STATEC

Système de management de la sécurité de l'information (SMSI)

Politique de sécurité de l'information (ST-SécuInfo)

Informations générales

Type	Politique
Référence	00-00
Version	1.1
État	Version finale
Gestionnaire	RSSI
Classification	Publique

Historique

Version	Date	Auteur	Modifications
1.0	10/10/2017	STATEC	Mise en application d'une politique de Sécurité du système d'information
1.1	26/03/2019	S. Allegrezza	Validation de la version 1.1

Approbations

Nom	Fonction	Responsabilité	Signature
Serge Allegrezza	Directeur	Validation	04/04/2019 X Allegrezza serge Signed by: Sergio Allegrezza

Avant-propos du Directeur

Le STATEC (Institut national de la statistique et des études économiques du Grand-Duché de Luxembourg) est une administration publique, sous l'autorité du Ministère de l'Économie. Ses missions consistent à fournir aux décideurs publics et privés ainsi qu'aux citoyens un service public d'information statistique de haute qualité.

Dans le cadre de ces activités, la sécurité lors de la collecte, du traitement, du stockage et de la diffusion de l'information constitue un enjeu majeur, que ce soit en termes de confidentialité, d'intégrité, de disponibilité ou de traçabilité. En effet, en tant qu'entité étatique, mais aussi par la nature des informations qu'il publie ou le public qu'il touche, le STATEC peut être la cible d'attaques informatiques. De plus, dans un contexte global de numérisation, et d'interconnexions ou de sous-traitance, des vulnérabilités peuvent apparaître et compromettre la sécurité de l'information. Finalement, le contexte légal contribue également au devoir de sécurité grâce à des réglementations qui visent à protéger les informations à caractère personnel.

Il est donc primordial de définir les principes, les objectifs, les règles de sécurité ainsi que le système de management qui gouvernent la sécurité de l'information au sein du STATEC, ce qui est réalisé à travers cette politique de sécurité de l'information et tous les documents y référés.

Notre approche est alignée avec l'approche générale de l'État luxembourgeois et s'appuie sur les normes ISO/IEC 27001:2013 qui décrit les exigences à un système de management que le STATEC aimerait atteindre à terme, et ISO/IEC 27002:2013, qui est le guide de référence des bonnes pratiques en matière de sécurité de l'information. Le cadre d'évaluation, prôné par EUROSTAT au travers de l'ESS IT Security Framework, est également basé sur cette norme.

Je demande à tous les agents et tout le personnel impliqué à respecter cet engagement, à contribuer avec toutes leurs compétences pour atteindre l'objectif de protection adéquate des informations que nous gérons.

Luxembourg, le 26 mars 2019

Table des matières

Liste des tableaux

1 Introduction

1.1 Contexte

Le STATEC (Institut national de la statistique et des études économiques du Grand-Duché de Luxembourg) est une administration publique, sous l'autorité du Ministère de l'Économie.

Ses missions consistent à fournir aux décideurs publics et privés ainsi qu'aux citoyens un service public d'information statistique de haute qualité. Dans l'exercice de ces missions, le STATEC bénéficie de l'indépendance scientifique et professionnelle.

Dans le cadre de ces activités, la sécurité lors de la collecte, du traitement, du stockage et de la diffusion de l'information constitue un enjeu majeur, que ce soit en termes de confidentialité, d'intégrité, de disponibilité ou de traçabilité. En effet, en tant qu'entité étatique, mais aussi de par la nature des informations qu'il publie ou le public qu'il touche, le STATEC peut être la cible d'attaques informatiques. De plus, dans un contexte global de numérisation, et d'interconnexions ou de sous-traitance, des vulnérabilités peuvent apparaître et compromettre la sécurité de l'information. Finalement, le contexte légal contribue également au devoir de sécurité grâce à des réglementations qui visent à protéger les informations à caractère personnel.

Il est donc primordial de définir les règles ainsi que l'organisation qui gouvernent la sécurité de l'information au sein du STATEC, ce qui est réalisé à travers cette politique de sécurité de l'information.

Le présent document met donc en application une politique de sécurité de l'information et un Système de Management de la Sécurité de l'Information (SMSI) pour le STATEC. Il décrit les objectifs, les piliers et le cadre d'évolution de la sécurité d'information.

Cette politique est alignée avec la politique de sécurité de l'information de l'État luxembourgeois, qui a été approuvée par le Conseil de gouvernement en date du 25 juillet 2018.

Elle s'appuie sur la norme ISO 27002:2013, qui est le guide de référence des bonnes pratiques en matière de sécurité des systèmes d'information. Le cadre d'évaluation, prôné par EUROSTAT au travers de l'ESS IT Security Framework, est également basé sur cette norme.

1.2 Objectifs

La présente politique de sécurité de l'information du STATEC, abrégée ST-SécuInfo, décrit les objectifs généraux de sécurité (au chapitre 2) et les principes (au chapitre 3). Elle vise à énoncer l'engagement et la vision de la Direction en ce qui concerne la sécurité du système d'information ainsi que la gestion des risques (au chapitre 4) et la structure des documents du SMSI (au chapitre 5). Elle exige l'engagement de tout le personnel pour contribuer à atteindre ces objectifs.

Elle définit la manière dont la politique de sécurité de l'information est communiquée à l'ensemble du personnel, et détermine les principales tendances de la gestion de la sécurité de l'information. L'objectif de cette politique et des politiques, procédures et standards connexes est d'assurer que les meilleures pratiques soient utilisées et le soin nécessaire appliqué, afin de protéger les informations traitées au STATEC. Ainsi, elle contribue à assurer la confiance des citoyens, du gouvernement, des partenaires, et d'Eurostat dans les services du STATEC.

1.3 Domaine d'application

Le domaine d'application de ce document est l'ensemble des activités et des actifs du STATEC. Par le terme « actif », il faut comprendre tout ce qui présente une valeur pour l'organisation, par exemple :

- les informations et les données ;
- les documents et les archives indépendamment de leur format (numérique ou analogique) ;
- les actifs techniques, par exemple les systèmes d'information ;
- les bâtiments et les sites ;
- les processus et services.

La présente politique s'applique à l'information pendant tout son cycle de vie, c'est-à-dire, depuis sa création, durant son traitement, son archivage, et jusqu'à sa destruction.

Il s'adresse à l'ensemble des utilisateurs du système d'information du STATEC dont :

- l'ensemble des agents du STATEC autorisés à accéder, utiliser ou traiter des informations ou des ressources du système d'information quel que soit leur statut ;
- les chercheurs de STATEC Research ASBL travaillant dans les locaux du STATEC ;
- les stagiaires, les étudiants, les apprentis ;
- les personnels engagés dans le cadre d'une mesure d'emploi ;
- les employés de sociétés prestataires ;
- les visiteurs occasionnels.

1.4 Entrée en vigueur et consignes de lecture

Ce document entre en vigueur une fois approuvé selon les processus du SMSI et mis à disposition à l'ensemble du personnel du STATEC sous https://www.statec.etat.lu/InfoSec.

Le non-respect de ce document SMSI et des documents annexes est susceptible d'engager la responsabilité de l'utilisateur conformément aux lois et réglementations en vigueur, et tout particulièrement au statut du fonctionnaire et à l'article 458 du Code pénal.

Il restera en vigueur jusqu'à sa révocation ou son remplacement sur https://www.statec.etat.lu/InfoSec. Seule la version actuelle sur le site est le document de référence.

L'usage de l'indicatif présent ou des termes « DOIT », « OBLIGATOIRE », « EST REQUIS » ou « DEVRA » dans une déclaration signifie que l'énoncé est considéré comme une obligation.

L'utilisation de mots tels que « DEVRAIT » ou de l'adjectif « RECOMMANDÉ » signifie qu'il peut exister des raisons licites qui permettraient de se dispenser d'exécuter l'affirmation contenue dans le document, mais que les implications d'une telle dispense doivent être parfaitement comprises et évaluées avant d'agir autrement.

L'expression « Il PEUT » ou l'adjectif « OPTIONNEL » signifient que la mise en œuvre de l'affirmation est laissée au choix de l'exécutant.

1.5 Références

[1] STATEC, SMSI, Liste de documents du SMSI, STA_01-01.

[2] STATEC, SMSI, Référentiel de documents SMSI classifiés internes, mis à la disposition de tous les employés de STATEC, https://www.statec.etat.lu/InfoSec

[3] ANSSI, Politique de Sécurité de l'Information de l'État luxembourgeois, Politique générale (PSI-LU).

[4] Loi modifiée du 10 juillet 2011 portant organisation de l'Institut national de la statistique et des études économiques.

[5] Règlement modifié CE N°223/2009 du PARLEMENT EUROPÉEN ET DU CONSEIL du 11 mars 2009 relatif aux statistiques européennes.

[6] STATEC, SMSI, Liste des rôles et responsabilités, STA_01-02

1.6 Acronymes

ANSSI	l'Agence Nationale de la Sécurité des Systèmes d'Information
CNPD	Commission Nationale pour la Protection des Données
CTIE	Centre des Technologies de l'Information de l'État
DPO	Délégué à la protection des données (angl. Data Protection Officer)
ESS	European Statistical System
RSSI	Responsable de la Sécurité des Systèmes d'Information
SMSI	Système de Management de la Sécurité de l'Information

1.7 Glossaire

Actif	Tout ce qui a de la valeur pour l'organisation.
Amélioration continue	Activité régulière destinée à améliorer les performances.
Analyse du risque	Processus mis en œuvre pour comprendre la nature d'un risque et pour déterminer le niveau de risque.
ANSSI	Autorité nationale en matière de sécurité des systèmes d'information classifiés et non classifiés installés et exploités par l'État et les opérateurs d'infrastructures critiques pour leurs besoins propres.
Confidentialité	Propriété selon laquelle l'information n'est pas rendue disponible ni divulguée à des personnes, des entités ou des processus non autorisés.
Conformité	Satisfaction d'une exigence.
Contrôle de sécurité	Mesure technique ou organisationnelle mise en œuvre par le STATEC pourdétecter, prévenir ou réduire le risque lié à une menace ou une vulnérabilité.
Disponibilité	Propriété d'être accessible et utilisable à la demande par une entité autorisée.
Entité	Département ministériel, administration ou service de l'État ainsi qu'opérateur d'infrastructure critique qui applique cette politique de sécurité. Synonyme du terme organisme dans ISO/IEC 27001 : Personne ou groupe de personnes qui a ses propres fonctions, avec les responsabilités, les pouvoirs et les relations nécessaires pour atteindre ses objectifs.
Exigence	Besoin ou attente formulé(e), habituellement implicite, ou imposé(e). Note 1 : « Habituellement implicite » signifie qu'il est d'usage ou de pratique courante pour l'organisme et les parties intéressées de considérer le besoin ou l'attente en question comme implicite.

	Note 2 : Une exigence spécifiée est une exigence qui est formulée, par exemple, dans des informations documentées.
Fiabilité	Propriété relative à un comportement et des résultats prévus et cohérents.
Gestion de la continuité d'activité	Processus de management holistique qui identifie les menaces potentielles pour une organisation ainsi que les impacts que ces menaces, si elles se concrétisent, peuvent avoir sur les opérations liées à l'activité de l'organisation, et qui fournit un cadre pour construire la résilience de l'organisation avec une capacité de réponse efficace préservant les intérêts de ses principales parties prenantes, sa réputation, sa marque et ses activités productrices de valeur.
Gestion des incidents liés à la sécurité de l'information	Processus pour détecter, rapporter, apprécier, intervenir, résoudre et tirer les enseignements des incidents liés à la sécurité de l'information.
Gestion des risques	Activités coordonnées dans le but de diriger et piloter une organisation en prenant en compte les risques.
Incident	1 : Situation qui peut être, ou conduire à, une perturbation, une perte, une urgence ou une crise. 2 : Événement indésirable ou inattendu d'origine externe au STATEC, relatif à la sécurité des informations et risquant de compromettre les activités opérationnelles ou de menacer la sécurité des informations (confidentialité, intégrité, disponibilité, traçabilité).
Intégrité	Propriété d'exactitude et de complétude.
Politique	Intentions et orientation d'un organisme telles que formalisées par sa direction.
Privacy by design	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 produit, au lieu de les ajouter ultérieurement sous forme de compléments.
Revue	Activité entreprise afin de déterminer l'adaptation, l'adéquation et l'efficacité de l'objet étudié pour atteindre les objectifs établis.
Sécurité de l'information	Protection de la confidentialité, de l'intégrité et de la disponibilité de l'information.
Système de management de la sécurité de l'information	Système de management visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer la sécurité de l'information d'un organisme afin que celui-ci atteigne ses objectifs métier. Note. Un SMSI se base sur l'appréciation du risque et sur les niveaux d'acceptation du risque définis par l'organisme pour traiter et gérer efficacement les risques.
Utilisateur	Désigne une personne ayant accès au système d'information du STATEC dans le cadre de sa mission, quel que soit son statut.

2 Objectifs de la sécurité de l'information

2.1 Parties prenantes

Afin de déterminer les objectifs de sécurité, il est important de comprendre les besoins et attentes des parties prenantes en matière de sécurité de l'information. Pour cette raison nous listons ci-dessous les principales parties prenantes ainsi que leurs attentes :

- Les citoyens et les entreprises luxembourgeoises : confidentialité des données utilisées pour la production de statistiques, fourniture régulière de statistiques de qualité, production de statistiques de manière transparente.
- Le Ministère de tutelle du STATEC, l'État luxembourgeois et ses administrations publiques: confidentialité des données administratives utilisées pour la production de statistiques, fourniture de statistiques de qualité.
- Les fournisseurs de données à la base de nombreuses statistiques dont nous pouvons noter les principaux :
  - les communes, syndicats de communes et établissements publics placés sous la surveillance des communes ;
  - les autorités de régulation et de surveillance telles que l'Institut Luxembourgeois de Régulation, la Commission de Surveillance du Secteur Financier ou le Commissariat aux Assurances ;
  - la banque centrale ;
  - les établissements publics en charge de la gestion de la sécurité sociale,

  exigent tous la confidentialité des données sous leur charge.
- Les entités du système statistique luxembourgeois : la production de statistiques de qualité.
- Eurostat : la fourniture de statistiques de qualité, le respect des délais impartis, la transparence dans la production de statistiques ainsi que et la conformité par rapport au framework ESS IT SEC.
- Les chercheurs : accès aux micro-données statistiques à des fins de recherche, collaboration dans le cadre d'études statistiques.

Les besoins et attentes des parties prenantes nous permettent de formuler les critères et objectifs de sécurité définis dans les prochains chapitres

2.2 Les critères de sécurité

La sécurité des systèmes d'information repose sur quatre critères :

- **confidentialité** (propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des processus non autorisés) : afin de garantir que seules les personnes autorisées ont accès aux éléments considérés (applications, fichiers...) ;
- **intégrité** (propriété d'exactitude et de complétude) : afin de garantir que les éléments considérés (données, messages...) sont exacts et complets et qu'ils n'ont pas été modifiés ;
- **disponibilité** (propriété d'être accessible et utilisable à la demande par une entité autorisée) : afin de garantir que les éléments considérés (fichiers, messages, applications et services) sont accessibles au moment voulu par les personnes autorisées ;

- **traçabilité** (capacité à suivre la vie d'une donnée à travers son déploiement, son accès et son utilisation) : afin de garantir que les accès et tentatives d'accès aux informations sont tracés et que ces traces sont conservées et exploitables en temps voulu.

Les besoins de sécurité s'appliquent aussi bien aux ressources du système d'information (stations de travail, équipements réseau, applications, etc.) qu'aux données traitées par ces ressources. Il est nécessaire d'inventorier et de classifier ces données afin d'en identifier le degré de sensibilité et donc le besoin de protection nécessaire.

2.3 Objectifs généraux

La sécurité de l'information est un facteur clé de succès pour les services fournis par le STATEC. La présente politique a été définie dans le but de soutenir cet objectif, mais également de le cadrer avec les autres objectifs stratégiques.

Les objectifs de sécurité peuvent s'exprimer comme suit :

- Préserver **la confidentialité** de toutes les données sensibles qui sont confiées au STATEC et en particulier les données définies en chapitre 2.3.1.
- Assurer **l'intégrité** des informations et des processus de gestion de l'information.
- Assurer **la disponibilité** adéquate des services.
- **Apprécier et traiter les risques** liés à la sécurité de l'information de telle façon à adopter des mesures de sécurité appropriées. La valeur de l'information peut être estimée au regard des conséquences négatives pour STATEC que causerait l'absence, la perte, le vol ou la corruption de ladite information.
- **Assurer la gestion de la sécurité** selon des méthodes effectives, efficaces, documentées et transparentes.
- **Assurer la mise en œuvre des principes de protection des données à caractère personnel** et **garantir l'exercice de la responsabilité (accountability**) pour les traitements effectués.

Le terme « information » inclut dans ce contexte aussi bien des données propres du STATEC que celles des personnes concernées.

2.3.1 Base légale pour la protection des informations

La loi modifiée du 10 juillet 2011 portant sur l'organisation de l'Institut national de la statistique et des études économiques « STATEC » [4] définit la notion de « donnée confidentielle » dans le cadre de ses activités :

Extrait de l'article N° 16 : *« Les données utilisées pour la production de statistiques sont considérées comme confidentielles lorsqu'elles permettent l'identification, directe ou indirecte, d'une personne physique ou morale ou comportent un risque de divulgation d'informations individuelles. Pour déterminer si une personne physique ou morale est identifiable, il est tenu compte de tous les moyens dont on pourrait raisonnablement admettre qu'ils puissent être utilisés par un tiers pour identifier ladite personne. Toutefois, les données qui sont tirées de sources accessibles au public et qui restent accessibles conformément à la législation ne sont pas considérées comme confidentielles. Il en est de même en cas d'autorisation expresse du redevable de l'information statistique. »*

Le règlement CE N°223/2009 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 11 mars 2009 relatif aux statistiques européennes [5] définit les notions de « secret statistique » et de « données confidentielles » :

Article 2.e : « secret statistique »: les données confidentielles relatives à des unités statistiques individuelles qui sont obtenues directement à des fins statistiques ou indirectement à partir de sources administratives ou autres doivent être protégées, et cela implique que l'utilisation à des fins non statistiques des données obtenues et la divulgation illicite de ces dernières soient interdites ;

Article 3.7 : « données confidentielles »: des données permettant l'identification, directe ou indirecte, d'unités statistiques, ce qui a pour effet de divulguer des informations individuelles. Pour déterminer si une unité statistique est identifiable, il est tenu compte de tous les moyens appropriés qui pourraient raisonnablement être utilisés par un tiers pour identifier l'unité statistique ;

Information à caractère personnel

Toutes les données à caractère personnel sont traitées conformément à la législation :

- un délégué à la protection des données (Data Protection Officer - DPO) est nommé afin de vérifier l'application des dispositions inscrites aux lois et règlements applicables en la matière ;
- l'accès aux données confidentielles et aux données à caractère personnel doit être accordé uniquement aux personnes dont les fonctions et les responsabilités requièrent l'accès à ces données ;
- les outils de surveillance mis en œuvre par le STATEC doivent être conformes aux lois et règlements applicables afin de garantir le respect de la protection des données personnelles ;
- afin de pouvoir assurer le respect de la vie privée, des règles sont établies permettant d'identifier les contenus à caractère personnel.

2.4 Les politiques par domaine

Dans le cadre de la définition du SMSI, les politiques par domaine indiquées dans « Tableau 1 : Politiques par domaine » sont élaborées et mises en application.

Ces documents seront en général identifiés à l'aide de deux nombres reliés, p. ex., 00-01, où le premier nombre est le numéro du domaine et la valeur 00 réfère à la politique générale. Le deuxième nombre est un nombre séquentiel des documents de ce domaine. Ces nombres commencent avec le nombre 00 qui désigne toujours un document de type « politique » qui définit les objectifs de sécurité. En suivant cette logique, ce document a la référence : POL_00-00. S'il existe un grand nombre de documents, ceux-ci peuvent être identifiés avec une lettre supplémentaire aux deux nombres reliés, p. ex. 01-07-C qui désigne l'annexe C au document 01-07.

Les numéros de 5 à 18 des domaines ont été choisis pour être alignés avec ISO/IEC 27002 et ainsi simplifier l'implémentation et le suivi par le personnel formé à l'usage des normes. Ces domaines initiaux peuvent être complétés en cas de besoin, comme c'est par exemple déjà le cas pour le domaine 02 liée à la protection des données.

2.4.1 Documents applicables

L'ensemble des documents lié à la politique de sécurité de l'information, y compris les politiques (POL), les plans (PLA), les procédures (PRO) et les standards (STA) qui en résultent, une fois mis en vigueur, ont le même caractère obligatoire.

Toutes les politiques (et autres documents du SMSI) en vigueur sont renseignées dans la liste des documents [1], et les documents qui s'adressent à tout le personnel sont mis à disposition sous https://www.statec.etat.lu/InfoSec.

Id.	Acronyme	Nom du domaine et de la politique	Commentaire
00-00	**ST-SécuInfo**	Politique de sécurité de l'information	Ce document
01-00	**ST-SMSI**	Système de gestion de la sécurité de l'information	Est l'outil de gouvernance complet de la sécurité de l'information traitée par le STATEC ; établit un SMSI conforme à ISO/IEC 27001 et avec les précisions requises par cette norme.
02-00	**ST-ProtDCP**	Politique de protection de données à caractère personnel	Transpose des exigences de la réglementation en matière de protection des données à caractère personnel.
05-00	**ST-GestRisq**	Gestion des risques	Définit les objectifs et exigences pour la gestion des risques liés à la sécurité de l'information.
06-00	**ST-OrgSécu**	Organisation de la sécurité	Décrit les rôles et responsabilités ainsi que les exigences sur les processus de gestion de la sécurité de l'information.
07-00	**ST-SécuRH**	Sécurité liée aux ressources humaines	Définit les objectifs et exigences liées aux ressources humaines.
08-00	**ST-GestActifs**	Gestion des actifs	Définit les objectifs et exigences pour la gestion des actifs, en particulier les informations et les systèmes d'information.
09-00	**ST-CtrlAccès**	Contrôle d'accès	Définit les objectifs et exigences du contrôle d'accès, p. ex. l'utilité de l'authentification forte.
10-00	**ST-Crypto**	Cryptographie	Définit les objectifs et exigences pour l'usage de la cryptographie.
11-00	**ST-SécuPhys**	Sécurité physique et environnementale	Définit les objectifs et exigences de sécurité physique et environnementale.
12-00	**ST-SécuExpl**	Sécurité de l'exploitation	Définit les objectifs et exigences sécurité de l'exploitation des systèmes d'information.
13-00	**ST-SécuComm**	Sécurité des communications	Définit les objectifs et exigences de la sécurité des réseaux de communications, p. ex. interne, réseau de l'État, messagerie électronique.
14-00	**ST-Systèmes**	Acquisition, développement et maintenance	Définit les objectifs et exigences pour l'acquisition, le développement et la maintenance des systèmes d'information.
15-00	**ST-RelFourn**	Relations avec les fournisseurs	Définit les objectifs et exigences pour la relation avec les fournisseurs.
16-00	**ST-GestInc**	Gestion des incidents liés à la sécurité de l'information	Définit les objectifs et exigences assurant une gestion adéquate des incidents liés à la sécurité.
17-00	**ST-Continuité**	Gestion de la continuité d'activité	Définit les objectifs et exigences pour assurer la continuité de l'activité même en cas d'incidents importants.
18-00	**ST-Conformité**	Conformité	Définit les objectifs et exigences pour assurer la conformité par rapport aux exigences légales, par rapport aux exigences contractuelles et par rapport à cette politique.

Tableau 1 : Politiques par domaine

3 Principes

Les présents principes sont repris de politique de sécurité de l'information de l'État [3] et adaptés au STATEC.

3.1 Une sécurité bien comprise

Les objectifs, mesures et consignes mis en place par le STATEC dans ce domaine sont connus de tous, grâce à la mise en œuvre d'un programme de sensibilisation de l'ensemble du personnel. Chaque agent du STATEC, en tant qu'utilisateur d'un système d'information, est informé de ses droits et devoirs et est régulièrement formé et sensibilisé à la sécurité de l'information et aux risques.

3.2 Le respect des normes, des contrats et des lois

En matière de gestion de la sécurité, le STATEC propose de suivre les normes internationalement reconnues et approuvées, et de les mettre correctement en application. La politique de sécurité de l'information et les documents connexes visent à respecter les normes ISO/IEC 27001 et 27002 et d'autres normes et référentiels applicables dont en particulier le framework ESS IT SEC.

Il va de soi que cette politique de sécurité soutient aussi le respect des exigences contractuelles et légales du STATEC, par exemple celles émanant de la loi sur la protection des données à caractère personnel.

3.3 Analyse et gestion du risque

Les mesures de sécurité sont sélectionnées en fonction d'une analyse du risque effectuée selon une méthode documentée, de façon à minimiser les risques inutiles et à maintenir les coûts de sécurité à un niveau acceptable. Le STATEC cherche à réduire les risques selon le principe de la proportionnalité et de la nécessité, mais il se réserve le droit d'assumer des risques résiduels. Toutefois, ces risques devront être dûment compris, documentés et acceptés par des personnes qualifiées et responsables.

3.4 Ressources

Les moyens humains et financiers consacrés à la sécurité de l'information de l'État sont planifiés, quantifiés et identifiés dans le cadre de l'exercice budgétaire annuel. Un budget approprié sera affecté à la sécurité de l'information.

En particulier le STATEC met en place les moyens humains nécessaires pour que les postes et responsabilités du RSSI et du comité de sécurité comme définis ci-dessous soient couverts.

3.4.1 Le Responsable de la Sécurité des Systèmes d'Information (RSSI)

Le rôle du RSSI est de définir, de mettre en œuvre et de contrôler le processus de sécurité du système d'information afin de veiller au respect de la confidentialité, de l'intégrité, la disponibilité et de la traçabilité des informations.

Le RSSI est rattaché hiérarchiquement à la Direction du STATEC.

Responsabilités

Le RSSI possède les responsabilités clés suivantes :

- il définit la politique de sécurité du système d'information en accord avec la Direction ;
- il communique la politique de sécurité et sensibilise l'ensemble des personnels aux risques et contraintes de sécurité ;
- il évalue la vulnérabilité du système d'information et met en œuvre les mesures de sécurité appropriées ;
- il effectue avec l'aide de sociétés externes des revues régulières du système de management de la sécurité de l'information (SMSI), reporte les non-conformités détectées à la direction et établit un plan d'action pour les corriger ;
- il prépare et coordonne les actions en cas de crise de sécurité de l'information ;
- il assure la veille technologique et réglementaire pertinente au SMSI ;
- assiste pour la prise en compte de la sécurité dans les projets.

3.4.2 Le Comité de Sécurité

Le Comité de Sécurité est composé des membres permanents suivants :

- le directeur adjoint qui préside le comité ;
- le responsable de la sécurité des systèmes d'information (RSSI) qui est l'animateur de ce comité ;
- le délégué à la protection des données (Data Protection Officer - DPO) ;
- le responsable informatique ;
- le responsable de la division des services généraux.

En fonction des circonstances et des besoins, des membres temporaires peuvent rejoindre le Comité de Sécurité.

Responsabilités et missions

Le Comité de Sécurité dispose de responsabilités stratégiques :

- il valide les objectifs de sécurité concernant les activités stratégiques ;
- Il assure la gestion des incidents majeurs ;
- il veille à ce que les choix en matière de sécurité ainsi que le niveau de sécurité mesuré soient en phase avec les objectifs stratégiques du STATEC ;
- il veille à la bonne application de ces mesures.

3.5 Un développement continu vers l'excellence

L'environnement de gestion des informations de l'État change continuellement. Voilà pourquoi il n'est pas suffisant d'assurer la sécurité de l'information aujourd'hui : il convient de mettre en place des procédures pour adapter et améliorer la sécurité de l'information pour la maintenir en phase avec les défis futurs.

3.6 Une sécurité intégrée et transversale

La sécurité de l'information n'est pas une discipline déconnectée, mais elle fait partie intégrante de toute activité du STATEC, de la conception à la maintenance en passant par la spécification, l'implémentation, le déploiement et la mise en service. Elle est la pierre angulaire de la gestion de tous les projets, de tous les processus et dans les activités quotidiennes.

Concernant l'intégration de la sécurité de l'information au niveau de la conception de systèmes traitant des données à caractère personnel, le principe « Privacy by design » est respecté.

3.7 Communication et travail d'équipe

Une équipe efficace et attentive a besoin d'être au courant du fonctionnement de la sécurité de l'information. Le personnel du STATEC est un vecteur très important dans la lutte contre les risques et s'aide mutuellement dans la réalisation des objectifs de sécurité.

3.7.1 Responsabilités des utilisateurs

Tout utilisateur du système d'information du STATEC, quel que soit son niveau, s'engage à s'informer des règles de sécurité en vigueur et à les respecter.

Chaque responsable du STATEC s'engage à faire respecter les règles de sécurité en vigueur auprès des membres de son équipe et du personnel externe intervenant sous sa responsabilité.

Tout utilisateur du système d'information a le devoir de signaler toute violation constatée des règles, politiques et contrôles de sécurité au RSSI.

Lors du départ d'un utilisateur du système d'information du STATEC en fin de contrat ou en fin de mission (employés, consultants, stagiaires, etc.), son responsable doit s'assurer :

- avec l'aide de l'unité informatique qui pourra fournir une liste, du retour des matériels physiques et électroniques mis à disposition de cet utilisateur ;
- du maintien des connaissances et des compétences au sein de son unité avant le départ de cet utilisateur ;
- de la récupération, avant son départ, des travaux et des données produits par l'utilisateur dans le cadre de sa mission au STATEC ;
- qu'aucune fuite d'information ne puisse être réalisée par un utilisateur du système d'information suspendu de ses fonctions, en effectuant une revue de ses accès, ceci avec l'aide de l'informatique et du RSSI qui mettront à disposition des outils dédiés ou des listes de contrôle.

3.8 Contrôle et sous-traitance

Pour l'assister à maîtriser les systèmes d'information et réduire des risques, le STATEC fait appel à des opérateurs et des prestataires de confiance.

3.9 Respect et traçabilité

La protection des systèmes d'information est assurée par l'application rigoureuse de règles précises définies dans le cadre de cette politique de sécurité de l'information.

Les membres du personnel ont une obligation éthique, morale et légale de protéger et de maintenir la confidentialité, l'intégrité et la disponibilité des informations. Exemples : Les agents ne peuvent abuser, essayer d'abuser ou aider d'autres à abuser des informations ou des systèmes d'information. Ils ne peuvent exposer ni divulguer de l'information à des personnes non autorisées.

Tout le personnel interne et externe connaît ces règles et l'importance de la sécurité de l'information et contribue activement à la réalisation des objectifs de la politique de sécurité de l'information. Ils respectent en toutes circonstances les objectifs et les règles de la présente politique de sécurité de l'information et des documents connexes.

Afin de s'assurer du bon fonctionnement du système de gestion de la sécurité et le respect des règles, les activités et décisions, concernant le management du SMSI, sont rigoureusement tracées.

3.10 Politique et culture de sécurité

La politique de sécurité de l'information établit un point de départ pour une gestion appropriée de la sécurité de l'information. Toutefois, afin de réduire de manière efficace les risques, le STATEC compte sur la coopération active de chaque membre du personnel en vue d'instaurer un environnement de travail sécurisé et d'apporter des améliorations à la présente politique de sécurité de l'information et aux documents y relatifs. Avec le temps, la sécurité de l'information ne sera plus garantie par le simple respect de consignes, mais surtout par des valeurs vécues et partagées par le personnel en vue de maîtriser les risques de leur activité. Les objectifs de la politique contribuent ainsi à créer une culture de sécurité.

4 Engagement de la direction

En signant cette politique, la direction du STATEC prend certains engagements afin d'atteindre ses objectifs de sécurité :

4.1 Adéquation

Les exigences et recommandations de cette politique et des documents reliés mises en application sont compatibles avec l'orientation stratégique du STATEC.

4.2 Intégration

Les exigences et recommandations de cette politique et des documents reliés sont intégrées ou sont à intégrer dans les processus métiers du STATEC.

4.3 Engagement quant aux ressources

Le STATEC est fortement engagé à prendre toutes les mesures économiquement justifiables pour assurer la sécurité du personnel, des données, des produits, des services, des locaux et des actifs. La direction met à disposition les ressources nécessaires pour analyser et combattre les risques dans l'intérêt des parties intéressées.

4.4 Formation et sensibilisation du personnel

La direction s'engage à former son personnel aux questions de sécurité et de risques, leur permettant ainsi de respecter en permanence la politique de sécurité. Plus précisément elle organise :

- une formation spécifique pour les nouveaux utilisateurs organisée par le RSSI ;
- une séance de sensibilisation organisée chaque année par le RSSI afin de rappeler des règles importantes de sécurité et afin de communiquer sur les nouveaux risques ;
- des communications par courrier électronique envoyées par le RSSI, lorsque de nouvelles menaces apparaissent ;
- des sessions de sensibilisation concernant la protection des données à caractère personnel réalisées par le délégué à la protection des données (DPO – Data Protection Officer).

4.5 Résultats escomptés

La direction s'assure que le SMSI est mis en application et produit le résultat escompté : à l'aide de revue régulière, elle s'assure que les objectifs sont atteints.

4.6 Délégation de responsabilités et responsabilité du personnel

La direction attribuera à l'aide du SMSI les responsabilités et autorités concernant les activités liées à la sécurité à différentes personnes du STATEC.

Ces rôles sont précisés dans la liste des rôles et responsabilités [6]. Certaines responsabilités sont attribuées à chaque employé. Les employés suivent strictement les exigences de sécurité. De plus, ils contribuent

activement à améliorer les méthodes de sécurité en signalant rapidement les événements de sécurité aux gestionnaires concernés.

5 Structure de la politique de sécurité de l'information

5.1 Structure des documents

Les documents du SMSI sont classés en cinq niveaux :

1. **Politiques de sécurité de l'information (POL)** : documents qui définissent les objectifs de la politique de sécurité de l'information et le caractère obligatoire des instructions dérivées. Cela inclut la politique générale initiale, la politique du SMSI (c'est-à-dire ce document) et les politiques spécifiques au domaine (politique organisationnelle, politique de gestion des risques, politique de classification des actifs, etc.).
2. **Plans (PLA)** : documents qui contient des indications tactiques sur quand et comment les objectifs seront atteints dans chaque domaine (domaine d'applicabilité, déclaration d'applicabilité de chaque entité, plans de traitement des risques, plans d'action pour atteindre les objectifs, liste des exceptions, résultats d'évaluation et traitement des risques, etc.).
3. **Procédures (PRO)** : documents qui décrivent les processus et les responsabilités des acteurs (processus de classification des biens, processus de gestion des données de sortie, processus d'installation du système informatique, etc.).
4. **Standards (STA)** : documents qui contiennent les instructions et les règles de sécurité (instructions de gestion, codes de conduite, règles de sécurité applicables aux informations classifiées, liste des outils cryptographiques acceptés, etc.).
5. **Enregistrements (ENR)** : tous autres éléments qui peuvent servir de preuve de la bonne exécution de la gestion de la sécurité de l'information (registre des visiteurs, journal des événements, etc.).

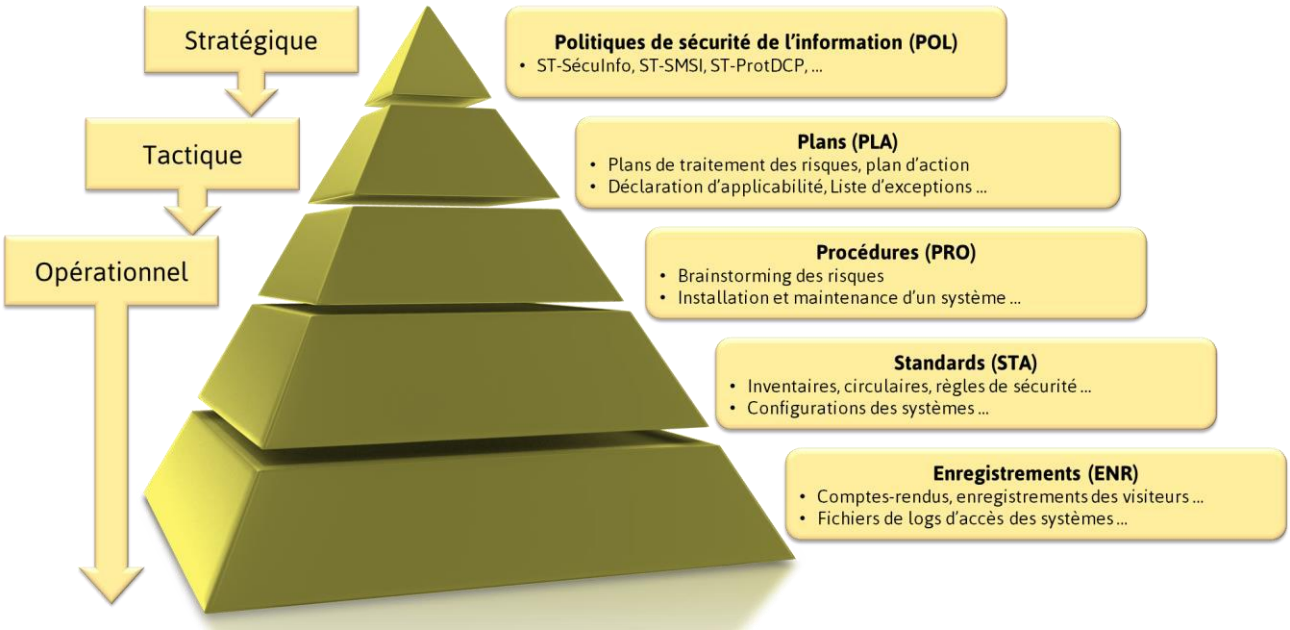

Figure 1 : Pyramide de structure des documents

5.2 Intranet

La version en vigueur de chaque document relatif au SMSI est mise à la disposition de tous les membres du personnel dans le répertoire interne [2].

5.3 Mise à jour

La politique de sécurité de l'information est amenée à évoluer dans le temps. Elle doit notamment être revue afin de prendre en compte :

- les évolutions des menaces et les retours d'expérience lors du traitement des incidents de sécurité ;
- les résultats d'analyses de risques ainsi que les actions découlant de contrôles ou d'inspections ;
- les évolutions des contextes organisationnels, juridiques, réglementaires et technologiques ;
- des contraintes et recommandations émises par l'Agence nationale de la sécurité des systèmes d'Information (ANSSI) ;
- des contraintes liées au fonctionnement du centre des technologies de l'information de l'État (CTIE) :
- Les évolutions du framework ESS IT SEC.

Tous les documents de la politique sont révisés annuellement et mis à jour si nécessaire, où toutes les suggestions d'amélioration d'un document sont prises en considération. Dans le cas de besoin de modifications organisationnelles ou d'événements de sécurité majeurs, les documents sont mis à jour immédiatement.

La revue et la mise à jour de cette politique sont du ressort du Responsable de Sécurité des Systèmes d'Information du STATEC (RSSI), qui en est le gestionnaire.

Le comité de sécurité s'assure que les évolutions de la politique de sécurité proposées par le RSSI soient alignées avec l'activité et la stratégie du STATEC. Il peut également proposer des amendements ou des évolutions. In fine, le comité de sécurité valide toutes les évolutions de la politique.

Annexe 1 : Information sur les normes sur le SMSI

La Politique de Sécurité de l'Information et les documents connexes ont été rédigés dans le but de s'aligner aux normes ISO/IEC 27001 et 27002. Ces normes proposent les bonnes pratiques internationales de gestion de la sécurité de l'information applicable à toute organisation, aussi bien aux administrations publiques, aux opérateurs d'infrastructures critiques et aux petites entreprises.

5.4 ISO/IEC 27001 – SMSI – Exigences

La norme ISO/IEC 27001 fournit des exigences pour l'établissement, la mise en œuvre, le fonctionnement, la surveillance, l'examen, la mise à jour et l'amélioration du Système de Management de la Sécurité de l'Information (SMSI). Elle incite ses utilisateurs à souligner l'importance de :

- la compréhension des exigences relatives à la sécurité de l'information d'une entité ainsi que la nécessité de mettre en place une politique et des objectifs en matière de sécurité de l'information ;
- la mise en œuvre et l'exploitation des mesures de gestion des risques liés à la sécurité de l'information d'une entité dans le contexte des risques globaux liés à l'activité de l'entité ;
- la surveillance et l'examen des performances et de l'efficacité du SMSI et
- l'amélioration continue du système sur la base de mesures objectives.

Elle spécifie également les exigences relatives à la mise en œuvre des mesures de sécurité adaptées aux besoins de chaque entité. Le SMSI est destiné à assurer le choix de mesures de sécurité adéquates et proportionnées qui protègent les actifs et donnent confiance aux parties intéressées.

5.5 ISO/IEC 27002 – Code de bonne pratique pour le management de la sécurité de l'information

La norme ISO/IEC 27002 présente une série de préconisations concrètes, abordant des aspects tant techniques qu'organisationnels.

La norme définit un code de bonne pratique destiné à être utilisé par les responsables chargés de mettre en place ou de maintenir un système de management de la sécurité de l'information. La sécurité de l'information est définie comme « la préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information ».

La norme intègre 114 objectifs de sécurité et se compose de 14 chapitres correspondant aux domaines principaux de la sécurité :

- Politiques de sécurité de l'information,
- Organisation de la sécurité de l'information,
- 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.

STATEC établit pour chacun de ces domaines un document annexé qui fait partie intégrante de la politique de sécurité et qui fixera les objectifs pour le domaine.

5.6 ESS IT Security Framework

L'objectif de l'« ESS IT Security Framework » est de définir un cadre commun applicable à tous les membres du système statistique européen afin d'augmenter la sécurité et la confiance mutuelle.

Le framework ainsi que les lignes directrices ont été développés afin de réaliser l'objectif de systèmes d'informations sécurisées et de gestion des risques effective en :

- Fournissant une liste stable de mesures de sécurité répondant aux besoins actuels et futurs de sécurité selon les menaces, besoins et technologies changeantes ;
- Créant une fondation pour le développement de méthodes d'évaluation et de procédure pour déterminer l'efficacité des mesures de sécurité ;
- Facilitant la communication et l'échange d'information sur la sécurité informatique entre les membres ESS.

« ESS IT Security Framework » se base sur la norme ISO27002 pour établir ses mesures de sécurité en reprenant les 14 chapitres et la majorité des contrôles. De plus, le framework définit pour chaque contrôle la liste des preuves d'audit à présenter.

Le périmètre du framework est limité à la gestion et à l'échange de micro donnés entre les différents pays membres.