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

Agence nationale de la sécurité
des systèmes d'information

Modèle de Politique Générale de Sécurité de l'Information pour une entité

Avril 2026

Contactez-nous

En cas de question ou de besoin d'accompagnement concernant l'application du présent document, le Haut-Commissariat à la protection nationale (HCPN), dans sa fonction d'Agence nationale de la sécurité des systèmes d'information (ANSSI), se tient à votre disposition.

Pour toute demande, vous pouvez nous contacter par courriel : support@anssi.etat.lu ou par téléphone : 247-88930.

Recommandations d'adaptation du modèle de PGSI

Le présent document constitue un modèle de référence pour l'élaboration d'une Politique Générale de Sécurité de l'Information (PGSI). Il est mis à disposition des entités de l'État par le Haut-Commissariat à la protection nationale (HCPN), dans le cadre de sa fonction d'Agence nationale de la sécurité des systèmes d'information (ANSSI), afin de vous accompagner dans la formalisation de votre propre cadre de sécurité de l'information, en cohérence et en conformité avec la PGSI de l'État luxembourgeois.

Ce modèle n'a pas vocation à être repris de manière strictement littérale. Vous êtes invités à vous l'approprier et à l'adapter à votre contexte organisationnel, à vos missions, à votre taille, à vos ressources, à votre niveau de maturité ainsi qu'à vos enjeux et à votre environnement de risques spécifiques. Cette adaptation doit permettre de garantir que votre PGSI reflète fidèlement la réalité de votre organisation, vos capacités effectives de mise en œuvre et vos priorités de sécurité.

Dans ce cadre, il vous appartient d'ajuster le périmètre du document, les rôles et responsabilités, les mécanismes de gouvernance, ainsi que le niveau de détail des principes énoncés, en tenant compte des dispositifs déjà en place. Vous veillerez également à assurer une bonne articulation de la PGSI avec votre référentiel documentaire interne, afin d'éviter toute incohérence, redondance ou décalage entre les principes définis et les pratiques effectivement mises en œuvre.

Les dispositions relatives aux différents domaines de la sécurité de l'information doivent être adaptées avec discernement. Elles peuvent être conservées dans la PGSI ou déclinées, selon vos besoins, dans des documents associés. Dans tous les cas, les formulations retenues doivent demeurer proportionnées, réalistes et cohérentes avec les moyens effectivement disponibles.

Il est recommandé que l'adaptation du présent modèle fasse l'objet d'une concertation avec les parties prenantes concernées au sein de votre entité ainsi que d'une revue par votre service juridique, afin de s'assurer de sa conformité aux exigences légales et réglementaires applicables. L'objectif est de vous permettre de disposer d'une PGSI claire, crédible, applicable et durable, constituant un véritable document de référence pour le pilotage de la sécurité de l'information. Le document s'appuie sur les conventions de lecture suivantes :

Convention	Signification	Action attendue
[Instruction]	Élément variable à compléter par l'entité.	Remplacer par le contenu propre à l'entité.
« *Note* »	Recommandation du HCPN / ANSSI destinée à orienter l'entité dans la personnalisation du document.	Prendre connaissance, puis supprimer la note de la version finale.
Texte courant	Contenu de référence proposé par le HCPN / ANSSI.	Adopter tel quel ou adapter dans le respect des principes de la PGSI de l'État.

Politique Générale de Sécurité de l'Information de [Nom_entité]

Catégorie du niveau de sensibilité	Non publique
Liste de distribution	Ensemble des collaborateurs
Version du document	1.0
Organe approbateur	Organe de direction
Date d'approbation	**[Date1]**
Date d'entrée en vigueur	**[Date2]**
Date de prochaine revue	**[Date3]**

Table des matières

1 Objet du document

« Note : ce document est mis à disposition par le HCPN/ANSSI en tant que modèle de référence. Chaque entité est invitée à l'adapter à son contexte, à sa taille, à ses enjeux de sécurité, et à son environnement de risques spécifiques. »

La présente Politique Générale de Sécurité de l'Information (PGSI) constitue le document fondateur du cadre de sécurité de l'information de **[Nom de l'entité]**. Établie en conformité avec la PGSI de l'État, elle définit les orientations stratégiques, les principes directeurs, l'organisation et les objectifs en matière de sécurité de l'information.

Elle formalise l'approche globale de l'entité en matière de gestion de la sécurité des réseaux et des systèmes d'information. À ce titre, elle s'applique à l'ensemble des actifs, systèmes, processus et procédures relevant de son périmètre et repose sur une démarche structurée fondée sur l'analyse des risques, la définition d'une gouvernance adaptée ainsi que la mise en œuvre de politiques, règles et mesures de sécurité proportionnées aux enjeux.

La PGSI est définie de manière à être cohérente et complémentaire avec la stratégie globale de l'entité, ses priorités institutionnelles et ses objectifs opérationnels. Elle vise à intégrer les exigences de sécurité de l'information dans les processus décisionnels, les activités métiers et les projets, afin de soutenir la réalisation des missions de l'entité dans des conditions maîtrisées en termes de risques, de continuité et de conformité.

Elle vise également à offrir à l'ensemble des parties prenantes, internes et externes (p.ex. organe de direction, agents, prestataires), une compréhension commune des enjeux de sécurité, de l'approche retenue pour maîtriser les risques et du cadre mis en place pour y répondre.

Les principaux objectifs poursuivis par la PGSI sont les suivants :

- Renforcer la confiance des citoyens, des partenaires et des autres entités de l'État ;
- Préserver le patrimoine informationnel de l'entité ainsi que les données des parties prenantes contre toute atteinte à leur confidentialité, leur intégrité ou leur disponibilité ;
- Maintenir la capacité de l'entité à assurer ses missions de service public, en prévenant les incidents de sécurité et en limitant leurs conséquences ;
- Adopter une approche de sécurité proportionnée aux risques, en veillant à ce que le niveau de protection soit adapté à la sensibilité des informations et des systèmes concernés ;
- Assurer le respect des obligations légales et réglementaires applicables, notamment celles issues de la directive NIS 2.

La présente PGSI constitue le document de référence opposable en matière de sécurité de l'information au sein de l'entité. Elle s'impose à l'ensemble des acteurs concernés et est déclinée en dispositifs et mesures précisant ses modalités d'application.

2 Champ d'application

La PGSI s'applique aux informations dont [Nom de l'entité] a la responsabilité, aux systèmes d'information qui les traitent, ainsi qu'aux activités qui y sont associées.

Elle concerne toute personne physique ou morale ayant accès à ces informations ou à ces systèmes d'information, notamment les agents, quels que soient leur statut ou leur fonction, ainsi que les parties

externes (p. ex. prestataires, sous-traitants, partenaires) et leurs collaborateurs. Ces personnes sont tenues de respecter et d'appliquer, dans la mesure applicable à leurs activités, les exigences définies par la présente politique de sécurité de l'information et le référentiel de sécurité de l'entité.

Sont exclus du champ d'application de la présente PGSI :

- Les exigences relatives à la continuité des activités et à la gestion de crise sont définies dans une politique dédiée, articulée avec la présente PGSI.
- Les systèmes traitant des informations classifiées, soumis à une réglementation spécifique, notamment la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité, ainsi que ses évolutions ;
- **[Autre exclusion dûment justifiée, si pertinente].**

3 Diffusion et prise de connaissance

La PGSI et les règles qui en découlent sont portées à la connaissance des personnes concernées dans un format adapté à leurs responsabilités et à leurs besoins, en veillant à ce que les informations communiquées soient pertinentes, accessibles et compréhensibles.

Une diffusion effective et, lorsque pertinent, traçable de ces éléments est assurée. Il est également veillé à ce que les personnes concernées, internes comme externes, reconnaissent formellement leurs obligations en matière de sécurité de l'information.

Cette reconnaissance peut notamment prendre la forme d'une signature, d'une validation électronique, d'une clause contractuelle ou de tout autre mécanisme équivalent permettant d'en conserver la preuve. Lorsque nécessaire, la communication peut être adaptée sous forme d'extraits ou de synthèses, afin de ne diffuser que les informations pertinentes au regard des responsabilités des destinataires et de préserver la sensibilité de certaines informations.

4 Réglementations, références légales et normatives

« Note : cette section n'a pas vocation à être exhaustive. Il convient de ne mentionner que les principaux textes structurant le cadre de sécurité applicable à l'entité. »

La PGSI tient compte des lois et réglementations en vigueur applicables à [Nom de l'entité], notamment :

- Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (directive NIS 2) ;
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD) ;
- **[Autres textes applicables – à compléter par chaque entité].**

Elle est inspirée des normes, standards et bonnes pratiques internationalement reconnus et approuvés dans le domaine de la sécurité de l'information, dont notamment les normes ISO/IEC 27001 et 27002.

5 Engagement de l'organe de direction

L'organe de direction affirme son engagement en faveur de la sécurité de l'information et veille à la mobilisation des moyens nécessaires à la mise en œuvre de la présente politique, à la maîtrise des risques et au soutien des missions de l'entité.

À ce titre, il s'assure de la mise à disposition des ressources humaines, financières, organisationnelles et techniques appropriées, incluant notamment les compétences, les moyens, les outils et les technologies requis, afin de garantir la mise en œuvre, le maintien et l'amélioration continue du dispositif de sécurité de l'information.

6 Revue et évolution de la PGSI

6.1 Revue

La PGSI est appelée à évoluer dans le temps afin de garantir son adéquation avec le contexte, les enjeux et les risques de l'entité. À ce titre, elle fait l'objet d'une revue au moins annuelle, ainsi que de revues ponctuelles lorsqu'un incident significatif, une évolution importante des risques, de l'organisation, des activités, du cadre légal et réglementaire ou des systèmes d'information le justifie.

Ces revues visent à s'assurer de la pertinence, de l'adéquation et de l'efficacité de la politique au regard de l'évolution des menaces et du contexte de l'entité. Elles s'appuient notamment sur les retours d'expérience issus des incidents, des exercices et des activités de contrôle et d'évaluation.

Les résultats de ces revues sont formalisés et conservés. Ils peuvent donner lieu, le cas échéant, à des mises à jour de la PGSI, soumises à validation et approbation par l'organe de direction.

6.2 Suivi de la mise en œuvre

La mise en œuvre de la PGSI fait par ailleurs l'objet d'un suivi régulier, permettant d'apprécier de manière consolidée le niveau de maîtrise des risques, l'état d'avancement des actions engagées ainsi que l'évolution du niveau de maturité en matière de sécurité de l'information.

Ces éléments de pilotage sont définis, suivis et consolidés dans le cadre d'un dispositif dédié de pilotage de la sécurité de l'information. Ils font l'objet d'une communication régulière à l'organe de direction et, le cas échéant, au Comité de Sécurité de l'Information (CSI), afin de soutenir la prise de décision et l'orientation des priorités en matière de sécurité.

6.3 Amélioration continue

L'entité s'inscrit dans une démarche d'amélioration continue de la sécurité de l'information, fondée sur l'analyse des risques et l'exploitation des enseignements tirés des incidents, des exercices et des activités de contrôle et d'évaluation.

Cette démarche vise à adapter en permanence le dispositif de sécurité, à renforcer son niveau de maturité et à assurer la maîtrise des risques dans la durée.

Le pilotage de ces évolutions est assuré par le Délégué à la Sécurité de l'Information (DSI), qui veille à leur consolidation, leur suivi et leur formalisation.

7 Gouvernance de la sécurité de l'information

7.1 Rôles et responsabilités

Les rôles, responsabilités et autorités en matière de sécurité de l'information sont définis, formalisés et attribués en fonction de l'organisation et des besoins de l'entité. Ils sont documentés, maintenus à jour et portés à la connaissance de l'organe de direction, afin de garantir une gouvernance claire, une prise de décision appropriée et une supervision effective des enjeux de sécurité de l'information.

Les fonctions correspondantes sont confiées à des personnes disposant des compétences appropriées, fondées sur leur formation, leur expérience ou leur niveau de qualification.

Chaque rôle s'accompagne des autorités nécessaires à son exercice effectif. À ce titre, les fonctions concernées disposent, dans leur périmètre respectif, des capacités d'arbitrage, de validation, d'escalade et de décision requises, ainsi que d'un droit d'alerte auprès de l'organe de direction en cas de risque significatif pour la sécurité de l'information.

L'entité veille, lorsque cela est pertinent et proportionné à sa taille et à son organisation, à identifier et à séparer les responsabilités incompatibles, afin de réduire les risques d'erreur, de conflit d'intérêts, de fraude ou de modification non autorisée. Cette séparation concerne notamment les activités de mise en œuvre, de validation, de contrôle et d'évaluation. Lorsque cette séparation ne peut être pleinement assurée, des mesures compensatoires appropriées sont mises en place et documentées.

Les rôles, responsabilités et autorités en matière de sécurité de l'information font l'objet d'une revue périodique et sont mis à jour lorsque nécessaire, notamment en cas d'évolution organisationnelle, d'incident significatif ou de modification du niveau de risque.

« Note : les rôles ci-dessous sont définis à titre indicatif. Chaque entité les adaptera à sa structure organisationnelle. Pour plus de détail, consulter les lignes directrices pour la gestion de l'organisation de la sécurité de l'information ainsi que le Référentiel des rôles et responsabilités en sécurité de l'information. »

7.1.1 Organe de direction de l'entité

L'organe de direction assure la supervision globale de la sécurité de l'information au sein de l'entité, notamment 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 ;
- Veillant à ce 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.

7.1.2 [Optionnel] Le Comité de Sécurité de l'Information

« Note : pour une entité de petite taille, disposant de ressources et d'enjeux de sécurité plus limités, le dispositif de pilotage peut reposer sur un mécanisme de coordination formalisé entre le DSI et l'organe de direction. Pour les autres entités, la mise en place d'une instance dédiée, telle qu'un Comité de Sécurité de l'Information (CSI), est recommandée.

Pour plus de détail, consulter la politique pour la gestion de l'organisation de la sécurité de l'information et ses lignes directrices. »

Le Comité de Sécurité de l'Information (CSI) constitue une instance transversale de gouvernance visant à appuyer la coordination, l'analyse et la préparation des décisions en matière de sécurité de l'information. Il réunit les parties prenantes concernées, incluant notamment un représentant de l'organe de direction.

Le CSI agit comme une instance d'appui à la décision et de suivi, sur la base d'un reporting consolidé, factuel et orienté risques. À ce titre, il contribue à l'instruction des sujets stratégiques et à la priorisation des actions en matière de sécurité de l'information.

7.1.3 Délégué à la Sécurité de l'Information (DSI)

« Note : le périmètre des responsabilités du DSI peut varier selon la structure organisationnelle de chaque entité. Pour plus de détail, se référer à la fiche « Description de poste – Délégué à la Sécurité de l'Information (DSI) » publiée par le HCPN / ANSSI. »

Le Délégué à la Sécurité de l'Information (DSI), désigné par l'organe de direction, constitue la fonction centrale de pilotage et de coordination de la sécurité de l'information au sein de l'entité, en :

- Conseillant l'organe de direction en matière de sécurité de l'information ;
- Définissant, pilotant et veillant à la mise en œuvre de la politique générale de sécurité de l'information (PGSI) de l'entité, en cohérence avec la PGSI de l'État ;
- Pilotant l'élaboration, la validation, la diffusion et le suivi de la mise en œuvre des politiques thématiques et procédures de sécurité de l'information ;
- Définissant et pilotant l'approche de gestion des risques liés à la sécurité de l'information ;
- Supervisant la gestion, le traitement et le suivi des incidents de sécurité ;
- Assurant le suivi de la conformité de l'entité aux exigences légales et réglementaires applicables en matière de sécurité de l'information ;
- Promouvant et diffusant une culture de la sécurité de l'information au sein de l'entité ;
- Assurant la coordination des parties prenantes internes impliquées dans la sécurité de l'information.

Le Délégué à la Sécurité de l'Information (DSI) rend compte directement à l'organe de direction des questions relatives à la sécurité de l'information, de manière régulière ainsi que lors de la survenance d'événements significatifs, notamment en cas de risque ou d'incident majeur. Il peut, à cette fin, s'appuyer sur les travaux et analyses réalisés dans le cadre du Comité de Sécurité de l'Information (CSI), sans que celui-ci ne constitue un intermédiaire obligatoire.

7.1.4 Fonction informatique

La fonction informatique assure l'exploitation, le maintien en condition opérationnelle et la sécurisation des systèmes d'information de l'entité. Elle met en œuvre les mesures techniques et opérationnelles de sécurité conformément aux politiques et exigences définies, et contribue au maintien du niveau de sécurité dans la

durée. Elle agit en coordination avec le Délégué à la Sécurité de l'Information (DSI) afin d'assurer la protection et la résilience des systèmes d'information.

7.1.5 Responsabilités individuelles

Les responsables hiérarchiques

Les responsables hiérarchiques assurent la déclinaison opérationnelle de la PGSI au sein de leur périmètre. À ce titre, ils veillent à ce que leurs équipes disposent d'un niveau d'information, de sensibilisation et de formation adapté aux risques et aux responsabilités associées à leurs fonctions. Ils s'assurent également du respect effectif des règles de sécurité et de l'intégration des exigences de sécurité de l'information dans les activités quotidiennes.

Les agents

Chaque agent contribue à la sécurité des informations et des systèmes d'information en respectant les règles établies, en adoptant des usages responsables, en appliquant les mesures adaptées à la sensibilité des informations traitées, en signalant sans délai tout incident ou anomalie, et en participant aux actions de sensibilisation.

7.1.6 [Optionnel] Autres fonctions à considérer

« Note : certaines fonctions spécifiques contribuent, en complément des rôles décrits ci-dessus, à la gouvernance et à la mise en œuvre de la sécurité de l'information. À titre indicatif et en fonction de l'organisation de l'entité, peuvent être par exemple concernés le responsable de la continuité des activités, le délégué à la protection des données personnelles (DPD), la fonction conformité/contrôle interne, le responsable de la gestion des risques (risk manager) ou la fonction d'audit interne. »

7.2 Référentiel de sécurité

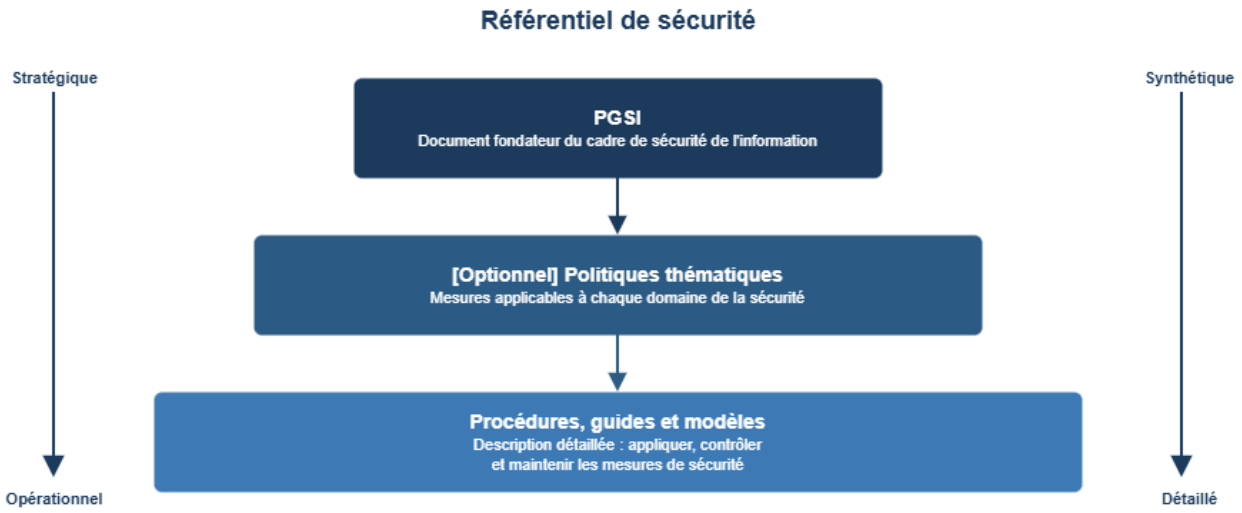
7.2.1 Présentation

« Note : le référentiel de sécurité proposé ci-après constitue une base indicative. Il a vocation à compléter et renforcer les documents existants de l'entité, le cas échéant. Pour plus de détails, consulter le « Guide d'utilisation du référentiel de sécurité de l'information. » »

Le référentiel de sécurité de l'entité s'appuie sur des normes, standards et bonnes pratiques internationalement reconnus, notamment les normes ISO/IEC 27001 et 27002, et se structure autour d'un ensemble cohérent de documents hiérarchisés, comprenant la Politique Générale de Sécurité de l'Information (PGSI), et **[préciser la structure documentaire de l'entité, comme par exemple : les politiques thématiques, ainsi que les procédures, guides et documents opérationnels associés.]**

[Optionnel : Les politiques thématiques précisent notamment, pour chaque domaine de sécurité, les exigences applicables et les responsabilités associées. Elles font l'objet d'une approbation au niveau de gouvernance approprié. Les décisions d'approbation et les versions associées sont formalisées et conservées conformément aux règles de gestion documentaire de l'entité.]

Sa construction s'inscrit dans une logique structurée, pouvant être représentée selon une approche pyramidale :



Exemple de structure de référentiel de sécurité

« Note : Afin de faciliter la formalisation du référentiel de sécurité de l'entité, le HCPN/ANSSI met à disposition des entités des documents permettant de construire le référentiel de sécurité de chaque entité :

- *Un modèle de PGSI pour les entités (le présent document),*
- *Des modèles de politiques générales thématiques et des lignes directrices fournissant des recommandations d'implémentation,*
- *Ainsi que des procédures, des guides pratiques et modèles facilitant la mise en œuvre concrète de ces recommandations.*

L'ensemble de ces documents constitue un cadre de référence que chaque entité est invitée à adapter à sa taille, ses ressources, ses enjeux de sécurité. L'utilisateur est invité à consulter le « Guide d'utilisation du référentiel de sécurité de l'information » pour une compréhension globale de l'architecture du référentiel et des modalités d'utilisation associées. »

7.2.2 Gestion et conservation

L'entité identifie, maintient et conserve la documentation nécessaire à la mise en œuvre, au pilotage et à la traçabilité de son dispositif de sécurité de l'information.

Cette documentation couvre notamment la Politique Générale de Sécurité de l'Information (PGSI) et **[préciser la structure documentaire de l'entité, comme par exemple : les politiques thématiques, ainsi que les procédures, guides et documents opérationnels associés.]**, les analyses de risques et les plans de traitement et d'actions correctives associés, les registres et journaux relatifs aux incidents de sécurité, les rapports d'audit, de contrôle et de revue, ainsi que les registres de dérogations et les décisions associées. Elle inclut également tout document contribuant à la gouvernance, à la mise en œuvre ou à l'évaluation de la sécurité de l'information.

La gestion de la conservation de ces documents est assurée en cohérence avec les recommandations des Archives nationales de Luxembourg.

Cette documentation est rendue accessible aux seules personnes autorisées, conformément au principe du besoin d'en connaître. Elle est protégée en termes de confidentialité, d'intégrité et de disponibilité, et maintenue à jour afin d'en garantir la pertinence et la fiabilité dans le temps.

7.3 Gestion des dérogations

Un cadre formalisé de gestion des dérogations aux règles de sécurité de l'information est défini, afin d'encadrer toute situation dans laquelle une exigence du référentiel de sécurité ne peut être respectée de manière temporaire ou permanente.

Ce cadre précise les modalités de demande, d'analyse de risque, de validation, de mise en œuvre de mesures compensatoires, de suivi et de révision des dérogations accordées.

Une dérogation fait l'objet d'une justification documentée, d'une approbation formelle par l'autorité compétente, d'une durée de validité définie et d'un enregistrement dans un registre dédié tenu à jour.

8 Objectifs de la sécurité de l'information

« Note : les domaines de sécurité présentés dans ce chapitre constituent une base de référence pour structurer le référentiel de sécurité de l'entité. Le HCPN/ANSSI met à disposition, en complément du présent modèle de PGSI, des modèles de politiques thématiques ainsi que des lignes directrices précisant les modalités de mise en œuvre opérationnelle associées. Ces ressources visent à accompagner l'entité dans la définition de son cadre de sécurité de l'information.

Les entités adaptent la structure de leur référentiel de sécurité en fonction de leurs enjeux, notamment liés à leur taille, à leurs ressources et à leur exposition aux risques. À ce titre, elles peuvent intégrer directement les domaines de sécurité présentés dans le présent chapitre au sein de la PGSI, ou, lorsque les enjeux de sécurité sont plus élevés, les décliner en politiques thématiques formalisées distinctes.

Pour une vision d'ensemble de l'architecture du référentiel et des modalités d'utilisation associées, il est recommandé de se référer au « Guide d'utilisation du référentiel de sécurité de l'information ».

Les politiques thématiques, lorsqu'elles sont mises en place, peuvent être complétées par des procédures, guides ou tout autre document opérationnel, assurant leur déclinaison et leur mise en œuvre effective au niveau approprié au sein de l'entité. »

[Optionnel : Les domaines thématiques de sécurité présentés dans le présent chapitre peuvent constituer les politiques thématiques de l'entité. Ils couvrent les principaux périmètres de la sécurité de l'information et définissent les objectifs, principes et orientations encadrant leur mise en œuvre.]

8.1 Organisation de la sécurité de l'information

Objectif : Mettre en place un cadre organisationnel structuré permettant de piloter, mettre en œuvre, superviser et améliorer en continu la sécurité de l'information.

L'organe de direction assume la responsabilité globale de la sécurité de l'information et définit les orientations stratégiques, en cohérence avec les missions et les objectifs de l'organisation. Il veille à la mise à disposition des ressources nécessaires afin de garantir la mise en œuvre, le maintien et l'amélioration continue du dispositif de sécurité.

La gouvernance de la sécurité repose sur une répartition claire, formalisée et communiquée des rôles, responsabilités et autorités, adaptée aux besoins de l'organisation et régulièrement revue. Une fonction dédiée, telle qu'un Délégué à la Sécurité de l'Information (DSI), est désignée pour piloter et coordonner le dispositif et rendre compte directement à l'organe de direction. Elle agit en coordination avec la fonction informatique, responsable de la mise en œuvre opérationnelle et du maintien en condition de sécurité des systèmes d'information.

Un dispositif de gouvernance est mis en place afin de structurer l'organisation de la sécurité et d'en assurer le pilotage, notamment au moyen d'un reporting structuré et, lorsque pertinent, d'une instance dédiée telle qu'un Comité de Sécurité de l'Information.

L'organisation maintient enfin des relations appropriées avec les autorités compétentes afin de renforcer ses capacités d'anticipation, de protection et de réponse en matière de sécurité de l'information.

8.2 Gestion des risques

Objectif : S'assurer que les risques pesant sur la sécurité de l'information sont identifiés, évalués, traités et maintenus à un niveau acceptable, conformément à l'appétence et à la tolérance aux risques définies par l'entité.

Un cadre structuré de gestion des risques appliqué à la sécurité des systèmes d'information est mis en place, fondé sur une méthodologie formalisée d'identification, d'analyse, d'évaluation et de traitement des risques. L'appétence au risque, les seuils de tolérance et les critères d'évaluation sont définis.

Chaque risque fait l'objet d'un traitement formalisé, consigné dans un plan de traitement précisant les mesures, les responsabilités, les échéances et les modalités de suivi. Les risques résiduels sont documentés et font l'objet d'une validation appropriée par les instances compétentes.

Un suivi continu de la mise en œuvre des mesures est assuré, ainsi qu'une mise à jour régulière des analyses et des plans de traitement, notamment en cas de changement significatif ou d'incident majeur. Un reporting régulier est assuré auprès de l'organe de direction afin de soutenir la prise de décision et le pilotage des risques.

8.3 Sécurité des ressources humaines

Objectif : Maîtriser les risques liés au facteur humain en garantissant que toute personne intervenant pour le compte de l'entité comprend et applique ses responsabilités en matière de sécurité de l'information.

L'entité intègre les exigences de sécurité de l'information à chaque étape du cycle de vie des ressources humaines, depuis le recrutement et l'intégration jusqu'au départ, en passant par les éventuelles mobilités ou changements de fonction ; ces exigences sont appliquées de manière proportionnée à la sensibilité des missions, aux risques encourus et aux accès associés.

Les rôles et responsabilités en matière de sécurité sont définis et portés à la connaissance des parties concernées, qui sont tenues de les respecter, y compris, le cas échéant, les fournisseurs et prestataires.

Des actions de sensibilisation et de formation continue à la sécurité sont mises en œuvre, adaptées aux rôles et aux niveaux d'exposition aux risques.

Enfin, les changements de fonction et les départs sont encadrés afin de garantir la mise à jour ou la révocation des droits d'accès dans des délais maîtrisés, la restitution des actifs, le maintien des obligations applicables, notamment en matière de confidentialité.

8.4 Gestion des actifs

Objectif : S'assurer que les actifs sont identifiés et bénéficient d'un niveau de protection adapté à leur sensibilité tout au long de leur cycle de vie.

La maîtrise des risques de sécurité de l'information repose sur une connaissance du patrimoine à protéger. À ce titre, les actifs, incluant les informations, sont recensés au sein d'un inventaire structuré et maintenu à jour.

Chaque actif fait l'objet d'une catégorisation formalisée de son niveau de sensibilité ou de criticité, fondée notamment sur les exigences de confidentialité, d'intégrité, de disponibilité, afin de définir le niveau de protection adapté.

Des règles encadrent la gestion et la manipulation des actifs sur l'ensemble de leur cycle de vie, incluant leur acquisition, leur utilisation, leur stockage, leur transfert et leur fin de vie. Ces règles sont adaptées au niveau de sensibilité des actifs et portées à la connaissance de l'ensemble des utilisateurs concernés, y compris les tiers.

Enfin, des règles d'usage acceptable des ressources sont définies et accompagnées d'actions de sensibilisation, afin d'assurer une protection effective et durable du patrimoine informationnel.

8.5 Gestion des accès logiques

Objectif : S'assurer que seuls les accès autorisés aux informations et aux systèmes sont possibles.

La protection des accès repose sur des règles formalisées de contrôle d'accès, fondées sur les besoins métiers et les exigences de sécurité.

Les droits d'accès sont attribués selon les principes du besoin d'en connaître et du besoin d'agir, du moindre privilège et, lorsque pertinent, de la séparation des tâches.

Le cycle de vie des identités et des droits d'accès est encadré, depuis leur création jusqu'à leur modification, leur révocation ou leur suppression, notamment en cas de changement de fonction, de départ ou de fin de contrat.

Les mécanismes d'authentification sont adaptés à la sensibilité des actifs accédés, avec une attention renforcée pour les accès à privilèges, les accès d'administration et les accès à distance.

Les identités et les droits d'accès font l'objet d'un suivi continu et de revues périodiques, afin d'en vérifier la légitimité, la conformité et le maintien dans le temps. Les activités liées aux accès font l'objet, lorsque pertinent, de mécanismes de journalisation et peuvent être soumises à des contrôles et analyses a posteriori.

8.6 Sécurité physique et environnementale

Objectif : Prévenir les accès physiques non autorisés, les dommages et les perturbations environnementales ciblant les systèmes d'information et les informations de l'entité.

Des mesures de protection proportionnées sont définies et mises en œuvre afin de répondre aux menaces physiques et environnementales, ainsi qu'aux risques liés aux dépendances envers les infrastructures techniques de support (électricité, télécommunications, climatisation). Elles couvrent notamment la sécurisation des locaux, la segmentation en zones de sécurité, ainsi que le contrôle, la traçabilité et la surveillance des accès physiques.

Les infrastructures techniques de support sont protégées, supervisées et maintenues en condition opérationnelle, selon des exigences adaptées à leur criticité, au moyen de dispositifs de redondance, d'alimentation de secours et de surveillance assortis de seuils d'alerte définis.

Les accès physiques sont formalisés, attribués selon le moindre privilège, régulièrement revus et révoqués. Les accès des tiers sont encadrés, limités dans le temps, tracés et supervisés, en cohérence avec les risques associés.

Une protection physique adaptée aux risques est mise en œuvre, reposant, lorsque pertinent, sur une organisation des zones et un contrôle des accès, complétés par des mesures de surveillance et de détection appropriées. Les mesures font l'objet de tests réguliers, de revues périodiques et d'améliorations continues.

8.7 Sécurité liée à l'exploitation

Objectif : Assurer le fonctionnement sécurisé et maîtrisé des systèmes d'information, en garantissant la protection des informations et la résilience des services.

Les systèmes d'information sont exploités dans un environnement maîtrisé, fondé sur une architecture sécurisée adaptée aux besoins de disponibilité, d'intégrité et de confidentialité. Cette architecture repose sur le principe de défense en profondeur, intégrant des mécanismes de cloisonnement, de segmentation et de contrôle des flux proportionnés aux risques.

Les activités d'exploitation sont identifiées, encadrées et documentées afin d'assurer un fonctionnement fiable et des interventions maîtrisées, y compris en cas d'incident.

Des mesures de sécurité sont mises en œuvre afin de réduire l'exposition aux menaces, incluant notamment la protection contre les codes malveillants, la gestion des vulnérabilités et l'application de correctifs adaptés à la criticité des systèmes.

Les changements, configurations et mises en production sont encadrés par des pratiques maîtrisées, incluant des tests préalables et une documentation appropriée, afin de limiter les risques de dysfonctionnement ou de compromission.

Des dispositifs de journalisation et de surveillance permettent de tracer les événements pertinents, détecter les activités anormales et traiter les alertes dans des délais appropriés.

Afin d'assurer la résilience des activités, des dispositifs de sauvegarde et de reprise sont mis en œuvre afin de garantir la préservation des données et la restauration des services dans des délais adaptés.

8.8 Sécurité des réseaux et communications

Objectif : Garantir la protection des réseaux et des communications contre les cybermenaces, en assurant la confidentialité, l'intégrité, la disponibilité et l'authenticité des flux d'information.

L'architecture des réseaux et des systèmes d'information est structurée selon des principes de segmentation permettant de cloisonner les systèmes et les flux en fonction de leur sensibilité, afin de contrôler les accès, limiter les communications aux besoins opérationnels et prévenir les accès non autorisés. Elle est documentée, maintenue à jour et revue régulièrement, notamment en cas d'évolution significative ou d'incident.

Les interconnexions avec des systèmes externes sont encadrées et sécurisées. Les accès au réseau, notamment à distance et par des tiers, sont contrôlés et soumis à des mécanismes d'authentification adaptés aux risques. Les communications reposent sur des canaux sécurisés, notamment par le recours au chiffrement lorsque pertinent.

Les réseaux et systèmes d'information font l'objet d'une surveillance adaptée aux risques afin de détecter les activités anormales, les flux illégitimes et les menaces potentielles.

8.9 Acquisition, développement et maintenance des systèmes d'information

Objectif : S'assurer que les systèmes d'information sont acquis, développés et maintenus de manière sécurisée, en intégrant les exigences de cybersécurité tout au long de leur cycle de vie.

L'entité intègre les enjeux de cybersécurité à chaque étape du cycle de vie de ses systèmes d'information, de leur conception à leur décommissionnement. Les besoins en matière de sécurité sont identifiés en amont, tant pour les développements internes que pour les acquisitions, afin de garantir un niveau de protection

adapté aux risques. Les exigences de sécurité sont définies dès la conception, selon le principe de sécurité dès la conception (security by design), afin de renforcer la résilience des systèmes.

L'acquisition de services et de produits informatiques intègre, de manière proportionnée, des considérations de sécurité de l'information, adaptées aux risques et aux besoins de l'entité.

Un cadre de développement sécurisé est défini et appliqué à l'ensemble des projets, internes ou externalisés, sur tout le cycle de vie. Des tests de sécurité sont intégrés de manière continue et adaptés à la criticité des systèmes.

Les environnements de développement, de test et de production sont séparés et sécurisés. Les changements sont encadrés, testés, autorisés et documentés avant leur mise en production, afin de limiter les risques et de garantir l'intégrité des systèmes. Des mesures appropriées sont mises en œuvre pour protéger les données utilisées à des fins de test.

Avant toute mise en production, les systèmes d'information font l'objet de vérifications de sécurité visant à s'assurer de leur conformité aux exigences définies et de leur adéquation aux risques.

8.10 Gestion de la cryptographie

Objectif : Garantir une utilisation appropriée et efficace de la cryptographie afin de protéger la confidentialité, l'intégrité et l'authenticité des informations.

Des mécanismes de cryptographie, notamment le chiffrement, sont mis en œuvre afin d'assurer la confidentialité, l'intégrité et l'authenticité des informations et de les protéger contre tout accès ou altération non autorisés. Leur utilisation est adaptée à la sensibilité des informations, aux systèmes concernés et aux risques associés, notamment pour les données stockées ou transmises.

Le choix des algorithmes, protocoles et solutions repose sur des standards reconnus, dans le respect des exigences légales et des bonnes pratiques.

La gestion des clés cryptographiques est maîtrisée sur l'ensemble de leur cycle de vie (génération, stockage, utilisation, rotation, révocation et destruction), avec des mesures garantissant leur protection, leur traçabilité et leur disponibilité.

8.11 Sécurité de la chaîne d'approvisionnement

Objectif : Assurer la maîtrise des risques liés à la chaîne d'approvisionnement en encadrant les relations avec les fournisseurs et prestataires.

Les relations avec les fournisseurs et prestataires sont encadrées par des exigences de sécurité de l'information définies en cohérence avec les risques identifiés et les standards reconnus, et proportionnées à la criticité des services fournis et des informations traitées. À cette fin, un référentiel des fournisseurs et prestataires est maintenu à jour afin de soutenir l'identification et le suivi des risques associés.

Les risques liés aux fournisseurs et prestataires, y compris ceux associés à la sous-traitance, sont analysés en amont de tout engagement, puis suivis tout au long du cycle de vie des services et produits Technologies de l'Information et de la Communication (TIC), jusqu'à la fin de la relation.

La sélection et l'évaluation des fournisseurs et prestataires reposent sur des exigences formalisées, incluant leurs pratiques de sécurité, leur capacité à satisfaire les exigences de l'entité, la résilience de leurs produits et services, ainsi que les risques de dépendance et de faible réversibilité.

Les relations contractuelles intègrent des exigences de sécurité adaptées, notamment en matière de gestion des incidents, des vulnérabilités, de contrôle des accès, de sous-traitance, de droit d'audit et de réversibilité, afin d'assurer la maîtrise des risques sur toute la durée des engagements.

Les fournisseurs et prestataires font l'objet d'un suivi et d'une évaluation structurés en matière de sécurité, portant notamment sur les incidents de sécurité, les vulnérabilités et toute évolution susceptible d'impacter la sécurité, avec mise en œuvre et suivi des mesures correctrices appropriées.

8.12 Gestion des événements et incidents liés à la sécurité de l'information

Objectif : Garantir une détection, une réaction et une communication rapides face aux événements et incidents cyber, afin d'en minimiser les impacts sur les activités de l'entité.

La détection des événements de sécurité repose à la fois sur une vigilance humaine et sur des mécanismes techniques. Une culture de sécurité favorise la remontée rapide de toute anomalie ou activité suspecte par les utilisateurs, tandis que des mécanismes de surveillance et de détection, adaptés aux risques, permettent d'identifier les événements de sécurité et de détecter les incidents dans des délais appropriés.

Un cadre structuré de gestion des événements et incidents de sécurité de l'information est défini, formalisé et maintenu. Il couvre l'ensemble du cycle de vie des événements et incidents, depuis la détection ou le signalement jusqu'au retour d'expérience.

Les rôles, responsabilités, modalités d'escalade, circuits de décision, critères de qualification et règles de catégorisation des incidents y sont précisés, afin d'en déterminer la nature, la gravité et la priorité de traitement.

Les incidents font l'objet d'une documentation et d'une analyse a posteriori visant à capitaliser les retours d'expérience (*lessons learned*), afin d'alimenter des actions d'amélioration continue du dispositif de sécurité.

8.13 Gestion de la conformité

Objectif : S'assurer que les exigences applicables en matière de sécurité de l'information, qu'elles soient issues des risques ou d'exigences réglementaires et contractuelles, sont mises en œuvre, maintenues et adaptées dans le temps.

La démarche de cybersécurité s'inscrit dans le respect du cadre légal et réglementaire applicable. À ce titre, les exigences applicables aux systèmes d'information sont identifiées, documentées, maintenues à jour et communiquées aux parties concernées.

Un dispositif formalisé permet de suivre et d'évaluer l'efficacité des mesures de sécurité, sur la base d'indicateurs pertinents et de méthodes reconnues (p.ex. activités de contrôles internes et d'évaluation ou tests de sécurité), mises en œuvre de manière régulière et proportionnée aux risques.

Les résultats sont analysés, consolidés et communiqués aux instances de gouvernance afin d'éclairer la prise de décision, de démontrer la conformité, d'identifier les non-conformités et de piloter les actions correctrices, en cohérence avec les priorités de traitement des risques.

9 Annexes

9.1 Glossaire

Le présent document s'appuie sur un ensemble de définitions techniques et organisationnelles visant à garantir une compréhension commune des concepts liés à la sécurité de l'information :

- [Définition 1]

- [Définition 2]
- ....

Note : L'entité définit, dans le présent glossaire, les termes spécifiques nécessaires à la compréhension du document. À ce titre, elle s'appuie sur le « Glossaire de la sécurité de l'information *» mis à disposition par le HCPN/ANSSI, auquel elle se réfère pour assurer la cohérence des définitions utilisées dans le présent document et, plus largement, dans l'ensemble du référentiel.*