ANSSI.lu | Agence nationale de la sécurité des systèmes d'information Luxembourg

Politique générale de la sécurité de l'information de l'État luxembourgeois

Version 2.0

Préambule

Cette nouvelle version de la politique générale de la sécurité de l'information de l'État a été élaborée sur base des conclusions d'un «proof of concept » réalisé, sur base d'une première version approuvée par le Conseil de Gouvernement en date du 25 mars 2016, au sein du Centre des technologies de l'information de l'État. Cette nouvelle version se veut plus condensée, plus générale et moins dirigiste. Elle tient en outre mieux compte du contexte spécifique dans lequel s'inscrit l'action de l'État et de ses entités.

La sécurité de l'information est une priorité majeure du gouvernement du Grand-Duché de Luxembourg et son importance justifie une politique dédiée à la sécurité de l'information de l'État. Elle a pour objet de garantir la confidentialité, l'intégrité et la disponibilité de l'information gérée par l'État.

Cette politique contribue à la mise en œuvre de la stratégie nationale de cybersécurité approuvée et rendue exécutoire par le Conseil de gouvernement en date du 26 janvier 2018. Elle constitue l'outil de gouvernance de la sécurité de l'information de l'État et étaie ainsi le développement de la société numérique dans l'esprit de l'initiative « Digital Lëtzebuerg ».

La gouvernance de la sécurité de l'information de l'État s'articule autour des principes fondateurs, dont voici les éléments clés:

- Afin d'atteindre les objectifs énoncés et de minimiser les risques liés au traitement de l'information, la sécurité de l'information s'inscrit au cœur de toutes les activités de l'État luxembourgeois.
- Les départements ministériels, les administrations et services de l'État luxembourgeois mettent en œuvre, en fonction de leurs compétences respectives, les mesures appropriées de protection de l'information contre toute modification, destruction et divulgation non autorisée, accidentelle ou intentionnelle et, le cas échéant, les mesures nécessaires pour assurer la fiabilité et la non-répudiation de l'information. À cette fin, ils s'investissent dans une démarche de gestion de la sécurité de l'information, basée sur une approche structurée de gestion des risques selon le principe de la proportionnalité.

Le personnel de l'État est invité à prendre connaissance de l'engagement demandé et à contribuer avec toutes ses compétences et son savoir-faire à la réalisation de l'objectif ultime qui est la protection appropriée de l'information, en vue d'assurer la confiance des citoyens, des entreprises exerçant une activité au Luxembourg et des États partenaires dans les services de l'État luxembourgeois.

Historique

Version	Date	Auteur	Commentaire
1.0	24/03/2016	ANSSI	Publication de la première version, approuvée par le Conseil du Gouvernement en sa séance du 16 mars 2016
2.0	25/07/2018	ANSSI	Publication de la deuxième version, approuvée par le Conseil du Gouvernement en sa séance du 13 juillet 2018

Table des matières

1 Introduction

1.1 Contexte

Par arrêté grand-ducal du 9 mai 2018 portant fixation de la gouvernance en matière de gestion de la sécurité de l'information, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), sous l'autorité du Haut Commissariat à la Protection Nationale (HCPN), a été chargée de définir, après concertation des acteurs concernés, la politique générale de sécurité de l'information de l'État luxembourgeois.

La présente politique, élaborée par l'ANSSI en étroite concertation avec le Centre des Technologies de l'Information de l'État (CTIE), a été approuvée par le Conseil de gouvernement.

La politique générale et l'ensemble des documents connexes sont dénommées « politique de sécurité de l'information de l'État luxembourgeois » (PSI-LU).

La PSI-LU est alignée aux objectifs de la stratégie nationale en matière de cybersécurité.

1.2 Objectifs

La présente politique décrit les objectifs généraux de sécurité de l'information (au chapitre 2), ses principes fondateurs (au chapitre 3) et le cadre organisationnel de la gestion de la sécurité de l'information de l'État (au chapitre 4). L'objectif de cette politique générale et des futurs documents connexes est d'assurer que les meilleures pratiques soient utilisées et le soin nécessaire appliqué afin de protéger l'information gérée par les départements ministériels, les administrations et services de l'État luxembourgeois. Ainsi, elle contribue à renforcer la confiance des citoyens, des entreprises exerçant une activité au Luxembourg et des États partenaires dans les services de l'État luxembourgeois.

1.3 Champ d'application

La présente politique générale, ainsi que les lignes directrices émises dans le cadre de futurs documents connexes, sont considérées comme recommandations aux départements ministériels, administrations et services de l'État luxembourgeois, dénommés par la suite « les entités ».

La sécurité de l'information concerne les actifs gérés par les entités.

Par le terme « actif », il y a lieu de comprendre tout ce qui présente une valeur pour l'entité, notamment :

- les informations et les données ;
- les documents et les archives[1] ;
- les actifs techniques, par exemple les systèmes d'information ;
- les bâtiments et sites ;
- les personnes physiques avec leurs connaissances et compétences ;
- les processus et services.

La politique de sécurité de l'information de l'État s'applique à l'information durant tout son cycle de vie, c'est-à-dire depuis la création, pendant le traitement, durant l'archivage jusqu'à la destruction.

La présente politique ayant un caractère général et étant inspirée des normes, standards et bonnes pratiques internationaux, est en principe applicable à tout type d'entité. Dans ce sens, elle peut aussi servir de référence aux organismes non directement concernés.

[1] sans préjudice des dispositions de la loi du 25 juillet 2015 relative à l'archivage électronique et portant modification: 1. de l'article 1334 du Code civil; 2. de l'article 16 du Code de commerce; 3. de la loi modifiée du 5 avril 1993 relative au secteur financier.

La politique contitue un socle minimal de règles qui s'appliquent sans préjudice de dispositions spécifiques plus contraignantes dans un contexte spécifique. [1]

2 Objectifs de la sécurité de l'information

2.1 Objectifs généraux

La sécurité de l'information est un facteur clé de succès pour les services fournis par l'État.

Les principaux objectifs généraux de la sécurité de l'information consistent à :

- préserver **la confidentialité** de l'information sensible gérée par l'État de façon à limiter l'accès et la divulgation aux seules personnes autorisées à en prendre connaissance ;
- assurer **l'intégrité** de l'information et des processus de gestion de l'information de façon à ce que l'information ne soit pas détruite ou altérée sans autorisation ;
- assurer **la disponibilité** de l'information et des services de façon à ce que l'accès à l'information par une personne autorisée soit garantie en temps voulu et de la manière requise ;
- apprécier et traiter **les risques liés à la sécurité de l'information** de façon à adopter des mesures de sécurité appropriées. La valeur de l'information peut être estimée au regard des conséquences négatives que causerait l'absence, la perte, le vol ou la corruption de ladite information ;
- assurer **la gestion de la sécurité de l'information** selon des méthodes effectives, efficaces, documentées et transparentes ;
- assurer **la mise en œuvre des principes de protection des données à caractère personnel**: conformité, transparence et responsabilisation (« accountability »).

Le terme « information » inclut dans ce contexte aussi bien les données propres que celles des citoyens, des entreprises et des partenaires lorsqu'elles sont gérées par l'État.

2.2 Objectifs génériques

Les objectifs génériques de la sécurité de l'information, permettant d'assurer l'atteinte des objectifs généraux, sont détaillés à titre indicatif dans l'annexe 1. Ils ont été dégagés de la série de normes internationales ISO/IEC 27000, ont été adaptés au contexte de la présente politique et sont structurés par domaines :

- Organisation de la sécurité de l'information et sécurité des ressources humaines ;
- Gestion des actifs ;
- Contrôle d'accès ;
- Cryptographie ;
- Sécurité physique et environnementale ;
- Sécurité liée à l'exploitation ;
- Sécurité des communications ;
- Acquisition, développement et maintenance des systèmes d'information ;
- Relations avec les fournisseurs ;
- Gestion des incidents liés à la sécurité de l'information ;
- Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité ;
- Conformité.

[1] Ainsi, par exemple, la sécurité des informations classifiées est régie par la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité et ne fait pas l'objet de la présente politique.

Dans le cadre d'une approche d'implémentation structurée qui tient compte de la situation spécifique de l'entité et de sa situation de risque, l'ANSSI assiste, en concertation avec le CTIE, et à leur demande, les entités à identifier les objectifs applicables et à définir les mesures de sécurité appropriées.

2.3 Politiques générales par domaine

A la demande des acteurs ayant dans leurs attributions des domaines spécifiques et en concertation étroite avec ceux-ci, l'ANSSI définit des politiques de sécurité de l'information par domaine, qui détaillent les objectifs génériques de la sécurité de l'information.

3 Principes fondateurs de la sécurité de l'information de l'État

3.1 Sécurité bien comprise

Le personnel de l'État est régulièrement sensibilisé et formé[1] aux aspects de la sécurité de l'information ainsi qu'aux consignes de base relatives à l'utilisation des systèmes d'information de l'État énoncées dans la Charte de bonne conduite en matière de sécurité de l'information numérique.

3.2 Respect des normes et des bonnes pratiques

La politique de sécurité de l'information de l'État est inspirée des normes, standards et bonnes pratiques internationalement reconnus et approuvés dans le domaine de la sécurité de l'information, notamment les normes de la série ISO/IEC 27000.

3.3 Approche basée sur le risque

Les mesures de sécurité de l'information sont sélectionnées en fonction d'une analyse de risque effectuée selon une méthode confirmée[2], de façon à minimiser les risques et à maintenir les coûts de sécurité à un niveau acceptable. L'État cherche à réduire les risques selon le principe de la proportionnalité et de la nécessité, mais se réserve le droit d'assumer les risques résiduels.

En fonction de l'évaluation des risques et du niveau de résilience visé, un ensemble de mesures de prévention, de détection, de réponse et de récupération est mis en œuvre.

3.4 Ressources

Les entités veillent à consacrer à la sécurité de l'information de l'État les moyens humains et financiers adaptés en fonction de la situation de risque spécifique.

3.5 Développement continu vers l'excellence

L'environnement de gestion de l'information de l'État change continuellement. Il convient d'adopter une approche itérative et d'amélioration continue pour rester en phase avec les défis actuels et futurs.

3.6 Sécurité intégrée et transversale

La sécurité de l'information n'est pas une fin en soi, mais elle fait partie intégrante de toute activité de l'État, de la conception à la maintenance en passant par la spécification, l'implémentation, le déploiement et la mise en service

[1] Formations dans le domaine de la sécurité de l'information de l'Institut national d'administration publique (INAP) en collaboration avec CASES

[2] L'ANSSI met à disposition des entités intéressées l'outil d'analyse et de gestion des risques MONARC de CASES hébergé au sein du GOVCLOUD et propose, à la demande, un accompagnement professionnel à la réalisation d'une première analyse des risques.

selon le principe de « Security by design ». Elle est la pierre angulaire de la gestion de tous les projets, processus et activités quotidiennes.

Lors de la conception de systèmes traitant des données à caractère personnel, les principes de « Protection des données dès la conception » et « Protection des données par défaut» sont considérés.

3.7 Communication et collaboration

La politique de sécurité de l'information de l'État, la Charte de bonne conduite en matière de sécurité de l'information numérique ainsi que les lignes directrices et circulaires relatives à la sécurité de l'information sont systématiquement communiquées à l'ensemble du personnel de l'État.

La sécurité de l'information est l'affaire de tous. Les entités et les agents de l'État sont appelés à contribuer activement à assurer la sécurité de l'information de l'État et à s'entraider mutuellement dans la réalisation des objectifs de sécurité de l'information.

3.8 Respect et tracabilité

Le personnel interne et externe connaît les règles émanant de la politique de sécurité de l'information de l'État et reconnaît l'importance de la sécurité de l'information pour l'État.

Les mesures prises pour mettre en œuvre la politique de sécurité sont documentées.

3.9 Culture de sécurité de l'information

La présente politique établit un point de départ pour une gestion appropriée de la sécurité de l'information. L'État compte sur la coopération active du personnel afin d'assurer un environnement de travail sécurisé.

La politique de sécurité de l'information contribue ainsi à instaurer progressivement une véritable culture de la sécurité de l'information.

3.10 Révision

La politique de sécurité de l'information de l'État est revue en cas de changements législatifs, organisationnels, technologiques, respectivement sur base de l'évolution de la situation des menaces et des risques.

4 Organisation et gestion de la sécurité de l'information de l'État

La sécurité de l'information de l'État est gérée, pilotée et coordonnée. Tous les acteurs impliqués travaillent de concert pour assurer la sécurité de l'information globale de l'État.

4.1 Les entités

Les entités sont responsables de la sécurité de l'information dans leur champ d'attribution et, à cette fin, elles prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques qui menacent la sécurité de l'information. Ces mesures garantissent un niveau de sécurité adapté au risque, compte tenu de la criticitéde l'information gérée, de la taille et de la structure de l'entité, de la complexité technologique des systèmes d'information de l'entité, des besoins et exigences spécifiques de l'entité en matière de sécurité de l'information, des coûts associés et des moyens disponibles.

L'annexe 2 met en évidence l'approche recommandée de mise en œuvre de la politique de sécurité de l'information de l'État en fonction du type d'entité.

4.2 L'Agence nationale de sécurité des systèmes d'information (ANSSI)

L'ANSSI assiste, à leur demande, les entités dans l'implémentation des politiques et lignes directrices de sécurité de l'information et propose aux entités intéressées un accompagnement dans le cadre de leur analyse et gestion des risques de la sécurité de l'information. Par ailleurs, l'ANSSI a la mission de promouvoir la sécurité de l'information par le biais de mesures de sensibilisation à l'adresse des dirigeants et des utilisateurs des entités.

Annexe 1: Objectifs génériques de la sécurité de l'information par domaine

Les objectifs de sécurité génériques ci-dessous, dégagés de la série de normes internationales ISO/IEC 27000, sont donnés à titre indicatif. Dans le cadre de l'implémentation et en tenant compte de la situation spécifique de l'entité et de sa situation risque, les objectifs applicables sont identifiés et les mesures de sécurité associées définies. À la demande, l'ANSSI, en concertation avec le CTIE, assiste les entités dans leur démarche d'implémentation.

Organisation de la sécurité de l'information et sécurité des ressources humaines

- la stratégie de l'entité en matière de sécurité de l'information est clairement définie et un cadre structuré de gestion de la sécurité de l'information, bénéficiant du soutien actif de la direction, est établi ;
- les rôles et responsabilités en matière de sécurité de l'information sont clairement définis et attribués à tous les niveaux de l'entité, et l'ensemble du personnel (interne et externe) en est systématiquement informé ;
- le personnel est régulièrement formé et sensibilisé à la sécurité de l'information ;
- la Charte de bonne conduite en matière de sécurité de l'information numérique est connue et respectée par tout le personnel ;
- les aspects de la sécurité de l'information, notamment la gestion des accès, font partie intégrante des processus de gestion de ressources humaines (arrivées, départs, mutations, changement de fonction du personnel, etc.) ;
- les aspects de la sécurité de l'information dans le contexte du télétravail, de l'accès à distance et de l'utilisation des appareils et technologies mobiles sont assurés par des moyens organisationnels et techniques appropriés.

Gestion des actifs

- les moyens de traitement de l'information de l'État et les actifs associés à la sécurité de l'information sont identifiés et gérés tout au long de leur cycle de vie ;
- les informations sont protégées en fonction de leur degré d'importance en ce qui concerne leur confidentialité, intégrité et disponibilité.

Contrôle d'accès

- l'accès à l'information et aux moyens de traitement de l'information est accordé en fonction des rôles et responsabilités du personnel, et selon un processus d'autorisation et de révision formalisé ;
- les identités des utilisateurs sont gérées et des moyens d'authentification adaptés au degré d'importance de l'information sont mis en œuvre ;
- l'attribution et l'utilisation d'accès privilégiés sont restreintes, contrôlées et tracées.

Cryptographie

- la confidentialité, l'authenticité et/ou l'intégrité de l'information sensible sont assurées par des mesures cryptographiques.

Sécurité physique et environnementale

- l'information et les moyens de traitement de l'information sont protégés par des mesures techniques et organisationnels appropriées contre tout accès physique non autorisé afin d'empêcher leur perte, endommagement, vol ou compromission ;
- les moyens de traitement de l'information et les supports d'information sensibles sont protégés contre les défaillances techniques (rupture de l'alimentation électrique, défaut du système de climatisation, etc.) et les risques environnementaux (incendie, inondation, etc.), les désastres naturels, les attaques malveillantes et les accidents.

Sécurité liée à l'exploitation

- les moyens de traitement de l'information sont exploités selon des procédures formalisées et les changements aux moyens de traitement sont gérés ;
- la séparation des environnements d'exploitation et de développement/test réduit les risques d'accès et de changement non autorisés de l'information et des moyens de traitement de l'information ;
- l'information et les moyens de traitement de l'information sont protégés contre les logiciels malveillants par des mesures de prévention, de détection et de récupération ;
- la disponibilité et l'intégrité de l'information et des moyens de traitement de l'information sont assurées par des sauvegardes régulières et des tests de restauration systématiques ;
- les événements liés à la sécurité de l'information sont journalisés et vérifiés régulièrement; les journaux d'événement sont protégés contre l'accès non autorisé et la compromission ;
- l'exposition aux vulnérabilités techniques est évaluée systématiquement et les mesures appropriées sont mises en œuvre pour traiter le risque associé.

Sécurité des communications

- les infrastructures de communication sont architecturées et sécurisées par des moyens techniques et organisationnels appropriés afin de protéger l'information véhiculée et les moyens de traitement de l'information ;
- les échanges d'information avec des tiers non étatiques sont régis par des accords formalisés et couverts par des engagements de confidentialité et de non-divulgation.

Acquisition, développement et maintenance des systèmes d'information

- la sécurité de l'information fait partie intégrante des systèmes d'information tout au long de leur cycle de vie.

Relations avec les fournisseurs

- les exigences applicables de la sécurité de l'information aux prestations de service et fournitures externes sont définies dans les contrats avec les fournisseurs.

Gestion des incidents liés à la sécurité de l'information

- les événements et failles de sécurité sont signalés et appréciés en vue de leur qualification comme incident; les incidents de sécurité sont gérés conformément aux procédures définies ; tous les incidents de sécurité d'envergure affectant les réseaux et les systèmes de communication et de traitement de l'information de l'État sont traités par le GOVCERT et, si nécessaire, selon les modalités du plan d'intervention d'urgence « PIU Cyber » ;
- les incidents de sécurité clôturés sont analysés systématiquement en vue d'une mise en œuvre de mesures préventives.

Aspects de sécurité de l'information dans la gestion de la continuité de l'activité

- les exigences en matière de sécurité de l'information et de continuité de la gestion de la sécurité de l'information font partie intégrante de la gestion de la continuité de l'activité ;
- les moyens de traitement de l'information sont suffisamment redondants pour répondre aux exigences de disponibilité.

Conformité

- le respect des exigences applicables de la politique de sécurité de l'information est assuré et vérifié régulièrement.

Annexe 2: Approche recommandée de mise en œuvre de la politique de sécurité de l'information de l'État par type d'entité

	Entités type A	Entités type B	Entités type C
Structure type	• entités de petite taille • entités sans service IT propre ou avec petit service IT avec ou sans personnel détaché du CTIE	• entités de taille moyenne • entité avec service IT propre de taille moyenne	• entités de taille moyenne à importante • entités avec service IT propre de taille appropriée et couvrant les différents domaines IT
Critères	• traitement exclusif de données peu sensibles ou publiques • pas de traitement de données à caractère personnel, respectivement pas de traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques dans le sens du RGPD[1] • recours aux services IT du CTIE et pas de dépendance significative des services métier d'une infrastructure IT propre • pas de contraintes légales ou réglementaires spécifiques dans le domaine de la sécurité de l'information	• traitement de données sensibles • pas de traitement de données à caractère personnel, respectivement pas de traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques dans le sens du RGPD • infrastructure IT hybride avec recours aux services IT du CTIE et dépendance des services métier d'une infrastructure IT propre • pas de contraintes légales ou réglementaires spécifiques dans le domaine de la sécurité de l'information	• traitement de données hautement sensibles • traitement d'un volume important de données sensibles • traitement de données à caractère personnel susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques dans le sens du RGPD • dépendance des services métier d'une infrastructure IT propre d'envergure • contraintes légales ou réglementaires spécifiques dans le domaine de la sécurité de l'information
Approche recommandée	• focus sur la sensibilisation du personnel • application de la Charte de bonne conduite en matière de sécurité de l'information numérique	• sensibilisation du personnel • application de la Charte de bonne conduite en matière de sécurité de l'information numérique • analyse des risques afin d'identifier et d'apprécier les risques et de définir l'approche appropriée de gestion de la sécurité de l'information • attribution du rôle de délégué à la sécurité de l'information (DSI) à un membre de la hiérarchie de l'entité	• sensibilisation du personnel • application de la Charte de bonne conduite en matière de sécurité de l'information numérique • établissement d'un cadre structuré de gestion de la sécurité de l'information basé sur une approche de gestion des risques • désignation d'un délégué à la sécurité de l'information (DSI) • rapprochement, conformité ou certification ISO/IEC 27001 ou autre norme équivalente

[1] 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 et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

Annexe 3: Acronymes et glossaire

Acronymes

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information.
CTIE	Centre des Technologies de l'Information de l'État.
GOVCERT	CERT Gouvernemental ; Centre de traitement des urgences informatiques.
HCPN	Haut-Commissariat à la Protection Nationale.
PSI-LU	Politique de sécurité de l'information de l'État luxembourgeois ; la politique générale de sécurité de l'information de l'État luxembourgeois et l'ensemble de ses documents connexes.

Glossaire

Confidentialité	Propriété selon laquelle l'information n'est pas rendue disponible ni divulguée à des personnes, des entités ou des processus non autorisés.
Disponibilité	Propriété d'être accessible et utilisable à la demande par une entité autorisée.
Intégrité	Propriété d'exactitude et de complétude.
Protection des données par défaut	Démarche qui consiste à intégrer les principes de protection des données et le respect de la vie privée directement dans la conception et le fonctionnement d'un système de traitement de l'information, mais également dans l'élaboration de pratiques responsables. Le respect de la vie privée par défaut signifie qu'un haut niveau de protection de la sphère privée/protection des données est une propriété par défaut d'un système de traitement de l'information. Les concepts de « Protection des données par défaut» et « Protection des données dès la conception» sont étroitement liés.
Protection des données dès la conception	Démarche qui consiste à intégrer les principes de protection des données et le respect de la vie privée directement dans la conception et le fonctionnement des systèmes et réseaux informatiques, mais également dans l'élaboration de pratiques responsables. Le respect de la vie privée dès la conception signifie prendre en compte dès le début les exigences en matière de protection de la sphère privée/protection des données et intégrer les outils de protection directement dans le système de traitement de l'information, au lieu de les ajouter ultérieurement sous forme de compléments. Les concepts de « Protection des données par défaut» et « Protection des données dès la conception» sont étroitement liés.
Security by design	Approche de conception qui vise à rendre les systèmes exempts de vulnérabilités et imperméables aux attaques.
Traçabilité	Possibilité d'identifier l'origine et de reconstituer les différentes étapes d'une activité de gestion ou de traitement de l'information.