ce document est de proposer des recommandations d'implémentation concernant l'organisation de la sécurité de l'information, afin de permettre la mise en œuvre des mesures de sécurité définies dans la politique de sécurité correspondante. Ces recommandations visent à structurer la gouvernance de la sécurité de l'information au sein de l'entité, en clarifiant les rôles, responsabilités et mécanismes de coordination nécessaires pour assurer une gestion cohérente et efficace de la sécurité de l'information.

Elles s'appuient sur les exigences des normes internationales ISO/IEC 27001:2022 et ISO/IEC 27002:2022, sur la directive (UE) 2022/2555 relative à des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'Union (directive NIS2), sur le règlement d'exécution (UE) 2024/2690, ainsi que sur les lignes directrices publiées par l'Agence de l'Union européenne pour la cybersécurité (ENISA) relatives aux mesures de sécurité prévues par le Code européen des communications électroniques (EECC). Elles sont structurées selon trois niveaux de maturité afin de permettre une mise en œuvre adaptée à la taille, aux ressources et aux enjeux de sécurité de l'entité.

3 Définition

Le présent document s'appuie sur un ensemble de définitions techniques et organisationnelles. 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 Rôles et responsabilités

Le présent document définit les rôles et responsabilités spécifiques à son périmètre. Il s'inscrit dans le cadre global de gouvernance de la sécurité de l'information de l'entité.

L'ensemble des rôles et responsabilités applicables au référentiel de sécurité de l'information proposé aux entités est défini dans le *Référentiel des rôles et responsabilités en sécurité de l'information* accessible via les espaces documentaires internes de l'agence (extranet ou GovSpace).

Organe de direction

L'organe de direction est responsable de la gouvernance et de la supervision globale de la sécurité de l'information au sein de l'entité. À ce titre, il s'implique activement dans la gestion des risques en matière de cybersécurité, en définissant les orientations stratégiques et en veillant à leur mise en œuvre effective. Il s'assure de la prise en compte des enjeux de sécurité dans l'ensemble des activités de l'entité et de l'allocation des ressources nécessaires.

Conformément aux exigences de la directive NIS2, il approuve les mesures de gestion des risques en matière de sécurité de l'information, supervise leur mise en œuvre et valide les résultats des analyses de risques ainsi que les plans de remédiation associés. Il veille également à disposer des compétences nécessaires pour comprendre les risques, notamment via des actions de formation adaptées.

Il garantit ainsi un niveau de sécurité proportionné aux risques, en conciliant sécurité, continuité des activités et performance de l'entité.

Délégué à la Sécurité de l'Information (DSI)

Le Délégué à la Sécurité de l'Information est chargé de piloter, coordonner et suivre le dispositif de sécurité de l'information de l'entité.

Il décline les orientations définies par l'organe de direction en politiques, procédures et mesures de sécurité applicables, et veille à leur cohérence et à leur mise en œuvre au sein de l'entité.

Il agit en tant que point de référence en matière de sécurité de l'information et assure le suivi global du dispositif.

Fonction informatique

La fonction informatique est responsable de l'exploitation, du maintien en condition opérationnelle et de la sécurisation des systèmes d'information de l'entité.

Elle met en œuvre les mesures techniques et opérationnelles de sécurité, conformément aux règles de sécurité de l'entité, et contribue au maintien du niveau de sécurité des systèmes d'information dans la durée.

5 Gestion de la sécurité de l'information

5.1 Gouvernance et organisation de la sécurité de l'information

5.1.1 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

	Recommandations
Niveau 1	L'organe de direction de l'entité devrait démontrer son engagement envers la sécurité de l'information en : • Approuvant et soutenant la mise en place d'une Politique Générale de Sécurité de l'Information (PGSI) ; • Approuvant les mesures de gestion des risques en matière de cybersécurité et supervisant leur mise en œuvre ; • S'assurant que les mesures techniques, opérationnelles et organisationnelles appropriées sont mises en œuvre pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information de l'entité ; • Veillant à ce que des ressources minimales et suffisantes soient disponibles pour la mise en œuvre des mesures de sécurité de l'information ; • Définissant et pilotant une vision de la sécurité de l'information à moyen et long terme (cf. mesure MF-006) ; • S'assurant que les rôles et responsabilités en matière de sécurité de l'information soient clairement définis, formalisés et attribués ; • Soutenant les initiatives visant à promouvoir activement une culture de sécurité de l'information au sein de l'entité.
Niveau 2	L'organe de direction de l'entité s'implique activement dans la gouvernance en : • Statuant sur les orientations stratégiques et les arbitrages majeurs ; • S'appuyant sur un reporting structuré pour suivre les risques, les incidents significatifs et l'efficacité du dispositif ;

	• Participant ou étant représenté dans les instances de gouvernance, notamment le Comité de Sécurité de l'Information (cf. mesure MF-004) ; • Approuvant les plans d'actions visant à traiter les risques significatifs liés à la sécurité de l'information ; • Favorisant une démarche d'amélioration du dispositif de sécurité et en suivant les principaux résultats.
Niveau 3	L'organe de direction adopte une approche intégrée et proactive de la sécurité de l'information en : • Portant une vision stratégique et anticipative de la sécurité comme levier de résilience et de performance ; • Arbitrant les décisions et investissements sur base d'une approche par les risques et des tendances (reporting consolidé) ; • S'impliquant dans des revues périodiques et, le cas échéant, dans des exercices de gestion de crise ; • Pilotant une amélioration continue structurée (audits, contrôles, retours d'expérience).

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 d'exécution UE 2024/2690 1.2.1
- ENISA guideline on security measures under the EECC 4th edition - SO_3

	Recommandations
Niveau 1	Chaque entité devrait désigner nominativement un Délégué à la Sécurité de l'Information (DSI). Le DSI devrait coordonner la mise en œuvre des mesures organisationnelles, techniques et humaines nécessaires à la protection des réseaux, des systèmes d'information et des actifs informationnels de l'entité. Ses responsabilités devraient notamment inclure : • Conseiller l'organe de direction en matière de sécurité de l'information ;

	• Définir, piloter et veiller à la mise en œuvre de la Politique Générale de Sécurité de l'Information (PGSI) de l'entité, en conformité avec la PGSI de l'Etat ; • Piloter l'élaboration, la validation et la diffusion des politiques thématiques et procédures de sécurité de l'information, et veiller à leur implémentation ; • Piloter les activités de gestion des risques ; • Superviser la gestion interne et le suivi des incidents de sécurité ; • Assurer le suivi de la conformité de l'entité aux exigences légales et réglementaires applicables en matière de sécurité de l'information ; • Promouvoir une culture de la sécurité de l'information au sein de l'entité ; • Assurer la coordination des parties prenantes internes impliquées dans la sécurité de l'information. Le DSI devrait disposer d'un accès direct et régulier à l'organe de direction afin de pouvoir présenter l'état de la sécurité de l'information, les risques associés et les actions de remédiation, et soutenir la prise de décision.
Niveau 2	Le DSI devrait formaliser et structurer le pilotage du dispositif de sécurité de l'information afin d'en assurer le suivi et l'intégration dans la gouvernance de l'entité. Ses responsabilités devraient notamment inclure : • La mise en place d'un reporting régulier (p.ex. 2 fois par an) à destination de l'organe de direction ou au Comité de Sécurité de l'Information (CSI), si existant ; • L'intégration de la sécurité de l'information dans les projets et processus de l'entité ; • Le suivi de la conformité aux exigences légales, réglementaires et internes en matière de sécurité de l'information.
Niveau 3	En complément, les responsabilités du DSI devraient notamment inclure le suivi d'indicateurs de sécurité (KPI/KRI) destinés à évaluer l'efficacité des mesures mises en œuvre.

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

	Recommandations
Niveau 1	Chaque entité devrait identifier formellement qui assure la fonction informatique. Cette fonction devrait notamment être responsable : • Du support aux utilisateurs pour le traitement des incidents et des demandes informatiques ; • De la gestion et du maintien en condition opérationnelle des infrastructures et des actifs informatiques (serveurs, réseaux, postes de travail, applications) ; • De la mise en œuvre des actions techniques nécessaires à l'exploitation du système d'information ; • De la coordination avec le DSI pour la mise en œuvre des actions techniques liées à la sécurité et à l'exploitation du système d'information.
Niveau 2	L'entité devrait définir et formaliser les responsabilités de la fonction informatique, qui devrait notamment inclure : • La rédaction, la mise à jour et la mise en œuvre des procédures et guides opérationnels ; • La mise en œuvre opérationnelle des exigences de sécurité définies par le DSI, notamment par leur traduction en configurations techniques et en procédures ; • L'appui technique au DSI pour la gestion des risques, la définition des exigences de sécurité et la gestion des incidents ; • La participation à la mise en œuvre et au suivi des mesures de sécurité tout au long du cycle de vie des systèmes d'information.
Niveau 3	La fonction informatique devrait être structurée et professionnalisée afin de renforcer la qualité et la résilience des services informatiques via notamment : • La définition d'un catalogue de services informatiques, décrivant les services fournis aux utilisateurs ;

	• La mise en place de processus documentés pour les activités vitales (par exemple : gestion des incidents, gestion des changements, gestion des actifs) ; • L'adoption d'un cadre de gestion des services informatiques reconnu (par exemple : ITIL ou équivalent ; • La participation aux exercices de continuité d'activité, de reprise informatique et de gestion de crise cyber, ainsi qu'aux activités d'amélioration continue du dispositif de sécurité.

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

	Recommandations
Niveau 1	Le DSI devrait mettre en place un mécanisme de coordination formalisé avec l'organe de direction, reposant sur un reporting régulier, structuré et orienté vers la prise de décision. Ce reporting devrait s'appuyer sur des indicateurs pertinents et fiables, comme par exemple le Plan Pluriannuel de la Sécurité de l'Information (cf. mesure MF-006), évolution du niveau de maturité, niveau de risques), afin de permettre un suivi clair des enjeux de sécurité de l'information, de faciliter l'arbitrage des priorités et de soutenir la prise de décision au niveau stratégique.
Niveau 2	Pour améliorer le pilotage de la sécurité de l'information, les entités devraient mettre en place un Comité de Sécurité de l'Information (CSI). Le CSI est une instance transversale de gouvernance. Il permet de structurer la prise de décision, de coordonner les acteurs concernés et d'assurer un pilotage partagé et régulier de la sécurité de l'information. Le CSI agit comme organe d'aide à la décision auprès de la Direction, sur base notamment d'un reporting consolidé, factuel et orienté risques. À ce titre, il est consulté en amont de toute décision susceptible d'avoir un impact significatif sur la sécurité de l'information. Le CSI a pour missions principales de :

	• Améliorer durablement la maturité et la résilience de l'entité ; • Maintenir un niveau de risque maîtrisé et acceptable, en disposant d'une vision consolidée des risques, incidents et dérogations ; • Prioriser et arbitrer les actions de sécurité, en tenant compte des analyses de risques, des ressources disponibles et des obligations réglementaires ; • Structurer la prise de décision, en impliquant les parties prenantes dans un pilotage partagé et régulier. Le CSI devrait idéalement inclure les membres suivants : • Un représentant de l'organe de direction (président du comité) ; • Le Délégué à la Sécurité de l'Information (DSI) ; • Le responsable de la fonction informatique ; • Des représentants métiers ; • Le Délégué à la Protection des Données (DPD). La présence permanente des fonctions suivantes est fortement recommandée lorsque ces rôles existent dans l'entité : • Gestionnaire des risques ; • Gestionnaire de la continuité des activités. Selon les sujets traités, d'autres participants pourraient être invités : • Gestionnaire des ressources humaines ; • Gestionnaire de la sécurité physique. Le comité se réunit au minimum deux fois par an afin d'assurer un pilotage continu et concerté de la sécurité de l'information. À ce titre, il devrait notamment : • Prendre connaissance des nouveautés et événements marquants depuis la dernière réunion (incidents significatifs, évolutions réglementaires, résultats d'audit, etc.) ; • Examiner les risques pour l'entité et leur évolution ; • Suivre l'avancement du Plan d'action Pluriannuel de la Sécurité de l'Information (cf. mesure MF-006) et identifier les difficultés ou besoins d'ajustement ;

	• Examiner la maturité du dispositif, les incidents, les dérogations et l'efficacité des contrôles ; • Arbitrer et décider sur les priorités, les adaptations du plan d'action, les risques résiduels et les demandes de dérogation.
Niveau 3	Les entités dont les activités sont vitales ou exposées à des risques élevés devraient organiser les réunions du Comité de Sécurité de l'Information de manière trimestrielle, afin de suivre plus étroitement l'évolution des risques, l'efficacité des mesures de protection et les incidents de sécurité.

5.1.2 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

	Recommandations
Niveau 1	Il n'y a pas de recommandation applicable.
Niveau 2	Il n'y a pas de recommandation applicable.
Niveau 3	L'entité devrait participer à des mécanismes d'échange d'informations relatifs aux menaces, aux vulnérabilités et aux bonnes pratiques en matière de cybersécurité, afin de renforcer sa posture de sécurité et de contribuer à la résilience collective. Cette participation peut notamment inclure : • La participation à des ateliers, conférences, forums techniques ou groupes de travail sectoriels et interinstitutionnels ; • L'implication dans des communautés d'expertise et des réseaux de coopération en cybersécurité ; • La contribution au partage d'informations (incidents, vulnérabilités, retours d'expérience, bonnes pratiques).

	Ces échanges devraient permettre à l'entité d'améliorer sa compréhension du paysage de menaces, d'anticiper les évolutions et d'adapter ses mesures de sécurité en conséquence.

5.2 Cadre de gestion de la sécurité de l'information

5.2.1 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

	Recommandations
Niveau 1	Le DSI devrait élaborer une Politique Générale de Sécurité de l'Information (PGSI) définissant les principes applicables à la protection des réseaux et des systèmes d'information pour l'entité. Celle-ci devrait être intégrée dans la gouvernance globale de l'entité et soutenir la gestion stratégique de la sécurité de l'information. Cette politique devrait notamment : • S'inscrire dans le cadre de référence de la PGSI de l'État luxembourgeois ; • Définir les objectifs de sécurité de l'information de l'entité ; • Préciser les principes de gouvernance applicables à la sécurité de l'information ; • Rappeler les responsabilités générales des parties prenantes en matière de sécurité ; • Établir l'engagement de l'entité à se conformer aux obligations légales et réglementaires applicables ; • Servir de cadre de référence pour l'ensemble des politiques et mesures de sécurité mises en œuvre au sein de l'organisation ; • Engager l'entité à adopter un modèle d'amélioration continue. La politique devrait être approuvée par l'organe de direction et mise à disposition des parties prenantes concernées. Elle devrait faire l'objet d'une revue lors de changements organisationnels, réglementaires ou technologiques significatifs.

Niveau 2	La PGSI devrait notamment être revue périodiquement tous les 3 ans afin de tenir compte de l'évolution du contexte de menaces, des risques et des exigences réglementaires. Cette revue peut être complétée par des mises à jour ponctuelles en cas d'évolution significative de l'organisation, du système d'information, du contexte réglementaire ou du niveau de risque, ainsi qu'à la suite d'un incident de sécurité majeur. La mise en œuvre de cette politique devrait faire l'objet d'un suivi régulier afin d'assurer son efficacité et son adéquation avec les objectifs de sécurité de l'entité.
Niveau 3	Il n'y a pas de recommandation applicable.

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, A.5.4, A.5.36
- Règlement d'exécution UE 2024/2690 1.1.1
- ENISA guideline on security measures under the EECC 4th edition – SO1

	Recommandations
Niveau 1	L'entité devrait établir et maintenir un Plan Pluriannuel de Sécurité de l'Information (PPSI) couvrant une période significative (par exemple, de 3 à 5 ans). Il permet à la direction, aux responsables métiers et au Délégué à la Sécurité de l'Information (DSI) de partager une vision commune des priorités en matière de sécurité de l'information, de prioriser les actions et d'orienter les investissements en matière de cybersécurité. Pour élaborer ce plan, l'entité devrait s'appuyer sur les résultats d'un état des lieux structuré de sa posture de sécurité, comprenant notamment : • Les écarts identifiés lors de l'auto-évaluation au regard des objectifs de sécurité, permettant de mesurer le niveau de maturité du dispositif ; • Les mesures de traitement issues des analyses de risques en sécurité de l'information, dont la macro-cartographie des risques, traduisant les priorités de remédiation en fonction des risques identifiés ; L'entité devrait prioriser les actions du plan pluriannuel de sécurité de l'information en fonction du niveau de criticité des risques et des enjeux associés, en tenant compte des contraintes et capacités de mise en œuvre (budget,

	ressources humaines, référents désignés), et définir pour chacune une trajectoire de mise en œuvre avec des échéances planifiées et des responsabilités clairement attribuées. *Note : L'entité peut s'appuyer sur le modèle de PPSI proposé par le HCPN / ANSSI, disponible sur l'extranet / Govspace.*
Niveau 2	Il n'y a pas de recommandation applicable.
Niveau 3	L'entité devrait définir et formaliser une stratégie de sécurité de l'information pluriannuelle, alignée sur ses objectifs stratégiques et fondée sur une approche par les risques. Cette stratégie précise la vision cible et les priorités de sécurité, s'appuie notamment sur les analyses de risques et les évaluations de maturité, et intègre un plan d'actions priorisé avec des ressources, des responsabilités et des échéances définies. Elle prévoit également des indicateurs de pilotage pour en suivre l'avancement et l'efficacité, et s'inscrit dans une logique d'amélioration continue. La stratégie est validée par l'organe de direction, pilotée par le DSI et suivie régulièrement au sein des instances de gouvernance.

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

	Recommandations
Niveau 1	Les mesures applicables à chaque domaine de la sécurité de l'information devraient être précisées dans la PGSI de l'entité.
Niveau 2	Des politiques thématiques, couvrant notamment les domaines suivants, devraient être définies, validées et implémentées : • Politique d'acquisition, de développement et de maintenance des systèmes d'information : précise les règles et bonnes pratiques à appliquer pour garantir la sécurité tout au long du cycle de vie des systèmes d'information ;

	• Politique de gestion des accès logiques : établit les règles permettant de gérer, contrôler et surveiller les droits d'accès aux actifs informatiques et informationnels du système d'information. • Politique de gestion des actifs : définit la catégorisation du niveau de sensibilité des actifs informationnels et informatiques ainsi que les mesures de protection associées, au cours de l'ensemble de leur cycle de vie ; • Politique de gestion des événements et des incidents liés à la sécurité de l'information : décrit les procédures de détection, déclaration, traitement et suivi des incidents de sécurité ; • Politique de gestion des risques : établit les méthodes pour identifier, évaluer et traiter les risques susceptibles d'affecter la sécurité des systèmes d'information. • Politique de sécurité des ressources humaines : précise les mesures de sécurité applicables à chaque étape du cycle de vie des relations professionnelles, du recrutement à la fin de fonction. Elle devrait inclure également les exigences en matière de sensibilisation et de formation des collaborateurs afin de renforcer leur niveau de vigilance et leurs compétences en sécurité de l'information. • Politique de sécurité liée à l'exploitation, pour les entités disposant d'activités informatiques significatives (p.ex. administration systèmes, bases de données ou réseaux. Celle-ci définit les mesures permettant de sécuriser les opérations courantes, notamment la gestion des changements, des capacités, des journaux, des sauvegardes, des vulnérabilités et des mises à jour, afin de prévenir les incidents opérationnels ; • Politique de sécurité physique et environnementale : décrit les mesures visant à protéger les locaux, équipements et infrastructures vitaux contre les accès non autorisés, les dommages et les perturbations. • Politique des relations avec les fournisseurs / sécurité de la chaîne d'approvisionnement : encadre les exigences contractuelles, organisationnelles et techniques applicables aux fournisseurs et aux prestataires tout au long de la chaîne d'approvisionnement.
Niveau 3	Afin de compléter le cadre défini aux niveaux précédents, le DSI devrait formaliser les politiques thématiques suivantes : • Politique de cryptographie, décrivant les mesures encadrant l'usage du chiffrement, la gestion complète du cycle de vie des clés (création,

	distribution, stockage, rotation, révocation), la conformité aux standards reconnus ainsi que les mécanismes garantissant la confidentialité, l'intégrité et l'authenticité des données ; • Politique de gestion de la conformité, décrivant les mesures visant à assurer le respect de l'ensemble des obligations légales, réglementaires, normatives et internes applicables à la sécurité des réseaux et des systèmes d'information, ainsi que les mécanismes de contrôle continu permettant de détecter et corriger les écarts ; • Politique de sécurité des réseaux, définissant les mesures de protection des communications et des interconnexions, couvrant notamment le cloisonnement, la segmentation, la surveillance, le durcissement des équipements et la gestion des flux, dans le but d'assurer la disponibilité, la confidentialité et l'intégrité des informations transitant sur les réseaux.

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

	Recommandations
Niveau 1	L'entité devrait identifier les autorités et structures nationales avec lesquelles elle est susceptible d'interagir dans le cadre de la gestion des incidents de sécurité. Ces acteurs peuvent notamment inclure : • Le Haut-Commissariat à la Protection Nationale (HCPN), dans sa fonction de GOVCERT.LU, qui est chargé de prévenir, détecter et traiter les incidents de sécurité affectant les systèmes d'information des entités publiques. Il assure la veille sur les menaces, coordonne la gestion des incidents, diffuse des alertes et recommandations de sécurité et fournit un appui technique aux administrations, afin de renforcer leur capacité de prévention et de réaction face aux cybermenaces ;

	• Le Centre des technologies de l'information de l'État (CTIE), pour les services qu'il met à disposition des entités de l'État ; • L'autorité compétente désignée dans le cadre de la directive NIS2 au Luxembourg, l'Institut Luxembourgeois de Régulation (ILR). À ce titre, l'entité notifie à l'ILR les incidents ayant un impact significatif, selon les délais et modalités prévus par la réglementation applicable, notamment via la plateforme SERIMA ; • Les autorités compétentes dans des domaines réglementaires connexes, telles que la Commission Nationale pour la Protection des Données (CNPD) notamment lorsque des incidents de sécurité de l'information impliquent des données à caractère personnel (violations de données), afin de satisfaire aux obligations de notification applicables ; • Toute autre entité publique ou organisme compétent avec lequel l'entité doit coopérer dans le cadre de ses missions ou de ses obligations réglementaires.
Niveau 2	Il n'y a pas de recommandation applicable.
Niveau 3	Il n'y a pas de recommandation applicable.

5.2.2 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

	Recommandations
Niveau 1	Il n'y a pas de recommandation applicable.
Niveau 2	L'entité devrait définir des procédures, processus ou guides opérationnels permettant de mettre en œuvre les exigences définies dans la Politique Générale de Sécurité de l'Information (PGSI) et dans les politiques thématiques. Ces documents opérationnels devraient notamment : • Préciser les activités à réaliser pour appliquer les règles définies dans les politiques ;

	• Identifier les rôles impliqués dans la mise en œuvre des mesures de sécurité ; • Décrire les modalités de contrôle ou de suivi permettant de vérifier l'application des politiques. Les procédures, processus ou guides opérationnels devraient être accessibles aux fonctions concernées et maintenus à jour.
Niveau 3	Il n'y a pas de recommandation applicable.

5.3 Contrôle et amélioration continue

5.3.1 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

	Recommandations
Niveau 1	Une demande de dérogation devrait être formalisée au moyen d'un formulaire dédié, comprenant au minimum les éléments suivants : le constat et la justification de la demande de dérogation, ainsi que l'identification de la ou des règles de sécurité auxquelles il est demandé de déroger. Le DSI devrait procéder à une évaluation systématique du risque associé à toute demande de dérogation, en identifiant les menaces et vulnérabilités concernées, en appréciant les impacts potentiels sur la confidentialité, l'intégrité et la disponibilité des systèmes et services, et en définissant les contrôles compensatoires applicables afin de ramener le risque résiduel à un niveau acceptable. Les dérogations présentant un risque élevé devraient être soumises, lorsque nécessaire, à l'avis ou à la validation de l'organe de direction ou du Comité de Sécurité de l'Information (CSI), notamment lorsque les mesures compensatoires applicables sont jugées insuffisantes pour atténuer le risque.

	Une dérogation approuvée devrait être strictement limitée dans le temps et assortie d'une date d'expiration clairement définie. Elle devrait être intégrée dans un registre centralisé de gestion des dérogations, permettant d'assurer le suivi structuré de l'ensemble des demandes, des analyses, des décisions et des révisions, afin de garantir une gestion efficace, ainsi que la transparence et la traçabilité. Une revue annuelle du registre des dérogations devrait être réalisée par le DSI afin de s'assurer que les dérogations encore actives demeurent justifiées, que les mesures compensatoires mises en place restent adaptées et que les dérogations arrivées à échéance ne perdurent pas sans que la situation à l'origine de la dérogation n'ait été régularisée.
Niveau 2	Il n'y a pas de recommandation applicable.
Niveau 3	La revue des dérogations devrait être effectuée dès que possible après l'expiration de chaque dérogation afin de vérifier la clôture effective et l'application correcte des mesures de sécurité associées, permettant ainsi de détecter rapidement toute dérive ou lacune potentielle.

5.3.2 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

	Recommandations
Niveau 1	Il n'y a pas de recommandation applicable.
Niveau 2	L'entité met en place des contrôles clés ciblés visant à vérifier le respect des règles de sécurité de l'information sur les domaines les plus sensibles (ex. gestion des accès, correctifs, sauvegardes). Ces contrôles restent ponctuels, avec un suivi des écarts et des actions correctives encore partiellement structuré.
Niveau 3	L'entité dispose d'un dispositif de contrôle interne formalisé, structuré et régulier permettant de s'assurer du respect des règles de sécurité de l'information.

	Ce dispositif inclut des contrôles périodiques couvrant l'ensemble des domaines, un suivi formalisé des écarts, des actions correctives tracées ainsi qu'un reporting régulier vers les instances de gouvernance.

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

	Recommandations
Niveau 1	Il n'y a pas de recommandation applicable.
Niveau 2	Il n'y a pas de recommandation applicable.
Niveau 3	L'entité devrait définir et mettre en œuvre un ensemble de KPI de sécurité pertinents, fiables et adaptés à son contexte, afin de soutenir le pilotage du dispositif de sécurité de l'information. Ces KPI pourraient par exemple comprendre le taux de mise en œuvre des exigences de sécurité, le délai de traitement des incidents, le taux de réalisation des actions correctives dans les délais, le taux de mise en œuvre des recommandations issues des contrôles ou audits, ou encore le niveau de sensibilisation des utilisateurs. Les KPI devraient être documentés, consolidés et analysés périodiquement, puis communiqués au CSI, s'il existe, ou à défaut à l'organe de direction, afin de soutenir la prise de décision.

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

	Recommandations
Niveau 1	Il n'y a pas de recommandation applicable.
Niveau 2	L'entité devrait mettre en œuvre des actions d'amélioration du dispositif de sécurité de l'information sur la base notamment des incidents survenus, de l'identification de nouvelles vulnérabilités ou menaces, d'évolutions du contexte ou des risques, ainsi que de changements organisationnels ou techniques susceptibles d'impacter le niveau de sécurité.
Niveau 3	L'entité devrait structurer un processus d'amélioration continue du dispositif de sécurité de l'information, reposant sur l'analyse régulière des indicateurs de sécurité (cf. mesure MC-003), des incidents, des résultats des contrôles internes et des évaluations de sécurité. Cette analyse devrait permettre d'évaluer l'atteinte des objectifs de sécurité de l'entité, d'identifier les axes prioritaires d'amélioration et d'ajuster les plans d'action (p.ex. le PPSI) en conséquence. Les actions correctives ou d'amélioration devraient être priorisées en fonction des risques identifiés et faire l'objet d'un suivi structuré de leur mise en œuvre dans le cadre du « reporting sécurité de l'information ».