



l'oxygène
à la source

N°060-26

POLITIQUE GENERALE DE SECURITE DES SYSTEMES D'INFORMATION DU SILA

Nombre de membres en exercice : 52
Présents : 27
Représentés : 3
Quorum : 27

**Délibérations
du Comité Syndical
Séance du 2 mars 2026**

L'an deux mille vingt-six, le deux mars à onze heures, le Comité du Syndicat Mixte du Lac d'Annecy, dûment convoqué en date du 17 février 2026, s'est réuni au siège du SILA, sous la présidence de Pierre BRUYERE. Mme Séverine MUGNIER est désignée en qualité de Secrétaire de séance.

ETAIENT PRESENTS

COMMUNAUTE D'AGGLOMERATION GRAND ANNECY

Mmes, MM. Michel BEAL, Pierre BRUYERE, François DEGENNE, Gérard GRANGER, Fabienne GREBERT, Adrien GUILMAIN, Michel HAUET, Georges HIERSO, Patrick LECONTE, Claire LEPAN, Christian MALAPLATE, Philippe MANDEREAU, Benjamin MARIAS, Christian MARTINOD, Christian ROPHILLE, Gilles VIVIAN

COMMUNAUTE DE COMMUNES DES SOURCES DU LAC D'ANNECY

Mmes, M. Marielle JUILIEN, Philippe PRUD'HOMME

COMMUNAUTE DE COMMUNES DES VALLEES DE THONES

MM. Pierre BARRUCAND, Sébastien BRIAND

COMMUNAUTE DE COMMUNES DU PAYS DE CRUSEILLES

M. Guy DEMOLIS

COMMUNAUTE DE COMMUNES FIER & USSES

Mme, MM. Roger DALLEVET, Yves GUILLOTTE, Séverine MUGNIER

COMMUNAUTE DE COMMUNES RUMILLY TERRE DE SAVOIE

MM. Roland LOMBARD, Yohann TRANCHANT

COMMUNAUTE DE COMMUNES USSES ET RHONE

M. Jean-Yves MÂCHARD

ETAIENT ABSENTS OU EXCUSES

Mmes, MM. Jean-Pascal ALBRAN, François ASTORG, Franck BOGEY, Sandrine DALL'AGLIO, Gilles FRANCOIS, Anthony GRANGER, Frédérique LARDET, Patricia MERMOZ, Olivier MOUZIN, Magali MUGNIER, Christophe PONCET, Marc ROLLIN, Didier SARDA, Sylvain STIHLE, Jacques DALEX, André PERRILLAT-AMEDE, Jean-Marc BOUCHET, Julie MONTCOUQUIOL, Serge FABBIAN, Colette BELLEMIN, Cédric VERNEY, Martine VIBERT, Emmanuel GEORGES, Didier GALMICHE, Christian VERMELLE

AVAIENT DONNE POUVOIR

Anthony GRANGER à Pierre BRUYERE
Marc ROLLIN à Michel BEAL
Patricia MERMOZ à Patrick LECONTE

PARTICIPAIENT EGALEMENT

Mmes & MM. Valérie GUICHARD, DGS, Pascale ABADIE, DGA Administration et ressources, Yovann LOIR, DGA Assainissement Traitement des déchets, Damien ZANELLA, DGA Environnement, Sonia PAPES, Directeur Financier, Pierre LOMBARD, Directeur des Systèmes d'Information et du Numérique, Camille MARGUIGNOT, Service Secrétariat général/Affaires juridiques.

POLITIQUE GENERALE DE SECURITE DES SYSTEMES D'INFORMATION DU SILA

Exposé du Président,

La politique générale de sécurité des systèmes d'information (PGSSI) a pour objectif de s'assurer que les systèmes d'information soient protégés contre les risques menaçant leur disponibilité, leur intégrité et leur confidentialité.

La PGSSI s'inscrit dans un cadre de normes et réglementation européennes et nationales liées aux systèmes d'information, ainsi que dans le cadre de la politique de sécurité du SILA, comprenant des mesures de sécurité « classiques » d'exploitation et des mesures de crise (plans de reprise et de continuité d'activité, plans de reprise et continuité informatique, plan de remédiation).

Cette politique se décline ainsi en deux parties :

1. Fixation du périmètre, objectif principal, principes et responsabilités nécessaires à la mise en œuvre de la PGSSI ; 12 principes généraux regroupés en 5 axes ;
2. Politique de sécurité des systèmes d'information (PSSI) : 262 exigences techniques ou organisationnelles, regroupées en règles et processus via 13 directives.

Les objectifs généraux de sécurité sont définis en cinq axes regroupant 12 principes de mise en œuvre :

- ✓ Axe 1 : Un système de management de la sécurité conforme aux meilleures pratiques
 - 1^{er} principe : documenter
- ✓ Axe 2 : Une gestion des risques régulière, efficace et proportionnée
 - 2^{ème} principe : gérer les risques
- ✓ Axe 3 : Des mesures de sécurité conformes aux meilleures pratiques
 - 3^{ème} principe : inventorier
 - 4^{ème} principe : sécuriser les utilisateurs et les usages
 - 5^{ème} principe : sécuriser les biens et les lieux
 - 6^{ème} principe : gérer les accès
 - 7^{ème} principe : déclarer les événements
 - 8^{ème} principe : prévoir la continuité
 - 9^{ème} principe : vérifier la conformité
- ✓ Axe 4 : Une exploitation et une évolution des SI conforme aux politiques de sécurité
 - 10^{ème} principe : maîtriser les environnements métiers
 - 11^{ème} principe : maîtriser l'environnement informatique
- ✓ Axe 5 : Une mise en œuvre progressive et pragmatique
 - 12^{ème} principe : mettre en œuvre

Le SILA est ainsi responsable, via les élus et la direction :

- D'adopter la PGSSI afin de définir les objectifs généraux et les principes de mise en œuvre de la protection des informations, en particulier les données personnelles, afin de garantir leur disponibilité, leur intégrité et leur confidentialité ;
- D'adopter, via une directive spécifique, les principes de gestion des risques ainsi que les critères d'évaluation et d'acceptation des risques ;
- D'accepter formellement les risques transversaux résiduels identifiés ;
- De mandater régulièrement des audits de sécurité ;
- D'adopter les propositions d'amélioration de la sécurité.

La politique de sécurité des systèmes d'information (PSSI) a pour objectif de fournir un ensemble de règles et d'exigences à mettre en œuvre au sein du SILA. Les 13 directives de la PSSI sont les suivantes :

- ✓ Politique et organisation de la sécurité de l'information
- ✓ Connaissance du système d'information et gestion des actifs
- ✓ Sécurité des ressources humaines
- ✓ Relation client/fournisseur
- ✓ La sécurité dans les projets
- ✓ Planification de la continuité d'activité informatique
- ✓ Conformité et audits
- ✓ Sécurité physique et environnementale
- ✓ Gestion des accès et cryptographie
- ✓ Sécurité opérationnelle
- ✓ Sécurité des communications
- ✓ Gestion des incidents de sécurité
- ✓ Sécurité des systèmes industriels

Les membres du Comité sont en conséquence invités à adopter la politique générale de sécurité des systèmes d'information du SILA.

- ADOPTÉ -
à l'unanimité

Voix POUR : 30
Voix CONTRE : 0
Abstentions : 0
Non votants : 0

Par délégation,
Pascale ABADIE,
DGA Administration et ressources

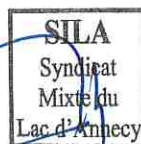


Mme Séverine MUGNIER,
Secrétaire de séance



Acte reçu à la Préfecture
Le 15 MARS 2026
Publié le 18 MARS 2026
18 MARS 2026

Exécutoire le
Le Président,
Pierre BRUYERE



La présente délibération peut faire l'objet d'un recours gracieux devant Monsieur le Président du SILA dans le délai de 2 mois à compter de sa publication ou de sa notification.

Un recours contentieux peut également être introduit devant le tribunal administratif de Grenoble par voie postale (2 place Verdun BP 1135 – 38022 GRENOBLE Cedex) ou par voie électronique (Télérecours citoyens, www.telerecours.fr) dans le délai de deux mois à compter de la notification de la délibération ou de sa date de publication ou à compter de la réponse du SILA, si un recours gracieux a été préalablement déposé.



**l'oxygène
à la source**

Politique Générale de Sécurité des Systèmes d'Information du SILA **(PGSSI)**

Politique de sécurité des systèmes d'information
(PSSI)



TABLE DES MATIERES

TABLE DES MATIERES	- 2 -
---------------------------------	--------------

GLOSSAIRE ET DEFINITIONS	- 5 -
---------------------------------------	--------------

INTRODUCTION	- 11 -
---------------------------	---------------

Objet et objectif du document.....	- 11 -
Domaine d'application	- 12 -
Périmètre et parties prenantes.....	- 12 -
Champ d'application	- 12 -
Références légales et normatives	- 12 -
Entrée en vigueur	- 12 -

POLITIQUE GENERALE DE SECURITE DES SYSTEMES D'INFORMATION.....	- 13 -
---	---------------

OBJECTIF GÉNÉRAL.....	- 13 -
Un contexte qui appelle à davantage de sécurité	- 13 -
Sécuriser selon quatre critères fondamentaux.....	- 13 -
AXES ET PRINCIPES DE MISE EN ŒUVRE	- 13 -
Axe 1. Un système de management de la sécurité conforme aux meilleures pratiques	- 14 -
1er principe : documenter	- 14 -
Axe 2. Une gestion des risques régulière, efficace et proportionnée.....	- 14 -
2 ^{ème} principe : gérer les risques.....	- 14 -
Axe 3. Des mesures de sécurité conformes aux meilleures pratiques	- 15 -
3 ^{ème} principe : inventorier	- 15 -
4 ^{ème} principe : sécuriser les utilisateurs et les usages.....	- 15 -
5 ^{ème} principe : sécuriser les biens et les lieux	- 15 -
6 ^{ème} principe : gérer les accès	- 15 -
7 ^{ème} principe : déclarer les évènements	- 15 -
8 ^{ème} principe : prévoir la continuité	- 15 -
9 ^{ème} principe : vérifier la conformité.....	- 15 -
Axe 4. Une exploitation et une évolution des SI conforme aux politiques de sécurité	- 15 -
10 ^{ème} principe : maîtriser les environnements métiers	- 15 -
11 ^{ème} principe : maitriser l'environnement informatique	- 15 -
Axe 5. Une mise en œuvre progressive et pragmatique.....	- 16 -
12 ^{ème} principe : mettre en œuvre	- 16 -
RESPONSABILITÉS.....	- 16 -

Le SILA	- 16 -
Le RSSI	- 16 -
Le DSI.....	- 16 -
Les Directions métiers.....	- 17 -
La DSIN	- 17 -
Les agents de la DSIN	- 17 -
Les intervenants techniques externes à la DSIN	- 18 -
Les utilisateurs du SI du SILA.....	- 18 -

POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION - 19 -

OBJET.....	- 19 -
EVOLUTION DE LA PSSI	- 19 -
PRINCIPES DES REGLES ET EXIGENCES EDICTEES DANS LA PRESENTE PSSI	- 19 -
1 - Politique et Organisation de la sécurité de l'information (PSI et ORG) / (ISO 5 et 6).....	- 20 -
1.1. Politique de sécurité des Systèmes d'information	- 20 -
1.2. Organisation interne	- 21 -
2 - Connaissance du SI et gestion des actifs (CSI) / (ISO 8)	- 22 -
2.1 Identification des objectifs de sécurité.....	- 22 -
2.2 Classification de l'information	- 23 -
2.3 Cartographie et gestion des actifs	- 25 -
3 - Sécurité des Ressources Humaines (RH) / (ISO 7)	- 26 -
3.1. Avant l'embauche ou la contractualisation	- 26 -
3.2. Pendant la durée du contrat.....	- 27 -
3.3. Rupture, terme ou modification du contrat	- 27 -
4 - Relation client/fournisseur (EXT) / (ISO 15).....	- 28 -
5 - La sécurité dans les projets (ISP) / (ISO 14)	- 29 -
6 - Planification de la continuité d'activité informatique (PCI) / (ISO 17).....	- 31 -
7 - Conformité et audits (AUD et CONF) / (ISO 18).....	- 31 -
7.1. Conformité aux exigences légales et contractuelles.....	- 31 -
7.2. Revues de sécurité de l'information	- 32 -
8 - Sécurité physique et environnementale (PHY) / (ISO 11).....	- 32 -
8.1. Zones sécurisées	- 33 -
8.2. Sécurité des équipements et des salles techniques	- 33 -
8.3. Sécurité du matériel utilisateur	- 34 -
8.4. Gestion des visiteurs	- 35 -
9 - Gestion des accès et cryptographie (ACC et CRY) / (ISO 9 et 10)	- 35 -
9.1. Gestion des accès et responsabilités utilisateurs	- 35 -
9.2. Accès à privilèges	- 37 -



9.3.	Accès à distance et aux solutions Cloud	- 38 -
9.4.	Cryptographie – chiffrement.....	- 38 -
10	- Sécurité opérationnelle (EXP) / (ISO 12)	- 39 -
10.1.	Procédures et responsabilités opérationnelles	- 39 -
10.2.	Protection des équipements.....	- 41 -
10.3.	Protection des équipements mobiles	- 43 -
10.4.	Sauvegarde et restauration.....	- 43 -
10.5.	Journalisation et supervision	- 44 -
11	- Sécurité des communications (RES) / (ISO 13)	- 45 -
11.1.	Sécurité réseau.....	- 45 -
11.2.	Transfert et partage d'information.....	- 47 -
11.3.	Opérations de télémaintenance	- 47 -
12	- Gestion des incidents de sécurité (INC) / (ISO 16).....	- 48 -
13	- Sécurité des systèmes industriels (IND).....	- 49 -
ANNEXES		- 51 -
1.1.	ORGANIGRAMME GENERAL DES SERVICES DU SILA (01/2026).....	- 51 -
1.2.	ORGANIGRAMME DE LA DSIN (01/2026).....	- 52 -
2.	CADRE LEGAL REGLEMENTAIRE ET NORMATIF	- 52 -

GLOSSAIRE ET DEFINITIONS

Sont ici définis et décrits les mots, concepts, notions, acteurs et acronymes liés à la sécurité informatique mise ou à mettre en œuvre au SILA. Ces définitions correspondent à l'état de l'art et à l'organisation du SILA au moment de la rédaction de ce document et ne sont pas nécessairement transposables en l'état à d'autres documents.

Les mots soulignés dans une définition ont leur propre définition dans le présent glossaire.

Actif : notion utilisée dans le présent document pour décrire tout élément unitaire du SI (système d'information) : poste informatique (portable, fixe, station de travail, poste renforcé), téléphone fixe ou mobile, disque dur (fixe ou amovible), écran, clavier, souris, éléments de l'infrastructure (câble, switch, borne wifi, répéteur, commutateur, autocom, serveur physique, serveur virtuel), ainsi que les logiciels, les bases de données, et l'ensemble des données qu'ils contiennent (données brutes, données d'exploitation, documentation).

AD (Active Directory) ; en français « répertoire actif » plus couramment traduit par « annuaire centralisé » ; service d'annuaire qui stocke des informations sur les objets d'un réseau et met ces informations à la disposition des utilisateurs et des administrateurs.

Administrateur technique : personne en charge de l'exploitation technique et du maintien en conditions opérationnelles d'un logiciel ou d'un matériel informatique. Dans la majorité des cas c'est un agent de la DSIN. L'administrateur technique peut avoir été le chef de projet technique lors du déploiement du logiciel ou du matériel.

Administrateur fonctionnel : personne en charge de l'exploitation fonctionnelle d'un logiciel ou d'un matériel informatique au sein de la Direction métier utilisatrice de l'outil. Il est généralement identifié comme référent sur cet outil et/ou propriétaire de l'actif. L'administrateur fonctionnel peut également avoir été le chef de projet fonctionnel lors du déploiement du logiciel ou du matériel.

Agents : il s'agit ici des agents territoriaux employés par le SILA.

AIPD (Analyse d'impact relative à la protection des données) : outil qui permet de construire un traitement conforme au RGPD et respectueux de la vie privée. L'AIPD concerne les traitements de données personnelles qui sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

Analyse de risque : Processus visant à identifier les risques, déterminer leur impact et leur probabilité d'occurrence afin de définir les mesures de sécurité permettant de les prioriser et de les traiter.

ANSSI (Agence nationale pour la sécurité de systèmes d'information) : Autorité nationale en matière de cybersécurité et de cyberdéfense en France, l'ANSSI a cinq grandes missions : défendre, connaître, partager, accompagner, réguler. La raison d'être de l'ANSSI est de construire et d'organiser la protection de la Nation face aux cyberattaques, et de contribuer à la stabilité du cyberspace. Son action s'inscrit dans le cadre des missions régaliennes de l'Etat, au service d'un objectif général de politique publique de sécurité et de résilience des administrations, de l'économie et de la société dans son ensemble.

Audit : Opération visant à analyser les actions effectuées sur des données ou des actifs ou à mesurer l'écart par rapport à un référentiel (par exemple la PSSI) ou à l'état de l'art.

Besoin d'en utiliser : désigne le fait de n'avoir accès qu'aux moyens de traitements de l'information (matériel informatique, applications, procédures, salles) dont on a besoin pour accomplir sa mission.

Besoin d'en connaître : désigne le fait de n'avoir accès qu'à l'information dont on a besoin pour réaliser ses tâches.

Chef de projet technique : personne en charge du déploiement technique d'un logiciel ou d'un matériel informatique. Dans la majorité des cas c'est un agent de la DSIN. Il œuvre généralement en binôme avec un chef de projet fonctionnel, issu de la Direction métier.

Chef de projet fonctionnel : personne en charge du déploiement fonctionnel d'un logiciel ou d'un matériel informatique. Dans la majorité des cas c'est un agent de la Direction métier utilisatrice de l'outil. Il œuvre généralement en binôme avec un chef de projet technique, issu de la DSIN.

Cloisonnement : Principe consistant à confiner des actifs du SI dans des zones de sécurité spécifiques (ou « zones réseau ») et à contrôler les communications entre les actifs situés sur des zones de sécurité distinctes.

Cloud computing ou « Cloud » ; *en français (informatique en nuage)* : ensemble de services informatiques (logiciels, stockage de données, serveurs) fournis via un réseau privé ou par Internet ; plusieurs niveaux de cloud existent (SaaS, IaaS, PaaS) ; par simplification on opposera le « cloud » aux solutions « on premise », c'est-à-dire installées sur l'infrastructure informatique dont le SILA est propriétaire et en son sein.

CNIL (Commission Nationale de l'Informatique et des Libertés) : instance nationale chargée de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papiers, aussi bien publics que privés. Elle a un rôle d'alerte, de conseil et d'information vers tous les publics mais dispose également d'un pouvoir de contrôle et de sanction.

Collectivité : il s'agit ici du SILA ; au pluriel (« les collectivités ») le terme désignera n'importe quelle strate de collectivité territoriale (commune, EPCI, Département, Région, etc.)

Confidentialité : critère de sécurité permettant de s'assurer que l'information n'est accessible qu'aux personnes autorisées.

Contrôle d'accès : Fonctionnalité de sécurité visant à autoriser l'accès à un bien (bâtiment, salle, local) ou un actif en fonction de l'utilisateur et des preuves d'identité fournies (badges, mot de passe, etc.) ainsi qu'en fonction des droits d'accès associés.

DG (Direction générale des services) : entité qui rassemble le poste de Directeur général des services (DGS) et les postes de Directeurs généraux adjoints (DGA), soit 4 postes à date au SILA. (Voir organigramme en annexe 1).

Direction métier : correspond dans ce document à toute Direction autre que la DG ou la DSIN. Il peut s'agir d'une Direction opérationnelle qui met en œuvre les compétences du SILA (assainissement, valorisation des déchets, environnement), comme d'une Direction ressources assurant le bon fonctionnement de la collectivité (finances, commande publique, RH, communication, etc)

Disponibilité : critère de sécurité ; aptitude d'une fonction à rendre le service attendu en temps voulu et dans les conditions d'usage prévues.

Droits d'accès : ensemble de droits accordés à un utilisateur sur une ressource, permettant d'effectuer des actions sur celle-ci (création, consultation, modification, suppression).

DSI (Directeur des systèmes d'information) : agent en charge de la DSIN et des activités liées ; il est en outre garant de la rédaction du présent document et de son application par toutes les parties prenantes. Par souci de clarté, nous distinguerons dans le présent document le DSI (poste et agent) de la DSIN (la Direction).

DSIN (Direction des systèmes d'information et du numérique) : Direction du SILA rattachée à la DG, la DSIN gère l'ensemble des infrastructures informatiques système et réseaux du SILA, gère le maintien en conditions opérationnelles des logiciels et solutions métiers qu'elle déploie ; en charge des orientations informatiques et numérique de la collectivité elle assure le volet cybersécurité ainsi que la gouvernance des données qu'elle met en œuvre. Enfin, elle accompagne les agents dans l'utilisation courante des outils en vue d'en améliorer les usages. Par souci de clarté, nous distinguerons dans le présent document le DSI (poste et agent) de la DSIN (la Direction).

EDR (Endpoint detective response) ; *en français « détection et réponse des terminaux »* : solution de sécurité permettant de détecter et de remédier aux cybermenaces ciblant les terminaux (ordinateurs, serveurs, etc).

Fournisseurs : entités ou organismes externes en relation contractuelle avec le SILA. Le fournisseur travaille à la demande et sous le contrôle du SILA.

GED (Gestion électronique des documents) : outil informatique de gestion et d'organisation des documents électroniques ; à défaut d'une GED centralisée, le SILA dispose de certaines GED métiers adossées à certaines solutions : il peut s'agir d'une partie de la base de données du logiciel, ou d'un répertoire sur les serveurs de fichiers de la collectivité ; dans le cadre de ce document, un répertoire de serveur de fichier conçu exclusivement à des fins de stockage de documentations spécifiques sera considéré comme GED.

Gestionnaire des données : dans le cadre du RGPD, il s'agit de l'agent en charge d'un traitement de données liés à son activité et dont il a la responsabilité en termes de conformité, confidentialité, sécurité et mise à jour.

Incident : tout événement qui ne fait pas partie du fonctionnement standard d'un service et qui cause, ou peut causer, une interruption ou une diminution de la qualité de ce service.

IA (Intelligence artificielle) : processus d'imitation de l'intelligence humaine qui repose sur la création et l'application d'algorithmes exécutés dans un environnement informatique dynamique.

IaaS (infrastructure as a service) ; *en français « interface en tant que service »* : ressources d'infrastructures (réseaux, serveurs, virtualisation et stockage) gérées dans le cloud par le fournisseur ; l'utilisateur est responsable du système d'exploitation, des machines virtuelles et de toutes les applications ou données qu'il pourra installer et gérer.

Incidents de sécurité : tout événement affectant ou pouvant affecter la disponibilité, l'intégrité, la confidentialité ou la traçabilité des SI du SILA.

Intégrité : critère de sécurité ; garantie de l'exactitude, de la fiabilité et de l'exhaustivité des informations et des méthodes de traitement.

IT (Information technology) : en français « technologie de l'information » : décrit au sens large l'informatique, mais permet de distinguer l'informatique bureautique de l'informatique industrielle (OT)

MCO (Maintien en conditions opérationnelles) : regroupe l'ensemble des opérations nécessaires pour garantir la disponibilité constante du SI.

MCS (Maintien en conditions de sécurité) : consiste à surveiller, analyser et améliorer en permanence la sécurité du SI à travers plusieurs points : la surveillance proactive des systèmes et réseaux, l'identification des vulnérabilités et menaces potentielles, la mise en place de correctifs et l'adaptation continue des stratégies de cybersécurité.

MDM (Mobile device management) ; en français « gestion de la flotte mobile » : solution logicielle permettant de gérer, sécuriser et surveiller à distance les appareils mobiles tels que les smartphones, tablettes et ordinateurs portables utilisés par les agents de la collectivité.

Métier : appellation désignant un domaine d'activité du SILA correspondant à des compétences, des connaissances et un savoir-faire homogène.

NIS 2 (Network Information Security) ; en français « sécurité des réseaux et des systèmes d'Information » : directive européenne relative à la sécurité des systèmes d'information industriel (OT). Elle définit un certain nombre de règles et obligations relatives à la sécurité informatique de l'OT, selon que l'entité concernée soit classée EE (entité essentielle) ou EI (entité importante). Le SILA est classé EI. A date, la directive n'est pas complètement retranscrite dans le droit français (notamment pour les délais de mise en œuvre requis, qui s'ils sont dépassés donneront lieu à des amendes de non-conformité). Aussi le présent document ne peut contenir l'ensemble des exigences de sécurité attendues au regard de cette norme.

OT (operating technology) ; en français « technologie opérationnelle » on parle aussi d'« informatique industrielle » de « systèmes industriels » ou de « systèmes d'information industriels » : consiste en l'utilisation du matériel et des logiciels pour contrôler l'équipement industriel. Au SILA il s'agit de l'informatique adossée au réseau d'assainissement, usines de dépollution des eaux, et usine de valorisation des déchets (bien que cette dernière soit hors du cadre de la présente PGSSI). Le terme OT est utilisé en complément ou opposition au terme d'II qui concerne l'informatique bureautique.

On premise ; en français « sur site » : se dit de tout actif installé, administré et exploité sur l'infrastructure informatique dont le SILA est propriétaire et en son sein (en opposition à toutes les formes de « cloud »)

PaaS (Platform as a service) ; en français « plateforme en tant que service » : ressources d'infrastructures matérielles et logicielles gérées dans le cloud par le fournisseur ; l'utilisateur peut développer, exécuter et gérer ses applications sans avoir à gérer l'infrastructure, les mises à jour logicielles ou la maintenance du matériel.

PCA (plan de continuité des activités) : plan qui décrit et organise les mesures à prendre pour maintenir et poursuivre les activités de la collectivité, même de manière dégradée, face à une crise majeure (catastrophe naturelle, accident industriel, pandémie...). Ce plan intègre toutes les ressources de la collectivité : ressources humaines, SI et moyen de communication, infrastructures,

partenaires, etc. Au SILA, et de manière générale dans les collectivités, c'est la DG qui est en charge de la rédaction et du pilotage, en cas de crise, du PCA.

PRA (plan de reprise des activités) : plan qui décrit et organise les mesures de reprise de l'activité suite à un arrêt partiel ou total, en conséquence d'une crise majeure (catastrophe naturelle, accident industriel, pandémie...). Au SILA, et de manière générale dans les collectivités, c'est la DG qui est en charge de la rédaction et du pilotage, en cas de crise, du PRA.

PCI (plan de continuité informatique) : plan qui décrit et organise les mesures à prendre pour maintenir et poursuivre les activités informatiques et numériques de la collectivité, même de manière dégradée, face aux conséquences d'une crise majeure (catastrophe naturelle, accident industriel, pandémie...) sur le SI. Au SILA, c'est la DSIN qui est en charge de la rédaction et du pilotage du PCI, en lien avec la DG (en charge du PCA).

PRI (plan de reprise informatique) : plan qui décrit et organise les mesures de reprise des activités informatiques et numériques suite à un arrêt partiel ou total de tout ou partie du SI, en conséquence d'une crise majeure (catastrophe naturelle, accident industriel, pandémie...). Au SILA, c'est la DSIN qui est en charge de la rédaction et du pilotage du PRI, en lien avec la DG (en charge du PRA).

Propriétaire de l'actif : définit dans ce document la personne ou l'entité responsable d'un actif du SI ; au sens donné dans le présent document ; par propriétaire de l'actif on entend « responsable » ou « référent » (il n'est pas question de propriété légale ou intellectuelle liée au matériel ou logiciel).

RGPD (règlement général de la protection des données) : texte réglementaire encadrant le traitement des données personnelles sur le territoire de l'Union européenne. Ce règlement européen s'inscrit dans la continuité de la Loi française Informatique et Libertés de 1978 et renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données les concernant.

RSSI (Responsable de la sécurité des systèmes d'information) : agent intervenant directement sur tout ou une partie du SI, il assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte sur la sécurité informatique et numérique du SILA. Le RSSI se trouve normalement rattaché à la Direction générale ou dans une Direction en charge des audits, du contrôle de gestion, ou du juridique, pour mieux exercer sa mission ; au SILA, au regard de la taille de la collectivité, il est de manière pragmatique rattaché directement au DSI (*organigramme de la DSIN en annexe 1.2*)

Responsable de traitement : dans le cadre du RGPD, il s'agit de la personne morale (entreprise, collectivité, etc.) ou physique qui détermine les finalités et les moyens d'un traitement, c'est à dire l'objectif et la façon de le réaliser. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal.

Restauration : Copie de données préalablement sauvegardées pour retrouver leur disponibilité suite à évènement accidentel (défaillance matérielle, humaine, accident, ...).

Risque : Scénario de réalisation d'une menace à travers une ou plusieurs vulnérabilités sur un ou plusieurs actifs engendrant des conséquences.

SaaS (software as a service) ; en français « logiciel en tant que service » : fourniture d'une ou de plusieurs applications complètes dans le cloud ; Les mises à jour logicielles, l'application des correctifs et les autres tâches de maintenance sont gérées par le fournisseur pour le compte de l'utilisateur. Aucun logiciel n'est installé sur les machines de la collectivité.

SAPM (Share account password management) ; en français « système de gestion des mots de passe » : solution centralisant l'ensemble des identifiants et mots de passe d'un utilisateur dans une

base de données ; le gestionnaire de mots de passe est protégé par un mot de passe unique, afin de n'en avoir plus qu'un seul à retenir.

Sauvegarde : Copie périodique des données d'un système sur un support pouvant être mis hors ligne et stocké hors du site de production, afin de permettre la récupération des données après incident ou sinistre.

SAE (Système d'archivage électronique) : solution logicielle conçue pour archiver les documents et les données électroniques telles que défini dans le Code du Patrimoine, Livre II. Il permet de collecter, traiter, organiser, stocker, gérer, conserver de manière pérenne des documents et données électroniques collectées, assurant ainsi un archivage à valeur probatoire.

SOC (Security Operation Center) ; en français « centre d'opérations de sécurité » : plateforme permettant la supervision et l'administration de la sécurité du système d'information au travers d'outils de collecte, de corrélation d'événements et d'intervention à distance.

SSI (Sécurité des systèmes d'information) : protection du SI contre les accidents (pannes, pertes, événements naturels ou physique, etc.), les erreurs (d'utilisation, de conception ou de fuite d'information) et les actes malveillants (piratage, falsification, fraude, vol, écoute, sabotage, ingénierie sociale, etc.) au moyen de mesures préventives et correctives, ainsi que de procédures de contrôle organisationnelles ou techniques appropriées.

SI (Système d'information) : ensemble organisé de ressources (données, personnel, procédures, matériels, logiciels...) permettant d'acquérir, traiter, stocker, diffuser ou détruire les informations utilisées par les entités du SILA dans le cadre de leurs activités et de leurs missions de service public, et ceci quel que soit le support de ces informations (numérique, papier, oral...). Ce système est partagé par l'ensemble des utilisateurs, mais il demeure la propriété de la collectivité.

SSO (Single sign-on) ; en français « authentification unique » ; service d'authentification de session et d'utilisateur qui permet à un utilisateur d'utiliser un ensemble d'informations d'identification (par exemple, identifiant et mot de passe) pour accéder à plusieurs applications.

Transformation numérique : adaptation des processus et des modèles de travail en intégrant les technologies informatiques et numériques. La transformation numérique contribue et répond à la transition numérique

Transition numérique : mutation sociétale engendrée par l'essor des nouvelles technologies et d'Internet.

Tiers : Entités ou organismes externes en relation contractuelle avec le SILA. Sont ainsi considérés comme des tiers : les fournisseurs, les intérimaires, les partenaires...

Traçabilité : Un des critères de sécurité ; ce critère traduit la garantie que les événements et les accès sont enregistrés à travers des traces accessibles et, si besoin, opposables.

Trace : Elle permet de suivre les traitements réalisés sur les informations au sein des processus et de mener des analyses a posteriori.

Utilisateur : Désigne toute personne susceptible de pouvoir accéder au SI du SILA. Sauf mention contraire, désigne également les administrateurs, les exploitants et les tiers intervenant sur les SI.

INTRODUCTION

Objet et objectif du document

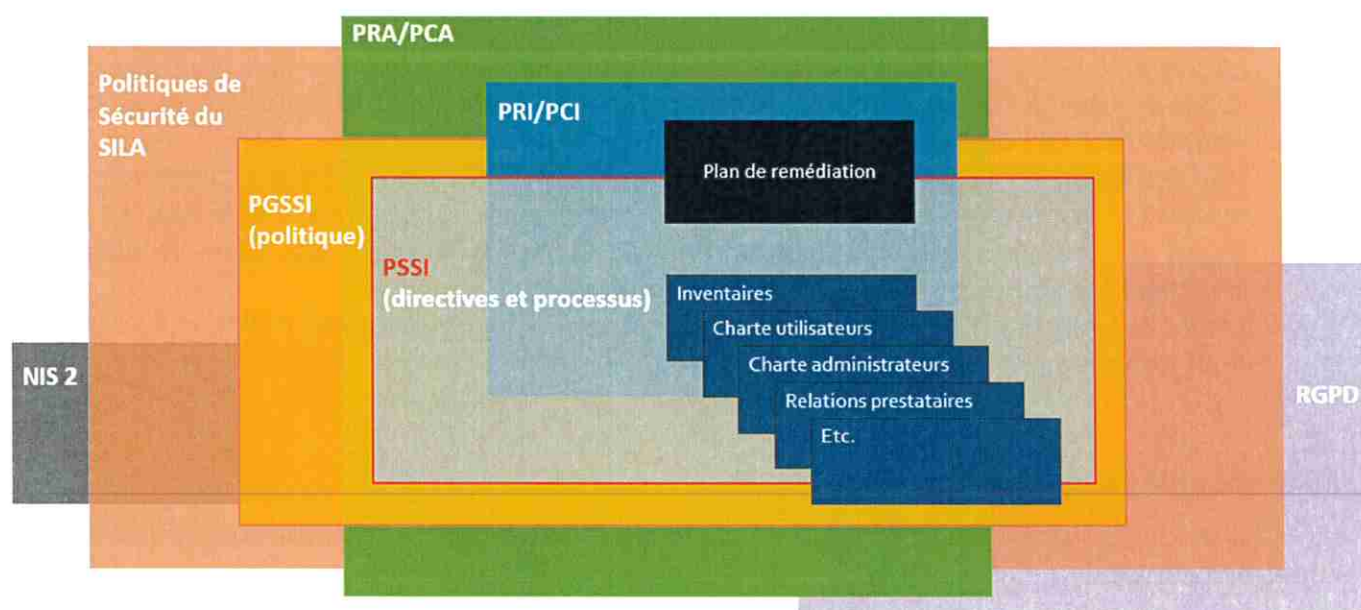
Ce document définit la politique générale de sécurité des systèmes d'information (PGSSI) que le SILA entend mettre en œuvre pour s'assurer que les systèmes d'information (SI) soient protégés contre les risques qui menacent leur disponibilité, leur intégrité et leur confidentialité.

Ce document se décline en deux parties :

- La première fixe le périmètre, l'objectif principal, les principes ainsi que les responsabilités nécessaires à la mise en œuvre de la PGSSI. Elle se décompose en 12 principes généraux regroupés en 5 axes.
- La seconde contient la politique de sécurité des systèmes d'information (PSSI) soit près de 262 exigences techniques ou organisationnelles, regroupées en règles et processus au travers de 13 directives,

Cette PGSSI s'inscrit dans un cadre de normes et réglementations européennes et nationales liées aux systèmes d'information, ainsi que dans le cadre de la politique de sécurité du SILA, comprenant des mesures de sécurité « classiques » d'exploitation et des mesures de crise telles que les plans de reprise et de continuité d'activité (PRA/PCA) et les plans de reprise et continuité informatique (PRI/PCI) et plan de remédiation.

Le schéma ci-dessous synthétise la hiérarchie des normes et leur « superposition » avec les politiques générales du SILA et celles dédiées à la sécurité informatique.



Domaine d'application

Périmètre et parties prenantes

La PGSSI s'applique :

- à toutes les entités du SILA ;
- à toute autre entité partenaire, par convention ou contrat la liant au SILA, selon des modalités qui préciseront la prise en compte totale ou partielle de la présente PGSSI (y compris l'unité de valorisation énergétique de SINERGIE de Chavanod, propriété du SILA sous gestion d'un prestataire dans le cadre d'un contrat d'exploitation, soumise à convention).

Cette PGSSI s'applique sur l'entièreté du système d'information (SI) du SILA, c'est-à-dire sur sa partie bureautique (IT) comme sur sa partie industrielle (OT).

Au regard du périmètre concerné, la PGSSI s'applique à tous les agents du SILA, aux élus, aux stagiaires, apprentis, ainsi qu'aux prestataires, fournisseurs et intervenants du SILA.

Champ d'application

Pour ces entités, la PGSSI et les exigences décrites dans la PSSI s'étendent à :

- Tous les fournisseurs de prestations dans le domaine des SI : entités internes ou externes fournissant, directement ou indirectement, des biens et services dans le domaine des systèmes d'information ;
- Tous les usagers internes et externes des SI : entités, agents, élus, ou personnel externe disposant d'un accès autorisé aux systèmes d'information ;
- Toutes les données dématérialisées nécessaires à l'exécution des missions de la collectivité.
- Tous les traitements des informations : ensemble des opérations effectuées avec des données sources pour produire des résultats permettant la prise de décision et/ou l'accomplissement d'une action ; ceci concerne tout le cycle de vie des données, depuis la saisie jusqu'à la destruction, en passant par le traitement, le transport, le stockage, l'exploitation et l'archivage ;
- Tous les éléments techniques matériels ou logiciels utilisés pour acquérir, produire, traiter, échanger, transporter, modifier ou stocker de l'information sous forme électronique ;
- Toutes les infrastructures : sites, bâtiments ou locaux contenant des biens matériels ou immatériels composant les systèmes d'information.
- Toutes les infrastructures industrielles : gestion technique centralisée (GTC), automates et équipements techniques.

Références légales et normatives

La PGSSI et la PSSI s'appuient et mettent en œuvre les bases légales, réglementaires et normatives listées en annexe 2.

Entrée en vigueur

La PGSSI et la PSSI entrent en vigueur de manière concomitante dès signature de ce document par le Président, après délibération qui vaut adoption par le SILA.

POLITIQUE GENERALE DE SECURITE DES SYSTEMES D'INFORMATION

OBJECTIF GÉNÉRAL

Un contexte qui appelle à davantage de sécurité

Le SILA considère que :

- Les SI sont devenus indispensables à l'ensemble de ses activités ;
- L'interconnexion entre les systèmes IT et OT devient une réalité et nécessite une attention particulière notamment sur la sécurité des accès et des liens entre ces deux écosystèmes
- Le déploiement des accès distants, les services cloud mais également l'avènement des IA exposent les SI à des risques nouveaux et croissants ;
- La transformation numérique nécessite un niveau adéquat de protection des matériels, des logiciels et des données du SILA par ses agents et pour ses usagers.

En conséquence, le SILA s'engage à mettre en œuvre une protection appropriée de son SI, contre toutes les menaces, qu'elles soient d'origine interne ou externe, naturelle, accidentelle ou délibérée. C'est l'objectif de cette PGSSI déclinée en exigences dans le chapitre PSSI.

Sécuriser selon quatre critères fondamentaux

L'objectif général de protection sera atteint par la mise en œuvre de mesures proportionnées visant à assurer le niveau de sécurité requis autour de 4 notions essentielles :

- **La confidentialité** : capacité du système à protéger les informations de toute divulgation non autorisée.
- **L'intégrité** : capacité du système à préserver les informations de toute altération, destruction ou modification non autorisée.
- **La disponibilité** : capacité du système à maintenir l'accessibilité aux informations en toute circonstance ainsi que le fonctionnement continu et fiable des applications.
- **La traçabilité** : capacité du système à relever et enregistrer les opérations qui sont effectuées dans un but de restitution ultérieure du déroulement des événements lorsque cela est nécessaire.

AXES ET PRINCIPES DE MISE EN ŒUVRE

Les objectifs généraux de sécurité permettent de définir et dimensionner les actions nécessaires à la protection informatique et numérique du SILA. Ces objectifs sont définis en cinq axes regroupant 12 principes de mise en œuvre.

Axe 1. Un système de management de la sécurité conforme aux meilleures pratiques

1er principe : documenter

La documentation du système de management de la sécurité se fonde sur une architecture à 3 niveaux : les politiques (niveau 1), les directives (niveau 2) et les processus (niveau 3).

Niveau 1 : les politiques sont des documents de niveau stratégique qui fixent les objectifs, les principes et l'organisation. Pour la sécurité du SI, on distingue deux politiques :

- La politique générale de sécurité des SI (PGSSI), définit les objectifs principaux, les principes de mise en œuvre et les responsabilités.
- La Politique de Sécurité des SI (PSSI) définit l'organisation et les processus autour des systèmes d'information, et leur mise en place pour répondre de manière technique et organisationnelle aux exigences de la PGSSI.

Comme spécifié en introduction, au paragraphe « entrée en vigueur », ces deux politiques sont regroupées dans le présent document qui est adopté par la Direction Générale du SILA qui a pris part à sa conception ; il est présenté aux élus qui adoptent de fait la PGSSI et la PSSI comme document de référence en matière de sécurité informatique au SILA.

Niveau 2 : les directives de sécurité sont des documents qui déclinent les politiques pour un domaine spécifique, afin de définir les exigences organisationnelles ou techniques de sécurité correspondantes. On distingue trois types de directives :

- Les directives de sécurité générales : elles sont élaborées par la DSIN, constituent le socle sécuritaire et s'appliquent à tout le périmètre de la PGSSI.
- Les directives de sécurité métiers à caractère technique peuvent compléter les directives générales de sécurité émises par la DSIN. Ces directives peuvent être élaborées par les directions métier pour répondre à des besoins spécifiques. Elles sont soumises à l'approbation de la DSIN, qui en évaluera l'impact et assurera la cohérence globale.
- Les directives de sécurité métiers à caractère non technique peuvent compléter les directives générales de sécurité émises par la DSIN. Elles sont élaborées par les directions métier en fonction de leurs besoins spécifiques.

Niveau 3 : les processus, procédures et modes opératoires sont des documents de niveau opérationnel qui décrivent les activités à réaliser (par qui, comment et avec quoi). Les processus des directions métier et de la DSIN intègrent les exigences de sécurité exprimées par les directives tant générales que spécifiques aux métiers.

Axe 2. Une gestion des risques régulière, efficace et proportionnée

2ème principe : gérer les risques

Tout SI fait l'objet d'une gestion des risques liés à la sécurité. Cette gestion assure que les exigences en matière de sécurité des systèmes sont identifiées et que l'identification, l'appréciation et le traitement des risques sur le SI sont régulièrement effectués. Elle permet de définir et de mettre en œuvre des mesures de sécurité adaptées en s'assurant que les actions prévues et les coûts engendrés sont proportionnés à la réduction de risque qui sera obtenue.

Axe 3. Des mesures de sécurité conformes aux meilleures pratiques

3^{ème} principe : inventorier

Tous les biens liés au SI sont identifiés, inventoriés et attribués à un propriétaire. Ils sont classifiés selon leur niveau d'importance afin de mettre en place et de maintenir une protection appropriée.

4^{ème} principe : sécuriser les utilisateurs et les usages

La sécurité relative aux ressources humaines est prise en compte, afin de réduire le risque de vol, de fraude ou de mauvais usage des SI, ainsi que de s'assurer que les utilisateurs connaissent leurs responsabilités et qu'ils sont en adéquation avec les fonctions qui leur sont attribuées.

5^{ème} principe : sécuriser les biens et les lieux

La sécurité physique est assurée afin d'empêcher tout accès non autorisé et de protéger les éléments du SI contre les menaces extérieures et environnementales.

6^{ème} principe : gérer les accès

Seuls les personnes ou systèmes autorisés ont accès aux systèmes d'information. Tout départ ou changement de fonction d'un utilisateur doit s'accompagner des ajustements nécessaires de ses droits d'accès.

7^{ème} principe : déclarer les événements

Tous les événements et les failles de sécurité sont signalés, traités et analysés par les responsables désignés, afin de limiter leur impact et de permettre la mise en œuvre d'actions correctives dans les meilleurs délais.

8^{ème} principe : prévoir la continuité

La continuité des activités est assurée par l'identification des sinistres envisageables et de leurs impacts ainsi que par la mise en œuvre des solutions de secours permettant, même en mode dégradé, la continuité des activités en fonction de la nécessité qu'il y a de les préserver.

9^{ème} principe : vérifier la conformité

La conformité des SI aux exigences légales, contractuelles et techniques est vérifiée à échéances régulières.

Axe 4. Une exploitation et une évolution des SI conforme aux politiques de sécurité

10^{ème} principe : maîtriser les environnements métiers

L'acquisition, le développement et la maintenance du SI sont maîtrisés en veillant à ce que la sécurité fasse partie intégrante du SI, afin de répondre aux besoins exprimés par les métiers concernés.

11^{ème} principe : maîtriser l'environnement informatique

L'exploitation du SI est maîtrisée à travers des responsabilités et des procédures clairement définies et documentées, afin de sécuriser et de surveiller les moyens de traitement de l'information

conformément aux besoins. La sécurité des échanges d'information est également prise en compte.

Axe 5. Une mise en œuvre progressive et pragmatique

12^{ème} principe : mettre en œuvre

La mise en œuvre de la gestion des risques et des mesures de sécurité qui en découlent est réalisée de manière pragmatique en abordant les risques transversaux et les risques sectoriels les plus importants dans le cadre de l'élaboration des schémas directeurs ou de l'évolution du SI jugés par les parties prenantes comme les plus critiques.

RESPONSABILITÉS

Pour assurer la mise en œuvre de la PGSSI et de la PSSI, les responsabilités sont réparties entre différentes parties prenantes, conformément au dispositif réglementaire en vigueur.

Le SILA

En tant qu'autorité territoriale, le SILA par la voix de ses élus et de sa DG, est responsable :

- D'adopter la PGSSI afin de définir les objectifs généraux et les principes de mise en œuvre de la protection des informations, en particulier des données personnelles, afin de garantir en tout temps leur disponibilité, leur intégrité et leur confidentialité ;
- D'adopter, via une directive spécifique, les principes de gestion des risques ainsi que les critères d'évaluation et d'acceptation des risques ;
- D'accepter formellement les risques transversaux résiduels identifiés par la DSIN ;
- De mandater régulièrement des audits de sécurité ;
- D'adopter les propositions d'amélioration de la sécurité proposée par la DSIN

Le RSSI

Le responsable de la sécurité du système d'information (RSSI) a en charge le pilotage de la sécurité du SI de la collectivité en collaboration avec les équipes techniques, la DG, les ressources humaines et le service juridique. Il travaille de pair avec le DSI et l'équipe de la DSIN pour s'assurer de la bonne prise en compte des orientations et actions demandées pour la SSI du SILA.

Il est le représentant et donc le contact privilégié de la collectivité auprès des autorités, partenaires, fournisseurs et clients en matière de SSI.

Le DSI

Le Directeur des systèmes d'information et du numérique a la responsabilité de veiller à la mise en œuvre d'un système de gestion de la sécurité conforme à la PGSSI ; la PSSI qui constitue le deuxième volet de ce document est sa feuille de route commune avec le RSSI, la DSIN et les Directions métiers. Le DSI a la charge de mettre en œuvre les actions de la PSSI pour répondre aux besoins généraux de la PGSSI.

Les Directions métiers

Les Directions métier, c'est à dire autres que la DSIN et la DG, ont la responsabilité avec l'appui de la DSIN :

- De définir les directives de sécurité métier à caractère non informatique.
- De proposer à la DSIN, si nécessaire, les directives de sécurité métier à caractère informatique ou numérique.
- D'assurer l'utilisation des SI conformément aux politiques et directives de sécurité.
- D'identifier les besoins de sécurité, les exigences légales, les menaces et vulnérabilités propres à leur métier.
- D'analyser et d'évaluer les risques, afin de déterminer les niveaux de sécurité requis, de sélectionner les mesures appropriées et d'accepter formellement les risques sectoriels résiduels.
- D'arbitrer, si nécessaire, le plan sectoriel de traitement des risques.
- D'assurer l'application de la PGSSI/PSSI et des directives associées dans le cadre de leur périmètre et, par extension, auprès de leurs usagers et fournisseurs internes ou externes.
- De demander à la DSIN, si nécessaire, les contrôles découlant de l'application de la loi sur le personnel.

La DSIN

La DSIN a la responsabilité de :

- Proposer à la DG et mettre en œuvre la PGSSI ;
- Intégrer les principes de la PGSSI dans ses processus et procédures (c'est-à-dire appliquer la PSSI) ;
- Soutenir les Directions métiers dans toutes les activités de gestion des risques de sécurité liées à leur transformation numérique ;
- Dresser périodiquement un état des lieux des risques de sécurité encourus et proposer des mesures préventives et correctives adaptées aux moyens qui lui sont alloués ;
- Mettre en œuvre et d'opérer les mesures de sécurité adoptées ;
- Valider les directives métiers à caractère informatique ou numérique ;
- Assurer l'utilisation, l'exploitation et l'évolution des SI conformément aux politiques et directives de sécurité ;
- Coordonner les activités des parties prenantes en matière de SSI ;
- Sensibiliser les agents et les tiers concernés aux risques encourus et aux mesures de sécurité correspondantes ;
- Communiquer les politiques et directives ainsi que sensibiliser les utilisateurs à la SSI.

Les agents de la DSIN

Chaque agent de la DSIN est responsable :

- De réaliser ses activités, de faire usage de ses droits d'accès, ainsi que d'utiliser et de traiter les informations qui lui sont confiées, conformément à la *Charte des ADMINISTRATEURS des systèmes d'informations et des outils numériques du SILA* et aux directives et procédures de sécurité ;
- De signaler à l'instance compétente de la DSIN tout fait ou comportement anormal qu'il pourrait observer dans le domaine de la SSI.

Le non-respect des exigences de sécurité entraînera l'application du dispositif prévu par la *Charte des UTILISATEURS des systèmes d'informations et des outils numériques du SILA*.

Les intervenants techniques externes à la DSIN

Chaque intervenant externe à la DSIN, mettant en œuvre directement ou indirectement des systèmes informatiques ou numériques permettant de traiter des données du SILA, est responsable des données produites et traitées ainsi que des traitements qu'il effectue, conformément à la présente politique et des textes en vigueur (RGPD et norme NIS2 notamment ; références en annexe 2). Le non - respect des exigences de sécurité prévues par le SILA au travers des différentes politiques, directives et chartes présentes au SILA entraînera des poursuites conformément aux bases légales en vigueur.

Les utilisateurs du SI du SILA

Les personnes qui se sont vues attribuer des accès au SI et/ou à des actifs appartenant au SILA :

- Sont responsables de la sécurité du matériel appartenant à la collectivité, incluant les postes de travail, ordinateurs portables, smartphones ou badges d'accès ;
- Doivent respecter l'ensemble des règles émises concernant la SSI au sein du SILA, notamment au travers des chartes en vigueur, et des cadres d'exigence soumis à certains utilisateurs dans certains cas de figure ;
- Doivent se conformer aux exigences des engagements de confidentialité ou accords de non-divulgaration, des réglementations et des lois auxquelles elles sont soumises dans le cadre de leurs missions ;
- Doivent alerter de tout incident ou suspicion d'incident de SSI dont elles auraient connaissance (conformément au chapitre 12 - Gestion des incidents de sécurité (INC) / (ISO 16) de la PSSI)

POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION

OBJET

La politique de sécurité des systèmes d'information (PSSI) a pour objectif de fournir un ensemble de règles et d'exigences à mettre en œuvre au sein du SILA afin de contribuer à la sécurité des systèmes d'information (SSI). Ces règles sont issues des résultats de l'analyse des risques de la SSI.

Elle est la déclinaison pratique de la PGSSI du SILA, décrite en première partie de ce document et qui précise les grands principes, les enjeux et l'organisation dans la SSI.

EVOLUTION DE LA PSSI

La PSSI est un document pérenne, qui n'a pas vocation à évoluer régulièrement. Cependant, elle doit tenir compte des changements technologiques et réglementaires qui peuvent affecter les SI et leurs environnements, notamment en termes d'enjeux et de menaces.

La PSSI doit en conséquence être mise à jour au regard des évolutions telles que :

- Les réorganisations (mise en place d'une nouvelle structure impactant les SI par exemple) ;
- Les évolutions technologiques significatives du SI ;
- Les évolutions significatives des orientations stratégiques et commerciales des éditeurs et fournisseurs de solutions ;
- Les évolutions significatives des conditions d'exploitation ;
- Les changements majeurs de la législation et de la réglementation ou des normes nationales, européennes ou internationales.

L'évolution de la PSSI est placée sous l'autorité du RSSI du SILA qui :

- Déclenche les opérations nécessaires à sa mise à jour ;
- Propose, en s'appuyant sur les acteurs nécessaires, les révisions et les versions successives qu'il soumet pour validation.

PRINCIPES DES REGLES ET EXIGENCES EDICTEES DANS LA PRESENTE PSSI

Les règles édictées dans la présente PSSI sont issues des risques identifiés dans l'analyse de risques de sécurité des SI, en lien avec les exigences de sécurité des norme ISO 27001 et 27002 et des bonnes pratiques de l'ANSSI. Les règles se présentent sous la forme ci-dessous :

Ref.*	Nom de la règle
1. Exigence 1. - Sous exigence 1. <i>Complément d'information</i>	

Ref* : Référence de la règle, de la forme PS-XY.

Mot clés utilisés : Les mots clés utilisés dans ce document doivent être interprétés comme décrit ci-dessous :

1. **DOIT** : ce mot, ou les termes « **OBLIGATOIRE** » ou « **DEVRA** », veut dire que la définition est une exigence absolue de la PSSI.
2. **NE DOIT PAS** : cette phrase, ou la phrase « **NE DEVRA PAS** », veut dire que la définition est une interdiction absolue de la PSSI.
3. **DEVRAIT** : ce mot, l'adjectif « **RECOMMANDÉ** », ou la formulation « **IL CONVIENT DE** » veut dire qu'il peut exister des raisons valides dans des circonstances particulières pour ignorer un point particulier.
4. **NE DEVRAIT PAS** : cette phrase, ou la phrase « **NON RECOMMANDÉE** » veut dire qu'il peut exister des raisons valides dans des circonstances particulières quand le comportement spécifique est acceptable ou même utile.
5. **PEUT** : ce mot ou l'adjectif « **OPTIONNEL** », signifie qu'un point est vraiment optionnel et fourni à titre d'indication ou d'exemple.

1 - Politique et Organisation de la sécurité de l'information (PSI et ORG) / (ISO 5 et 6)

Le SILA a défini un cadre de gestion de la sécurité de l'information au travers de sa PGSSI. La DG a validé les objectifs des projets d'amélioration de la SSI et assuré son engagement en validant formellement la PGSSI et les résultats des analyses de risques réalisées au sein de la collectivité.

1.1. Politique de sécurité des Systèmes d'information

PSSI-PSI-01	Politique de sécurité des systèmes d'information
1. Une PGSSI et une PSSI doivent être définies, formalisées et approuvées par la DG du SILA, et votées par les élus. Ces deux politiques peuvent être un seul et même document. 2. La PSSI doit être diffusée et communiquées aux utilisateurs et aux tiers concernés, soit en l'état, soit en la déclinant sous forme de chartes ou clauses faisant références à la PSSI. 3. La PGSSI et la PSSI n'ont pas vocation à évoluer régulièrement cependant elles doivent tenir compte des changements technologiques et réglementaires qui peuvent affecter les SI et leurs environnements, notamment en termes d'enjeux et de menaces. Le SILA doit a minima revoir sa PSSI tous les 3 ans.	

PSSI-PSI-02	Gestion des dérogations
Tous les écarts par rapport aux règles de sécurité devront être considérés comme des failles de sécurité et ne devraient pas être autorisés. Néanmoins, dans certains cas, certaines règles établies ne peuvent pas être appliquées. Il est alors possible de délivrer des dérogations : 1. Les dérogations doivent être validées par les propriétaires des actifs concernés par la faille, par le RSSI, et en cas de conflit, par la DG du SILA. 2. Les dérogations doivent être enregistrées et documentées pour conserver la trace de ces décisions, par le RSSI et/ou le DSI.	

1.2. Organisation interne

Les rôles et responsabilités ainsi que les instances de pilotage prévues au sein du SILA sont définies dans le chapitre « RESPONSABILITÉS » de la PGSSI.

PSSI-ORG-01	Définition et attribution des rôles et responsabilités
Les rôles et responsabilités liées à la sécurité de l'information doivent être identifiés et attribués : 1. Les rôles et responsabilités à l'échelle du SILA doivent être définis dans la PGSSI. 2. Les missions des principaux rôles liés à la SSI de la collectivité doivent être détaillés dans des fiches de postes. 3. Les rôles et responsabilités liées à la SSI doivent être communiqués à l'ensemble des agents pour qu'ils identifient les personnes ressources en la matière.	

PSSI-ORG-02	Séparation des tâches
1. Les tâches et les domaines de responsabilité incompatibles doivent être séparés pour limiter les possibilités de modification ou de mauvais usage, non autorisé ou involontaire, des actifs de la collectivité. 2. Les rôles attribués doivent, dans la mesure du possible, permettre la séparation des tâches de demande, validation, réalisation et de contrôle d'une activité.	

PSSI-ORG-03	Comités de pilotage sécurité
Des comités liés à la SSI doivent être identifiés, mis en place et réalisés de manière régulière. 1. Un comité doit être réalisé avec la DG afin notamment, de l'informer sur le niveau de risque SSI, sur l'avancement des projets sécurité et présenter les éléments nécessitant un arbitrage ou une prise de décision. Ce comité est constitué des membres de la DG, du RSSI, du DSI et des agents de la DSIN ayant un rôle dans la SSI (chef du service exploitation, technicien réseau et sécurité notamment) 2. Des points de pilotage de la sécurité doivent être réalisés avec les acteurs opérationnels (Directions métiers, intervenants externes) pour assurer le suivi des actions de sécurité et pour identifier des opportunités d'amélioration (évolution des besoins sécurité, nouvelles menaces, retours d'expériences suite à des incidents, etc.). 3. Les comités sont réalisés a minima de manière annuelle et à la demande autant que de besoin. Les comptes rendus sont stockés dans une GED accessible à l'ensemble des membres du comité.	

PSSI-ORG-04	Relations avec les autorités et groupes de travail spécialisés
1. Le RSSI devrait entretenir des relations appropriées avec les autorités compétentes (ANSSI, CERT-FR, DINUM). 2. Le RSSI devrait participer à des forums spécialisés dans la sécurité et adhérer au nom du SILA à des associations professionnelles, des groupes d'intérêts, et des événements spécialisés organisés par des acteurs de la cybersécurité (ANSSI, CNIL, ADIRA, les Assises de la Sécurité, le Forum International de la Cybersécurité (FIC), etc.) afin d'identifier les menaces susceptibles	

de nuire à l'organisation et aux SI, de suivre leur évolution et leur niveau d'impact pour les SI, ainsi que de proposer des mesures de sécurité permettant de les limiter.

2 - Connaissance du SI et gestion des actifs (CSI) / (ISO 8)

Afin d'avoir une gestion des risques de sécurité adéquate, il est important de disposer d'une bonne connaissance du système d'information et de ses composantes :

- Les données et informations manipulées ;
- Les processus mis en œuvre ;
- Les équipements matériels, logiciels et réseaux qui constituent ce SI.

2.1 Identification des objectifs de sécurité

Les informations et processus essentiels mis en œuvre par le système d'information doivent être identifiés afin de définir les besoins de sécurité des éléments sur lesquels ils reposent.

PSSI-CSI-01	Identification des informations et processus essentiels
1. Les informations et processus essentiels mis en œuvre dans et par le système d'information doivent être listés. - Les informations essentielles peuvent être des informations métiers ou opérationnelles essentielles à l'activité ou dont la divulgation peut porter préjudice aux activités. Elles peuvent également être des informations soumises à des contraintes légales (ex données personnelles et/ou sensibles par exemple) ou possédant une valeur probante (ex : documents signés électroniquement) - Les processus essentiels sont les fonctionnalités ou les services rendus par le système d'information, supports aux activités les plus importantes et dont la perte ou la dégradation rend la réalisation de l'activité difficile voire impossible. Cette liste doit permettre de déterminer sur quels composants du système d'information ces éléments essentiels reposent (bases de données, partages de fichiers, postes de travail, etc.). Ces composants correspondent aux éléments critiques (serveurs, postes, répertoires) pour l'activité. À ce titre, ils devront faire l'objet de mesures de sécurité spécifiques pouvant porter sur la surveillance, la sauvegarde, la journalisation, le contrôle des accès, etc.	

PSSI-CSI-02	Identification des objectifs de sécurité sur les éléments critiques
1. Les objectifs ou besoins de sécurité à couvrir sur le système d'information doivent être identifiés. Ces objectifs définissent le cahier des charges de la sécurité du système d'information. Ces objectifs sont déterminés à partir de l'analyse de risques, mais aussi de manière indépendante, à partir : - Des besoins en disponibilité, intégrité et confidentialité et traçabilité ; - De la liste des informations et processus essentiels et des éléments critiques à protéger (cf. PSSI-CSI-01) ; - De l'étude des menaces pesant sur l'organisme (éléments menaçants, étude des vulnérabilités) ; - De l'identification des risques réels pour l'organisme.	

2. Les objectifs de sécurité doivent être revus annuellement (mise à jour de l'analyse de risques, revue de la liste des informations et processus essentiels, étude des nouvelles menaces) pour s'assurer de leur adéquation avec les mesures de sécurité en place, et celle à prévoir (budgétairement et en charge de travail)

2.2 Classification de l'information

La notion d'information englobe l'ensemble des données (y compris les données à caractère personnel au sens du RGPD), documents, connaissances et échanges, quel que soit leur format ou support,

Les informations et les applications doivent être classifiées en fonction de leur besoin respectif de protection.

PSSI-CSI-03	Classification et protection des informations
1. L'ensemble des informations doit être classifié selon les échelles définies par le SILA et la réglementation en vigueur. 2. Un propriétaire doit être identifié au sein des métiers pour chaque type d'information. Ce dernier est en charge de l'identification et de l'évaluation de la sensibilité des informations dont il est propriétaire. 3. Des mesures de sécurité doivent être mises en œuvre pour assurer la protection des données en fonction de leur niveau de confidentialité.	

L'attribution du niveau de sensibilité des informations peut s'appuyer sur une échelle constituée des niveaux suivants :

Niveau	Définition
1 Public	Données pouvant être diffusées publiquement sans impact pour le SILA.
2 Interne (SILA)	Données destinées à n'être diffusées qu'en interne du SILA sans impact. La divulgation à d'autres personnes aurait un impact limité.
3 Restreint (service SILA)	Données sensibles, données à caractère personnel, ne devant être communiquées qu'à un groupe de personnes identifiées (restreintes à un service de la collectivité par exemple) ayant un intérêt légitime à y accéder. La divulgation à d'autres personnes pourrait avoir des conséquences néfastes pour le SILA, de manière ponctuelle.
4 Confidentiel	Données stratégiques, données à caractère personnel (DCP) sensibles... Accessibles uniquement à un nombre limité de personnes nominativement identifiées du SILA et en ayant le besoin. La divulgation à d'autres personnes pourrait avoir des conséquences néfastes pour la collectivité, de manière durable.

Les mesures de sécurité suivantes peuvent être appliquées en fonction du niveau de confidentialité défini :

Thèmes		Public	Interne (SILA)	RESTREINT (service SILA)	CONFIDENTIEL SILA
Marquage des documents		Marquage « Document public »	Marquage « Document à usage interne SILA »	Mention « RESTREINT SILA » sur le document	Mention « CONFIDENTIEL SILA » sur le document
Diffusion		Libre (interne et externe)	Libre, en interne du SILA	Seules les personnes mentionnées dans la liste de diffusion ont le droit d'en connaître. Aucune diffusion externe à cette liste ne peut être réalisée sans l'accord explicite de la Direction du SILA.	Seules les personnes mentionnées dans la liste de diffusion ont le droit d'en connaître. Aucune diffusion externe à cette liste ne peut être réalisée sans l'accord explicite de la Direction du SILA.
Impression		Libre	Récupération immédiate du document sur l'imprimante (contrôle par un PIN ou un badge)		
Stockage intermédiaire et courant	Information numérique	Libre	Supports mis à disposition ou explicitement autorisés (espaces disques des terminaux autorisés, répertoires partagés et espaces collaboratifs, supports amovibles mis à disposition), gestion des droits d'accès. Si valeur probante conservation dans un coffre -fort électronique ou SAE		Chiffrement obligatoire du fichier, du répertoire ou du disque dur Accès après authentification nominative, si valeur probante conservation dans un coffre -fort électronique ou SAE
	Information papier	Libre	Libre dans les locaux	Dans des tiroirs ou armoires fermés à clé	Dans des tiroirs ou armoires fermés à clé
Archivage définitif	Information numérique	SAE	SAE	SAE	SAE
	Information papier	Local d'archivage fermé à clef	Local d'archivage fermé à clef	Local d'archivage fermé à clef	Local d'archivage fermé à clef
Transmission	Information numérique	Libre	Envoi aux personnes autorisées Canaux autorisés (mail pro, liens et espaces collaboratifs)	Envoi aux personnes autorisées Canaux autorisés (mail pro, liens et espaces collaboratifs) Utilisation de plateforme sécurisée pour le partage de documents	Utilisation de plateforme sécurisée pour le partage de documents

	Information papier	Libre	Documents sous surveillance permanente du personnel	
Destruction	Information numérique	Libre, en accord avec la réglementation et sous autorisation du Contrôle scientifique et technique*	Nettoyage des supports (disques, supports de sauvegarde, support amovibles, périphériques, etc.), en accord avec la réglementation et sous autorisation du Contrôle scientifique et technique*	Nettoyage des supports (disques, supports de sauvegarde, support amovibles, périphériques, etc.), que ce soit pour réaffectation, mise au rebut ou pour opération de maintenance avec sortie d'équipement, en accord avec la réglementation et sous autorisation du Contrôle scientifique et technique*
	Information papier	Libre	Destruction sécurisée en accord avec la réglementation et sous autorisation du Contrôle scientifique et technique*	

* Agent de l'Etat, le directeur des Archives Départementales exerce, sous l'autorité du Préfet, **le contrôle scientifique et technique** de l'Etat sur les archives publiques. Il vérifie, par des contrôles sur pièces ou sur place, les conditions de gestion, de collecte, de sélection et d'élimination, de traitement, de classement, de conservation et de communication des archives des collectivités.

La gestion des cycles de vie des données et de leur durée de conservation réglementaire est également précisée dans les documents relatifs à la gouvernance de la donnée de la collectivité, et régie par les textes de lois cités en préambule.

2.3 Cartographie et gestion des actifs

Le SILA doit être en mesure de connaître l'ensemble des actifs qu'il possède afin de gérer efficacement leur sécurité.

PSSI-CSI-04	Inventaire et responsables des actifs
- Le propriétaire de chaque actif doit être identifié. Il aura notamment pour mission de : - S'assurer que les actifs sont inventoriés correctement, classés et protégés ; - Définir et revoir périodiquement les classifications et les restrictions d'accès aux applicatifs importants ; - S'assurer que les manipulations de suppression ou de destruction des actifs sont réalisées correctement. - L'ensemble des actifs du Système d'Information doit faire l'objet d'un inventaire exhaustif tenu à jour au minimum une fois par an. - Les inventaires des actifs peuvent être distincts en fonction de leur type (composants réseau, postes de travail, serveurs, téléphones, applications, etc.). Toutefois, ces inventaires devraient permettre de déterminer facilement les dépendances entre actifs, par exemple quels sont les équipements nécessaires au fonctionnement des applications métiers afin de faciliter les maintiens en condition opérationnels (MCO) et en condition de sécurité (MCS).	

PSSI-CSI-05	Attribution et restitution des actifs	
1. Les utilisateurs ou services se voyant remettre un actif doivent être identifiés dans l'inventaire des actifs ; 2. Le besoin de mise à disposition d'un actif pour un utilisateur doit être validé par le biais de la fiche de dotation ou tout autre formulaire de remise de matériel ; 3. Des procédures doivent être remises aux utilisateurs afin qu'ils utilisent les actifs qui leurs sont attribués de manière correcte ; 4. Les utilisateurs doivent restituer la totalité des actifs de l'organisation qu'ils ont en leur possession au terme de la période d'emploi, du contrat ou de l'accord ; 5. Les utilisateurs doivent signer un formulaire de remise des actifs lors de leur départs ; ces formulaires sont stockés par la DSIN.		

PSSI-CSI-06	Mise au rebut des supports et des actifs	
1. Les supports arrivant en fin de vie et qui sont susceptibles de contenir des informations non publiques doivent être effacés par les utilisateurs (cf. PSS-RH-03 : Charte) ; 2. Quand ils sont mis au rebut, les disques durs des équipements (postes de travail, serveurs, imprimantes ...) doivent être effacés selon un procédé garantissant l'impossibilité de reconstituer les données stockées. Le procédé doit être réalisé avec des logiciels certifiés par l'ANSSI tel que Blancco ; en cas d'impossibilité de supprimer les données les disques seront physiquement détruits (broyage) 3. En cas de délégation de cette tâche à un tiers, des bordereaux de destruction doivent être exigés et conservés dans la GED de la DSIN ;		

3 - Sécurité des Ressources Humaines (RH) / (ISO 7)

La sécurité est l'affaire de tous et requiert l'engagement de chacun. Afin de s'assurer de l'adhésion de chaque utilisateur à la démarche sécurité, le SILA a défini un ensemble de mesures permettant de responsabiliser les utilisateurs des SI, les administrateurs de la DSIN et des Directions métiers, et de diffuser les règles et bonnes pratiques de sécurité.

3.1. Avant l'embauche ou la contractualisation

PSSI-RH-01	Adoption de critères sécurité dans le recrutement	
1. Les compétences, ainsi que les connaissances des bonnes pratiques en sécurité des systèmes d'information nécessaires aux postes d'administrateurs techniques et ou fonctionnels du SI doivent être identifiées et intégrées aux critères de sélection des candidats. Le recrutement devrait notamment permettre de s'assurer que : - Les diplômes, certifications ou examens mentionnés par les candidats sélectionnés sont véridiques dans le cas d'un poste à hautes compétences ou responsabilités ; - Les compétences des collaborateurs sont en adéquation avec les enjeux et attentes du poste à pourvoir, notamment sur les aspects de sécurité de l'information ; - Leurs éventuels antécédents ne sont pas incompatibles avec le poste.		

PSSI-RH-02	Clauses de sécurité dans les contrats de travail	
1. Les contrats de travail des agents devraient intégrer des références vers les règlements applicables et notamment les chartes informatiques en vigueur (utilisateurs et administrateur ; cf. PSSI-RH-03) 2. La ou les chartes nécessaires au poste occupé par l'agent doivent être lues idéalement avant la prise de poste, et leurs récépissés signés avant la première connexion au SI.		

3.2. Pendant la durée du contrat

PSSI-RH-03	Chartes d'utilisation ou d'administration des systèmes d'information	
1. Les règles à respecter par les utilisateurs et/ou les administrateurs des SI sont définies et formalisées dans la charte des utilisateurs du SI et/ou la charte des administrateurs du SI ; 2. Les récépissés signés attestant de la lecture de l'acceptation de la charte sont stockés (physiquement et/ou numériquement) par les services du SILA		

PSSI-RH-04	Sensibilisation des utilisateurs	
1. Les différents utilisateurs (agents, administrateurs, apprentis, stagiaires) du système d'information doivent être sensibilisés et/ou formés à leur arrivée dans la collectivité. 2. Des sessions de sensibilisation et de formation sur la SSI sont mis en place de manière régulière. Les sujets doivent notamment porter sur : - Les risques et les exigences de sécurité informatique selon le profil des agents ; - L'utilisation des outils informatiques (exemple : la messagerie) et des mesures de sécurité ; - Les exigences juridiques (notamment sur les données personnelles) ; - La réaction face à des incidents de sécurité (vigilance et communication) ; 3. Cette sensibilisation doit s'étendre aux prestataires et fournisseurs disposant d'un accès prolongé ou régulier au SI.		

PSSI-RH-05	Formation des agents de la DSIN	
1. Un plan de formation spécifique à la SSI est mis en place pour les agents de la DSIN selon leur poste et leur profil ; il doit répondre à une mise à niveau régulière des compétences pour assurer le maintien en condition opérationnelle et en condition de sécurité du SI. 2. Les compétences clés doivent si possible être doublées afin de disposer de remplaçants avec des compétences et niveau de connaissance équivalent pour couvrir les phases vacantes.		

3.3. Rupture, terme ou modification du contrat

Des règles de sécurité sont prévues à la rupture, au terme ou lors de la modification du contrat d'un utilisateur du SI.

PSSI-RH-06	Mobilités internes	
1. En cas de mobilité interne d'un agent, les droits d'accès à l'ancien poste sont supprimés et les actifs remis à la DSIN 2. Les droits d'accès au nouveau poste et les actifs sont remis à la date effective de la mobilité.		

3. Les attributions sont faites dans le cadre des exigences de la règle PSSI -CSI-05

PSSI-RH-07	Gestion des départs utilisateurs
1. En cas de départ d'un utilisateur, ses identifiants et droits d'accès doivent être désactivés au jour du départ des effectifs ou de la date de fin de contrat ; 2. L'ensemble des actifs propriété de la collectivité et mis à disposition de l'utilisateur (cf. PSSI-CSI-05 : Attribution des actifs) doivent être au préalable restitué (poste de travail, smartphone, etc.) ; 3. Le départ d'un utilisateur est signifié par sa hiérarchie à la DSIN dans les meilleurs délais ; en complément la DRH envoie un tableau des départs à chaque fin de mois.	

4 - Relation client/fournisseur (EXT) / (ISO 15)

Les tiers impliqués dans la fourniture de services informatiques, accédant à des ressources du SI ou des données confidentielles sont porteurs de risques. Les tiers doivent prendre conscience de ces risques et être responsabilisés sur les règles de sécurité à respecter.

PSSI-EXT-01	Clauses et engagements de sécurité
1. Les prestations informatiques, ou les tiers accédant au système d'information, doivent être encadrés par des clauses ou exigences de sécurité que le tiers doit respecter dans le cadre de ses activités ; Ces clauses peuvent être basées sur : - Les règles de la présente PSSI ; - Les termes du marché / contrat / convention qui lie le tiers à la collectivité - Les normes en vigueur dans le cadre de l'activité concernée (NIS2, RGPD, etc.)	

PSSI-EXT-02	Sécurité dans les services externalisés
1. Le recours à des services externalisés (centre de service, solutions SaaS, PaaS ou IaaS) doit faire l'objet d'une étude au préalable afin d'identifier les problématiques de sécurité à prendre en compte dans la décision et la contractualisation. 2. L'étude porte sur : - La responsabilité entre le SILA et les prestataires des services externalisés (exploitation, mise à jour, gestion des incidents) ; - Le niveau de mutualisation des ressources fournies par les prestataires entre ses différents clients ; - La sécurité de la plateforme d'hébergement des services externalisés ; - Les modalités d'interfaces et d'accès du prestataire et des personnes tiers accédant aux données ainsi que l'étendue des droits d'administration et la journalisation de leur utilisation. - La maturité de gestion de la sécurité, notamment dans le support et la fourniture de correctifs de sécurité 3. Si le service externalisé est en lien avec l'OT, le cadre d'exigence NIS2 prévu par le SILA sera appliqué et l'étude s'y réfèrera. 4. Si le service externalisé traite des données sensibles de la collectivité, une AIPD sera nécessaire à l'étude.	

PSSI-EXT-03	Engagements de services sur les composants ou services critiques	
1. Pour tout contrat conclu avec un tiers portant sur un composant critique des SI (exemple : cœur de réseau ...), des engagements portant sur le niveau de services offert doivent être définis et l'atteinte de ces engagements doit faire l'objet d'un suivi régulier.		

PSSI-EXT-04	Suivi et contrôle des prestations fournies	
1. Afin de garantir un niveau de sécurité adéquat de la prestation dans le temps, celle-ci doit être contrôlée régulièrement notamment par : - Un contrôle, par les équipes encadrant la prestation, sur la conformité du prestataire au cahier des charges ; - Des points réguliers avec le prestataire sur le respect de ses engagements, avec si possible la fourniture de preuves.		

PSSI-EXT-05	Maîtrise des interventions externes	
1. Un enregistrement (automatique ou manuel) des actions menées par des intervenants externes (maintenance, infogérance) sur les systèmes internes doit être réalisé pour garder la maîtrise des modifications réalisées. L'utilisation d'un bastion d'administration permettra la traçabilité des interventions (historique des connexions, compte utilisé, ressource et compte associé, date, temps d'intervention, motif de l'intervention)		

5 - La sécurité dans les projets (ISP) / (ISO 14)

L'intégration de la sécurité dans les projets et le « Security by design » consiste à prendre en compte la sécurité sur tout le cycle de vie d'un projet. Les erreurs de conception, d'intégration ou les mauvaises pratiques de développement étant à l'origine de la plupart des vulnérabilités, il est nécessaire de se poser les bonnes questions à chaque phase d'un projet pour limiter la présence de failles intrinsèques.

PSSI-ISP-01	Intégration de la sécurité dans les projets	
1. Avant le lancement d'un projet dans la phase de faisabilité, les objectifs de sécurité doivent être définis pour identifier les éléments à protéger ou les menaces à couvrir ; 2. Les mesures de sécurité répondant aux objectifs de sécurité doivent être mises en place pour répondre à des besoins de protection, de prévention ou de réduction de la surface d'exposition ou de continuité/récupération. 3. Les mesures de sécurité doivent inclure les sujets suivants : - Protection physique ; - Contrôle d'accès ; - Protection des données d'accès ; - Cloisonnement des environnements et filtrage ; - Chiffrement des données et chiffrement des flux ; - Contrôle d'intégrité ; - Supervision et journalisation ;		

- Redondance et reprise d'activités.

PSSI-ISP-02

Principes d'ingénierie dans la sécurité des systèmes

Dans tous ses projets, le SILA doit suivre les principes généraux de la PSSI adoptés et encadrés par la DSIN :

1. Respecter l'ensemble des règles de la PSSI ;
 2. Utiliser des technologies maîtrisées par le SILA ;
 3. Changer les mots de passe par défaut des systèmes, si le système le permet ;
 4. Prévoir l'intégration des nouveaux composants dans les processus d'exploitation et de sécurité lors de toute installation, y compris sur les environnements amont. Les processus de sécurité à prendre en considération sont notamment :
 - Gestion de la détection et du traitement des incidents ;
 - Protection contre les logiciels malveillants ;
 - Gestion de la veille, des vulnérabilités et des mises à jour ;
 - Gestion des sauvegardes ;
 - Gestion de la journalisation.
 5. Respecter les mesures de sécurité concernant les réseaux (zones de cloisonnement, chiffrement, accès distants ...).
- Durcir les différents composants matériels et logiciels.

PSSI-ISP-03

Critères d'acquisition de progiciels

1. L'acquisition de progiciels, même géré directement par les Directions métiers, nécessite l'implication de la DSIN en amont du lancement du projet (phase de faisabilité) ou dans les instances de suivi d'exploitation de la solution.
2. Des critères de sécurité doivent être intégrés aux critères de sélection d'une application/progiciel externe ou système embarquant du logiciel. Ces critères doivent être basés sur :
 - Les objectifs de sécurité à remplir par le système/application/progiciel ;
 - La robustesse des mécanismes de sécurité embarqués ;
 - La prise en compte de la sécurité dans les développements (si l'information est disponible) ;
 - La prise en compte du RGPD pour les traitements de données inhérents à la solution ;
 - La présence de vulnérabilités publiques ;
 - La présence d'un support de l'éditeur ou d'une communauté, notamment pour la fourniture de correctifs ;
 - La réactivité de correction ;
 - L'ensemble des règles de la présente PSSI.
3. Dans le cas d'une solution IaaS, PaaS ou SaaS, les exigences de la règle PSSI-EXT-02 (Sécurité dans les services externalisés) s'appliquent.

PSSI-ISP-04

Sécurisation des services exposés sur des réseaux publics

1. Les applications et services web exposés sur des réseaux publics et traitant des données non publiques doivent être protégées par double authentification et chiffrement ;
2. Si l'application le permet, un filtrage par IP publique doit être mis en œuvre afin de réduire la surface d'exposition et la protéger contre d'éventuelles connexions malveillantes.

3. La sécurité des services les plus exposés et les plus critiques, doit être régulièrement auditée afin d'identifier les vulnérabilités
4. La mise à jour des services exposés doit être réalisée dans les plus brefs délais.

6 - Planification de la continuité d'activité informatique (PCI) / (ISO 17)

Les plans de continuité et de reprise d'activité sont des procédures permettant de maintenir ou récupérer les activités critiques suite à un sinistre. Au SILA ces plans sont déclinés en PCI / PRI (plan de continuité / plan de reprise informatique) ; en lien avec la PSSI, ils permettent de s'assurer que dans ces phases de reprise ou de modes dégradés, la continuité de la sécurité informatique est assurée.

PSSI-PCI-01	Définition des plans de continuité et de reprise
Les plans de continuité et de reprise informatique doivent être formalisés et permettre : 1. D'identifier les services et applications informatiques nécessaires au fonctionnement des activités, l'expression de leurs besoins en termes de niveau de service minimum indispensable et la durée d'indisponibilité maximale acceptable ; 2. D'identifier les sinistres types, tels que la défaillance de services essentiels (télécoms, énergies), les sinistres sur le site, les logiciels malveillants ou les cyberattaques ; 3. De mettre en place une infrastructure adéquate pour assurer la continuité de service ou le passage en mode dégradé ; 4. D'identifier les compétences et partenaires clés pour réaliser la continuité et la reprise informatique 5. D'identifier les actions à mener pour réaliser la continuité et la reprise informatique puis d'activité. 6. D'identifier toutes les sauvegardes de données et de configuration nécessaires pour la restauration des systèmes.	

PSSI-PCI-02	Tests des plans de continuité et de reprise
1. Des tests de continuité et de reprise informatique devraient être réalisés régulièrement (simulation de scénarios, tests de bascule, tests de restauration). Ces actions permettent de vérifier l'efficacité des procédures et de l'infrastructure. Ils permettent aussi d'entraîner les équipes à assurer la continuité et la reprise dans des délais impartis. Ces tests peuvent entrer dans le cadre de test plus large du PCA/PRA du SILA. 2. Les procédures de continuité et de reprise d'activité doivent être maintenues à jour au travers notamment de tests ou d'actes de maintenance réguliers.	

7 - Conformité et audits (AUD et CONF) / (ISO 18)

7.1. Conformité aux exigences légales et contractuelles

PSSI-CON-01	Responsabilité de la conformité aux exigences réglementaires et contractuelles	
1. La Direction Générale du SILA, par le relais du DSI, est responsable de la conformité des SI aux exigences réglementaires et contractuelles applicables ; 2. Une veille réglementaire doit être réalisée régulièrement par le RSSI afin d'identifier les nouvelles lois et réglementations applicables à la collectivité et impactant la sécurité de l'information (cf. PSSI-ORG-04)		

PSSI-CON-02	Protection des données personnelles	
1. Une politique de protection des données à caractère personnel doit être formalisée et appliquée ; elle est accessible dans la GED du SILA. 2. Des clauses relatives à l'application du RGPD sont automatiquement incluses dans les cahiers des charges des marchés publics ; 3. Afin d'uniformiser et de s'assurer de la bonne application du RGPD en interne, des process doivent être établis et documentés, et le registre des traitements doit être tenu à jour ; 4. Des actions de sensibilisation sont également menées auprès des agents du SILA afin de les responsabiliser sur leurs pratiques.		

7.2. Revues de sécurité de l'information

PSSI-AUD-01	Audit de sécurité et conformité à la PSSI	
1. Des revues indépendantes de l'approche retenue par l'organisation pour gérer et mettre en œuvre la sécurité de l'information doivent être réalisées tous les deux ans maximum ou lors de changements importants (audit de maturité) ; 2. Des revues régulières (a minima une par an) doivent être mises en œuvre par le RSSI afin de s'assurer de la bonne application ou de la mise en place des règles de la PSSI ; 3. Le RSSI contrôle et accompagne les administrateurs (techniques ou fonctionnels) les responsables de traitement et tout intervenant sur le SI, à revoir régulièrement la conformité du traitement de l'information et des procédures dont ils ont la charge au regard de la présente PSSI 4. Les systèmes d'information doivent être régulièrement audités d'un point de vue technique (audit de configuration, test d'intrusion) pour identifier les vulnérabilités techniques ; 5. En cas d'audit externe il conviendra de faire intervenir des auditeurs différents.		

8 - Sécurité physique et environnementale (PHY) / (ISO 11)

Les actifs, particulièrement ceux qui revêtent une importance cruciale pour le SILA, doivent être protégés physiquement contre les malveillances, les accidents et les événements naturels. Plusieurs dispositions et exigences s'imposent.

En préambule de cette directive, et dans l'organisation actuelle de la collectivité, il est à noter que la gestion bâtiminaire, y compris celle des contrôles d'accès aux locaux, est gérée par le Service Logistique de la Direction des ressources humaines et vie au travail (DRHVT). L'ensemble des règles ci-après sont à considérer en transparence et en forte collaboration entre la DRH et la DSIN.

8.1. Zones sécurisées

PSSI-PHY-01	Zones de sécurité physique
1. Les zones de sécurité physique doivent être identifiées en fonction de la criticité des éléments matériels contenus dans ces zones (équipement critiques, accès au réseau, documentation papier) et en tenant compte des lieux de passage. Les principales zones sont - La zone publique ; - La zone bureautique ; - Les zones techniques ; - Les zones industrielles (qui comprennent aussi des zones techniques) 2. Le périmètre extérieur des différents sites doit être clôturé (clôture, contrôle d'accès verrouillage des fenêtres en rez-de-chaussée donnant sur la voie publique). 3. Les sites concernés peuvent être protégés contre les accès non autorisés par des mécanismes de contrôle et de surveillance (vidéosurveillance, détection d'intrusion).	

PSSI-PHY-02	Contrôle d'accès physique aux zones
1. Un contrôle d'accès doit être installé entre chaque zone de sécurité, pour filtrer les utilisateurs autorisés à accéder à la zone de criticité la plus élevée ; 2. Une politique de contrôle d'accès physique doit être définie pour chaque zone et permet d'identifier : - Les catégories d'utilisateurs autorisés (agents, travailleurs temporaires, prestataires, tiers, usagers, services d'urgence, etc.) ; - Les périodes de temps pendant lesquelles les accès sont autorisés ; - Le type de passage à contrôler (porte simple, portes sécurisées, entrée de véhicule) ; - Les besoins et les contraintes spécifiques de passage (issues de secours). 3. L'accès aux zones techniques doit être limité aux administrateurs responsables de la maintenance de ces équipements, de leur sauvegarde et éventuellement d'une personne supplémentaire pour la sécurité humaine ; 4. Un système de traçabilité doit journaliser tous les accès physiques aux zones techniques ; 5. Les droits d'accès doivent être revus et mis à jour régulièrement, à minima 1 fois par an, afin de les révoquer si nécessaire. 6. La mise en place d'un système automatisé de contrôle d'accès, doit tenir compte de la continuité du service et de la continuité de la sécurité (tolérance aux pannes, autonomie en cas de panne de courant, temps de remplacement des équipements en maintenance, etc.).	

8.2. Sécurité des équipements et des salles techniques

PSSI-PHY-03	Protection des salles serveurs
1. Les équipements des SI doivent être hébergés dans les salles serveur. Elles ne doivent pas être utilisées à d'autres fins que l'hébergement des composants des SI ; 2. L'accès à ces salles doit être contrôlé par une authentification par badge et n'être accessible qu'aux seules personnes autorisées ; 3. Les salles serveurs disposant de fenêtres doivent être équipées de barreaux ;	

4. Le contenu de ces salles ne doit pas être communiqué largement. En particulier, les indications autour des salles sont interdites ;
5. Les salles serveur doivent disposer des mesures de protection suivantes :
 - Une continuité d'alimentation électrique doit être assurée (onduleurs, groupe électrogène pour la salle serveur principale) ;
 - Des moyens de protection contre les risques climatiques doivent être mis en œuvre (faux planchers, régulation hygrométrique, etc.) ;
 - Un système de climatisation sécurisé doit être installé (climatisation redondée et surveillée) ;
 - Un système de détection et d'extinction incendie adapté doit être installé ;
 - Un système anti-intrusion doit être mis en place.
6. L'agencement et la disposition des équipements au sein des salles informatiques doit permettre aux collaborateurs de circuler sans risque (fixation des faux planchers, rangement des câbles dans les faux planchers ou plafonds) pour l'exploitation quotidienne et les opérations de maintenances.
7. Les personnes étant amenées à travailler dans les salles serveur doivent respecter les règles suivantes :
 - N'accéder aux salles que lorsque ceci est nécessaire ;
 - Ne pas amener de nourriture ni de liquides dans les salles ;
 - Ne pas amener de matériel inflammable dans les salles.
 - Ne pas stocker de matériel non indispensable dans les salles.

PSSI-PHY-04
Protection des locaux techniques

1. Les équipements réseaux et électriques des SI doivent être hébergés dans des locaux techniques ;
2. Ces salles doivent être systématiquement fermées à clé, et n'être accessibles qu'aux seules personnes autorisées ;
3. Les locaux techniques doivent disposer des mesures de protection suivantes :
 - Une continuité d'alimentation électrique doit être assurée (deux réseaux dont un ondulé) ;
 - Des moyens de protection contre les risques climatiques doivent être mis en œuvre (faux planchers) ;
 - Un système de détection d'incendie doit être installé. Des systèmes d'extinction incendie doivent être maintenus opérationnels et accessibles à proximité des locaux.
4. Les personnes étant amenées à travailler dans les locaux techniques doivent respecter les règles suivantes :
 - N'accéder aux salles que lorsque ceci est nécessaire ;
 - Ne pas amener de matériel inflammable dans les salles ;
 - Ne pas stocker de matériel non indispensable dans les salles.

PSSI-PHY-05
Protection du câblage et des points d'extrémité

1. Les câbles électriques ou de télécommunication supportant des services d'information doivent être protégés contre toute interception ou dommage en appliquant, notamment, les mesures suivantes :
 - Enterrer les lignes électrique et de télécommunication, dans la mesure du possible ;
 - Séparer les câbles électriques des câbles de télécommunication ;
 - Verrouiller les points d'inspections, les chambres de câblages et les points d'extrémité.

8.3. Sécurité du matériel utilisateur

PSSI-PHY-06	Protection des matériels mis à disposition des utilisateurs	
1. Le matériel mis à disposition des utilisateurs (postes de travail, imprimantes...) doit être situé dans des locaux bureautiques sécurisés disposant à minima de : - Un système de contrôle d'accès ou d'un bâtiment fermant à clé ; - Un système de détection d'incendie et des systèmes d'extinction maintenus opérationnels et accessibles à proximité des locaux. - Des mesures techniques particulières de sécurité doivent être mise en place pour les matériels utilisés hors des locaux de la collectivité (cf. PSSI-EXP-01 : Sécurité des postes nomades).		

8.4. Gestion des visiteurs

PSSI-PHY-07	Principes d'accueil des visiteurs	
1. Pour réduire le risque de vol ou de compromission d'information au sein des zones d'accueil du public, en particulier dans les bureaux du personnel du SILA, les exigences suivantes doivent être appliquées avec les visiteurs selon qu'ils sont : - des usagers du service public : se présentent à l'accueil et sont accompagnés lors de leur déplacement dans les locaux par un agent du SILA. - des prestataires ou tiers intervenant au SILA : - Se présentent à l'accueil (ou sont redirigés vers celui-ci si cela n'a pas été fait) - Leurs dates et heures d'arrivée et de départ sont consignées dans un registre à l'accueil ; - Les visiteurs le remplissent et signent à leur arrivée et à leur départ ; - Les visiteurs doivent être accompagnés lors de leur présence sur site ; 2. Les agents du SILA doivent être sensibilisés au principe de vigilance concernant les visiteurs circulant dans certains couloirs et s'appliquer quelques règles élémentaires de sécurité : toujours fermer sa session informatique en cas d'absence même très brève, ranger les documents sensibles dans des caissons fermant à clé, utiliser le cordon de protection des PC portables, etc. ; (cf. PSSI-RH-03 : Charte des utilisateurs et des administrateurs du système d'information/ PSSI-RH-04 : Sensibilisation)		

9 - Gestion des accès et cryptographie (ACC et CRY) / (ISO 9 et 10)

Les accès « logiques » aux systèmes informatiques, aux réseaux et aux données doivent être contrôlés afin de prévenir toute utilisation non autorisée.

9.1. Gestion des accès et responsabilités utilisateurs

La gestion des accès consiste à autoriser les accès aux ressources (applications, données, services, etc.) selon les utilisateurs et leur profil, au regard des actions qu'ils auront à réaliser (consultation, modification, suppression).

PSSI-ACC-01	Gestion de l'accès utilisateurs	
1. L'attribution d'un accès doit suivre une procédure formelle respectant la séparation des rôles entre la demande, l'autorisation et l'administration des accès (cf. PSSI-ORG-02 : Séparation des tâches). Une trace de la validation (mail ou formulaire) doit être conservée ; la mise en œuvre est traçable. 2. Les demandes d'accès à des données, systèmes ou applications doivent être formellement autorisées. 3. Les accès doivent être accordés sur la base d'un besoin justifié de l'actif. 4. Les identifiants d'accès doivent être uniques et nominatifs. 5. Les identifiants communs (ou génériques) ne doivent être autorisés que lorsque les aspects opérationnels et liés à l'organisation de l'activité l'exigent. Ces identifiants communs doivent être approuvés et documentés (cf. PSSI-PSI-02 : Dérogation) ; 6. Les autorisations d'accès sont accordées sur la base d'un besoin d'en connaître, conformément à la sensibilité des données. Les droits d'accès sont gérés par rôle, et par type d'action autorisée sur les données et ressources (création, consultation, modification, destruction) ; 7. Après validation d'un accès par le propriétaire, l'administrateur du système ou de l'application est averti pour l'attribution ou la modification des accès conformément aux directives du propriétaire de l'actif ; 8. Les accès (identifiants et autorisations) des utilisateurs qui ont quitté l'organisation ou dont les fonctions ont changé doivent être immédiatement désactivés puis supprimés (PSSI-RH-07 : Départ) ; 9. Les accès (identifiants et autorisations) des utilisateurs qui ont changé de fonctions doivent être adaptés (cf. PSSI-RH-06 : Mobilité interne) ; 10. Les accès (identifiants et autorisations) sont revus régulièrement, à minima 1 fois par an, avec le propriétaire de l'actif pour : - Contrôler les autorisations d'accès sur les systèmes, applications ou données sous sa responsabilité ; - Révoquer les droits des personnes n'ayant plus le besoin d'en connaître ; - Vérifier la conformité des droits d'accès avec les règles de sécurité (compte nominatif, besoin d'en connaître, étendues des droits). 11. Les accès au SI devraient être gérés à l'aide d'un annuaire centralisé (AD) et d'une solution SSO.		

PSSI-ACC-02	Sécurité des mots de passe	
1. La sécurité des mots de passe est définie par le PSSI qui s'assure du suivi des recommandations de l'ANSSI en matière, et en demande l'application à la DSIN. 2. La DSIN applique ces recommandations via la politique des mots de passe qu'elle gère et met en œuvre. 3. La DSIN s'assure de la bonne application de sa politique des mots de passe, en la déployant sur les actifs qu'elle gère et en sensibilisant tous les utilisateurs par les chartes en vigueur (cf. PSSI-RH-03 chartes utilisateurs et administrateur du système d'information) ou par des communications et formations dédiées. 4. La politique des mots de passe est mise à jour autant que de besoin, est stockée dans la GED de la DSIN.		

PSSI-ACC-03	Responsabilité utilisateur	
-------------	----------------------------	--

1. L'utilisateur est responsable de la protection de ses codes d'accès (carte, login, mot de passe, etc.), et des accès à son compte (cf. PSSI-RH-03 : Charte). À ce titre :
 - Il doit choisir des mots de passe robustes et les modifier régulièrement ou selon la politique de mots de passe en vigueur ;
 - Il ne doit pas communiquer, à qui que ce soit et pour quelque raison que ce soit, ses codes d'accès (mots de passe, code PIN, etc.) ;
 - En cas d'initialisation ou de réinitialisation de son mot de passe par une autre personne (par un agent de la DSIN par exemple), il doit modifier son mot de passe dès que possible ;
 - Il ne doit laisser personne accéder à sa session de travail sur un poste, un serveur ou une application ;
 - Il doit verrouiller en permanence sa session de travail lorsqu'il s'absente de son bureau ;
 - En cas de suspicion de divulgation de ses codes d'accès, il doit les modifier immédiatement.
2. L'utilisateur remonte toute usurpation de son identité (avérée ou suspectée) à la DSIN.

9.2. Accès à privilèges

PSSI-ACC-04	Gestion et utilisation des accès à privilèges	
	1. Les comptes à privilèges sont : - Les comptes d'administration systèmes ou applicatifs ; - Les comptes avec des accès importants sur les répertoires critiques ; - Les comptes « techniques » utilisés par les systèmes. 2. L'attribution d'un accès à privilèges doit suivre une procédure formelle respectant la séparation des rôles entre la demande, l'autorisation et l'administration des accès (cf. PSSI-ORG-02 : Séparation des tâches). Une trace des actions de validation et des opérations de réalisation doit être conservée ; 3. Les demandes d'accès à privilèges doivent être formellement autorisées par le responsable hiérarchique et/ou le propriétaire de l'actifs, et le RSSI ; et validés par la hiérarchie (Directeur de rattachement) 4. Des identifiants dédiés et spécifiques « dit à privilège » doivent être créés et octroyés pour répondre aux besoins d'administrations ou de développement sur le SI. Un compte utilisateur standard ne doit pas être utilisé pour réaliser des tâches nécessitant des accès à privilèges ; 5. Des mesures particulières doivent être appliquées pour sécuriser les identifiants à privilèges génériques : - Un responsable (propriétaire) doit être clairement identifié pour les identifiants à privilèges génériques ; - Le mot de passe devrait être renouvelé lorsqu'un utilisateur privilégié qui avait connaissance du mot de passe de ce compte quitte l'organisation. 6. La politique de mot de passe est renforcée pour les comptes à privilèges ; elle se rapporte aux exigences « PSSI-ACC-01 Sécurité des mots de passe » de la présente PSSI. 7. L'utilisation d'un compte à privilèges doit uniquement se faire sur un environnement d'administration dédiée à cet usage (l'utilisation d'un compte à privilège ne doit pas se faire sur un poste de travail bureautique standard) ; 8. Pour les comptes techniques utilisés par les systèmes, un responsable doit être identifié pour la configuration du compte, des informations d'identification et la sauvegarde de ce compte. 9. Un inventaire complet des comptes à privilèges doit être réalisé et revu régulièrement pour le maintenir à jour et vérifier la nécessité de révoquer l'attribution de droits à privilèges.	

9.3. Accès à distance et aux solutions Cloud

PSSI-ACC-05	Accès à distance
1. Une solution VPN doit être utilisée pour protéger les flux en confidentialité et intégrité, lors de l'accès externe au SI interne du SILA ; 2. La solution VPN utilisée pour accéder au SI interne du SILA, doit permettre d'authentifier le terminal de l'utilisateur qui doit appartenir à la collectivité ainsi que l'utilisateur ; 3. L'authentification double facteur est obligatoire pour se connecter au SI du SILA via le VPN ;	

PSSI-ACC-06	Accès aux solutions Cloud
1. Pour renforcer le contrôle d'accès des utilisateurs distants aux solutions cloud de la collectivité (SaaS, PaaS et autre hébergement) une solution d'accès conditionnels doit être mise en œuvre avec une fédération des identités. Cette solution doit permettre, suivant les cas, d'authentifier au moins un des éléments suivants : - Le terminal de l'utilisateur qui doit appartenir à la collectivité ; - L'utilisateur par l'activation d'une solution multi-facteur ; - Mot de passe stocké dans un gestionnaire de mot de passe recommandé par l'ANSSI ; - La localisation géographique qui doit correspondre à la France.	

9.4. Cryptographie – chiffrement

La cryptographie constitue une technologie permettant d'assurer un niveau de sécurité élevé pour les informations stockées ou échangées sur les SI, sous réserve que :

- Les outils et algorithmes soient choisis de manière adaptée (exemple : désactivation des algorithmes faibles sur les systèmes proposant différents niveaux à sélectionner lors de la phase de négociation client – serveur) ;
- L'implémentation des algorithmes soit effectuée de manière robuste (exemple : caractère aléatoire des vecteurs d'initialisation) ;
- La longueur des clés soit suffisamment élevée pour résister aux attaques de type « brute force » ;
- La gestion des secrets permette d'assurer leur disponibilité et intégrité face à tout événement (sauvegarde, séquestre, etc.), ainsi que leur confidentialité à tout instant.

PSSI-CRY-01	Sécurité des mécanismes cryptographiques
1. La robustesse des algorithmes et la longueur des clés cryptographiques doivent présenter un niveau de robustesse au moins équivalent au niveau de robustesse standard défini par l'ANSSI ; 2. Le PSSI doit approuver les outils et les méthodes utilisés pour les mécanismes cryptographiques. 3. Pour chaque mécanisme cryptographique, les propriétaires des actifs doivent définir avec le PSSI les besoins de restauration des clés ou des données en cas de perte. Dans ce cas, les moyens de restauration doivent être placés au séquestre (physique ou logique, mais déconnecté des réseaux) ou à défaut dans un SAPM pour en assurer la protection en confidentialité, intégrité et disponibilité.	

10 - Sécurité opérationnelle (EXP) / (ISO 12)

On entend par sécurité opérationnelle, la sécurité informatique des systèmes en exploitation. Il est ici question du maintien en conditions opérationnelles (MCO) et du maintien en condition de sécurité (MCS) de tous les actifs de l'IT et de l'OT.

10.1. Procédures et responsabilités opérationnelles

PSSI-EXP-01	Maitrise des actifs en exploitation
1. Les actifs en exploitation, utilisés par les utilisateurs doivent être fournis par le SILA et être validés par la DSIN ; 2. Il est interdit d'utiliser un matériel personnel pour accéder aux données du SILA, sauf exception explicite de la DSIN et du RSSI (cf. PSSI-PSI-02 : Dérogation) ; 3. Seuls les supports amovibles liés aux métiers, fournis ou préalablement autorisés par la DSIN, peuvent être connectés sur les équipements informatiques du SILA ; 4. Tout poste de travail doit être masterisé et installé selon une configuration standard validée par la DSIN ; 5. L'installation et la mise à jour des logiciels et applications en exploitation doivent être réalisées par les administrateurs qualifiés de la DSIN. Les utilisateurs ne doivent pas pouvoir installer de logiciels sur leur poste de travail sauf autorisation de la DSIN et à travers une solution de gestion et de déploiement de logiciels mise en place par la DSIN ; 6. Les actifs autorisés sont inventoriés dans un registre ou consultable dans la solution de gestion et de déploiement de logiciels de la DSIN ; 7. Les utilisateurs ne doivent pas être administrateurs de leurs postes, sauf exception explicite de la DSIN et du RSSI (cf. PSSI-PSI-02 : Dérogation) ; 8. Un contrôle régulier des logiciels installés sur les postes de travail et serveurs doit être réalisé annuellement par la DSIN.	

PSSI-EXP-02	Documentation d'exploitation et cartographie
1. Les procédures d'exploitation et d'administration des SI doivent être documentées, tenues à jour et disponibles pour tout le personnel concerné ; 2. La DSIN doit établir et tenir à jour une cartographie technique et applicative qui doit préciser les datacenters, les architectures des réseaux informatiques du SILA, les points d'interconnexion avec Internet ou des réseaux de sensibilités différentes ainsi que les flux réseaux.	

PSSI-EXP-03	Gestion des opérations et supervision
1. Les caractéristiques des systèmes, des équipements réseaux et sécurité ainsi que des applications des SI doivent être supervisés afin de détecter les incidents dans les meilleurs délais et de réagir en conséquence ; 2. Les sources permettant d'identifier les incidents de sécurité doivent être supervisés afin de détecter ces incidents dans les meilleurs délais et de réagir en conséquence ;	

3. La réalisation des opérations d'exploitation doit être tracée, contrôlée et donner lieu à des comptes-rendus avec indicateurs de réussite ou d'échec ;
4. Les défaillances rencontrées doivent être identifiées, traitées et contrôlées. Une trace des opérations réalisées en conséquence de ces défaillances doit être conservée.
5. Les anomalies récurrentes doivent être identifiées pour donner lieu à un plan d'action spécifique de traitements.

PSSI-EXP-04	Gestion des changements	
	1. Les modifications apportées aux systèmes et aux applications en production, dès lors qu'ils impactent les utilisateurs du SI, doivent être effectuées dans un processus comprenant : - L'identification et l'enregistrement des changements importants ; - La planification et les tests des changements ; - L'évaluation des impacts potentiels dus aux changements, y compris les impacts sur la sécurité ; - Une procédure d'approbation officielle pour les changements proposés ; - Une communication sur les changements à toutes les personnes concernées avec le niveau de détail nécessaire ; - Des procédures de retour en arrière, avec les responsabilités et actions nécessaires pour l'annulation et la récupération suite à l'échec d'un changement ou face à des événements imprévus. 2. Les changements et les tests sur les systèmes en production doivent être effectués de manière contrôlée ; 3. S'ils sont nécessaires, tous les changements réalisés en production doivent s'effectuer systématiquement avec des procédures identifiées de retour en arrière ; 4. Une sauvegarde complète de l'environnement concerné doit être réalisée avant chaque changement majeur.	

PSSI-EXP-05	Gestion de la capacité	
	1. Les ressources des SI (capacité de calcul, mémoire vive, stockage) doivent être supervisées afin d'identifier les évolutions nécessaires des SI à court et moyen terme ; 2. Les tendances concernant l'utilisation des ressources des SI doivent être suivies afin d'identifier les besoins futurs et d'orienter les évolutions nécessaires des SI à moyen et long terme.	

PSSI-EXP-06	Gestion de l'obsolescence	
	1. Un inventaire des ressources obsolètes doit être réalisé, tenu à jour et suivi ; 2. Il doit être révisé de manière annuelle et tracé dans un document stocké dans la GED de la DSIN ; 3. Un plan de mise à jour ou suppression des ressources obsolètes doit être défini, appliqué et suivi. 4. Des mesures particulières d'isolement du reste du réseau et d'internet doivent être appliquées pour les ressources obsolètes.	

PSSI-EXP-07	Maintenance des matériels et logiciels	
-------------	--	--

1. Tous les matériels et logiciels doivent être installés et gérés par les administrateurs de la DSIN, sous garantie du fournisseur et avec un service de maintenance adéquat.

10.2. Protection des équipements

PSSI-EXP-08	Sécurité des configurations (Durcissement)
1. L'installation ou la mise à niveau d'actifs doit prendre en compte des règles de durcissement pour limiter leur surface d'exposition aux menaces. Les principales règles de durcissement à étudier pour chaque équipement sont : - Désinstaller les comptes par défaut ; - Désactiver ou contrôler les ports physiques inutilisés ; - Désactiver ou contrôler les supports amovibles, s'ils ne sont pas utilisés (USB, lecteur de carte, CD) ; - Désactiver les services non indispensables installés (logiciels, bibliothèques logicielles, outils, service web) ; - N'installer que les logiciels nécessaires et notamment pas d'outils de développement sur les serveurs de production ou stations opérateur ; - N'installer ou n'activer que les protocoles et services nécessaires ; - Éviter les choix proposés par défaut ; - Désactiver systématiquement les protocoles et fonctionnalités vulnérables et non sécurisés (serveur Web, FTP, etc.). En particulier, désactiver les protocoles de découverte automatique d'équipements ou de topologie après avoir vérifié qu'ils ne sont pas utilisés par des applications ; - Désactiver les modes de configuration et de programmation à distance sur les installations critiques ; - Appliquer des préconisations de durcissement des équipements et systèmes d'exploitation (exemple mis à disposition par les éditeurs, ANSSI, etc.) ; - Définir des droits d'accès stricts selon le besoin d'en connaître et le principe de moindre privilège ; - Chiffrer les données et les transferts de bout en bout ; 2. Les présentes règles de durcissement sont à intégrer dans les procédures d'installation et de mise à niveau de tout composant logiciel (applications, systèmes d'exploitation, firmware, etc.). 3. Les règles de durcissement sont consolidées et mise à jour dans un document annexe regroupant les bonnes pratiques de la collectivité en la matière.	

PSSI-EXP-09	Lutte contre les logiciels malveillants
1. Les équipements informatiques doivent être protégés contre les logiciels malveillants par des mesures de détection, de prévention et de récupération à l'aide d'une solution EDR. 2. La solution doit être managée par un prestataire externe en 24/7 qui alerte au besoin la DSIN par téléphone ou courriel ; 3. Les solutions contre les logiciels malveillants doivent notamment être paramétrées pour : - Effectuer des analyses régulières, en temps réel de détection et de traitement des fichiers malveillants sur les postes de travaux et les serveurs - Détecter et empêcher l'utilisation de sites web connus comme malveillants, et le téléchargement ou la réception de fichier malveillants (cf. PSSI-RES-04) ;	

- Détecter et traiter la réception d'emails malveillants ou non désirés (cf. PSSI-RES-05).
- 4. Les solutions contre les logiciels malveillants doivent être mises à jour régulièrement et contrôlées (cf. PSSI-EXP-03 : Opérations) ;
- 5. Les exceptions à la mise en place de solutions anti-logiciels malveillants doivent être officiellement approuvées au cas par cas par les administrateurs systèmes et le RSSI.
- 6. Les utilisateurs doivent être sensibilisés aux risques concernant les logiciels malveillants (cf. PSSI-RH-03 : Charte d'utilisation ou d'administration des systèmes d'information ; PSSI-RH-04 : sensibilisation des utilisateurs)

PSSI-EXP-10	Gestion des mises à jour de sécurité	
	1. La politique de mise à jour de sécurité doit être définie et formalisée pour identifier les mécanismes de veille de vulnérabilités et de mise à jour des composants logiciels, afin d'être en mesure de déployer efficacement les correctifs concernant les vulnérabilités. La politique de mise à jour devrait lister pour chaque composant : - Les responsabilités dans le processus de veille et de mise à jour ; - Le délai de réaction aux notifications relatives à d'éventuelles vulnérabilités ; - Les moyens utilisés pour obtenir, évaluer et déployer les mises à jour. 2. Un inventaire exhaustif et à jour des actifs et ressources concernés par cette politique doit être disponible pour gérer efficacement les vulnérabilités techniques. L'information nécessaire doit comporter : - L'éditeur du logiciel ; - Les numéros de version ; - L'état de déploiement ; - La personne responsable (propriétaire). 3. Il doit être révisé de manière annuelle stocké dans la GED de la DSIN ; 4. Les sources d'information sur les vulnérabilités publiques doivent être identifiées et surveillées pour les composants logiciels utilisés. Ces sources doivent permettre de relever les correctifs ou recommandations (site web des éditeurs, base de données des vulnérabilités publiques, sites web de CERT permettant de couvrir les vulnérabilités ; 5. Les mises à jour et les logiciels ne doivent être téléchargés que sur des sites fiables (privilégier le site de l'éditeur) ; 6. Une évaluation des mises à jour en termes d'impact sur le système doit être réalisée avant tout déploiement ; 7. Aucun composant ne doit être exclu de la politique de mise à jour. Si un composant logiciel ne peut pas être mis à jour une solution de contournement doit être mise en place. Si aucune solution n'est trouvée, il doit être isolé du reste du système d'information et d'internet ; 8. Une attention toute particulière devra être portée sur les composants à risques, notamment ceux cités ci-dessous : - Les composants d'infrastructure ou applicatifs exposés sur internet : les firewalls, les serveurs localisés en DMZ publique, les sites Web ... ; - Les composants logiciels faisant l'objet de nombreuses attaques : systèmes d'exploitation Microsoft et Linux, navigateurs internet, serveurs Web, applications bureautiques, autres applications Microsoft... 9. Pour ces composants, la politique de mise à jour minimale à appliquer doit être la suivante : - Un cycle mensuel doit être mis en œuvre pour identifier, tester et appliquer les correctifs sous un délai maximum de 2 mois. Un processus de surveillance doit être mis en œuvre afin d'identifier les vulnérabilités critiques et d'appliquer les correctifs dans les plus brefs délais.	

10.3. Protection des équipements mobiles

PSSI-EXP-11	Sécurité des terminaux mobiles
- La sécurité des postes nomades doit être renforcée par rapport à la sécurité des postes fixes : - Durcissement plus important des terminaux (cf. PSSI- EXP-07 : Durcissement) ; - Blocage maximum par le pare-feu local des connexions entrantes ; - Chiffrement complet du poste pour garantir leur sécurité en cas de perte ou de vol. - Un filtre de confidentialité doit être utilisé lors des déplacements ; - Une solution MDM doit piloter de manière centralisée la conformité des smartphones et tablettes à la politique de sécurité ; - Les mesures de sécurité suivantes doivent être appliquées sur les smartphones et les tablettes : - Verrouillage par code pin ; - Chiffrement du terminal. - En cas de perte ou de vol les smartphones ou tablettes doivent être effacés depuis le MDM. - Les règles de gestion du MDM sont décrites dans des documentations et procédures - Les terminaux mobiles de type smartphone ou tablettes ne doivent pas accéder au réseau local du SILA ; - Une sensibilisation particulière doit être réalisée auprès des utilisateurs sur les risques liés au nomadisme (PSSI-RH-04 : Sensibilisation)	

10.4. Sauvegarde et restauration

PSSI-EXP-12	Sauvegarde et restauration
- Les besoins de sauvegarde des données, des applications et des systèmes doivent être identifiés en tenant compte des besoins métiers, des besoins de sécurité, des exigences de continuité et de reprise d'activité ; - La stratégie de sauvegarde doit être basée sur les principes suivants : 3 copies de sauvegarde sur 2 supports différents dont 1 sauvegarde hors site en cas de sinistre et 1 copie locale pour restauration rapide ; - Les plans de sauvegarde doivent être définis avec une stratégie de sauvegarde (sauvegarde complète ou différentielle), la fréquence et le contrôle des sauvegardes. Le plan de sauvegarde suivant peut être appliqué : - Sauvegarde incrémentielle des données quotidiennement avec au minimum une rétention de 2 semaines ; - Sauvegarde complète chaque semaine avec au minimum une rétention de 1 mois ; - Sauvegarde complète chaque mois des données le nécessitant avec au minimum une rétention de 2 ans. - Les données stockées localement sur les postes de travail des utilisateurs ne sont pas sauvegardées, elles doivent être stockées sur des espaces réseau partagés pour être sauvegardées. Le stockage local des informations sur le poste de travail nomade est limité au strict nécessaire et doit être autorisé par la DSIN ;	

5. Les sauvegardes et les solutions de sauvegardes et restauration doivent être protégées au même niveau de confidentialité, d'intégrité et de disponibilité que pour les données, applications et systèmes qu'elles sauvegardent ;
6. Des mesures particulières de séparation et d'isolation des environnements de sauvegarde doivent être mise en œuvre pour éviter qu'une attaque réalisée sur l'environnement de production se propage sur l'environnement de sauvegarde et sur les données (cf. PSSI-RES-01) ;
7. L'ensemble des composants du système d'information (données, logiciels, applications, systèmes, configurations, système de sauvegarde) doivent être sauvegardés et externalisés pour permettre une reconstruction en cas de sinistre majeur (cf. PSSI-PCA-01) ;
8. Si la confidentialité des sauvegardes externalisées ne peut pas être assurée avec le même niveau que sur le système d'information, alors ces sauvegardes doivent être protégées par du chiffrement (exemple : si la protection physique des sauvegardes ne peut pas être assurée sur le site distant ou durant le transport vers le site distant) ;
9. Les sauvegardes doivent être stockées sur un emplacement distant, à une distance suffisante pour échapper à tout dommage causé par un sinistre sur le site principal ;
10. L'exécution des opérations de sauvegarde et de restauration doit être documentée, contrôlée et les défaillances rencontrées sont traitées pour garantir la disponibilité et l'intégrité des données sauvegardées. L'ensemble des opérations sont tracées et donnent lieu à des comptes-rendus avec indicateur de réussite ou d'échec (cf. PSSI-EXP-03 : Opérations) ;
11. Un test de restauration de chaque type de sauvegarde doit être réalisé au moins une fois par an. Les tests permettent de valider les procédures de restauration, de vérifier le temps requis et de tester la capacité de restauration sur des environnements séparés. Le compte rendu des tests est formalisé et conservé. Une validation métier peut être réalisée à cette occasion ;

10.5. Journalisation et supervision

PSSI-EXP-13	Journalisation des événements	
	1. Les journaux d'évènements enregistrant les activités de l'utilisateur, les exceptions, les défaillances et les événements liés à la sécurité doivent être activés, tenus à jour et revus régulièrement. Les besoins de surveillance doivent être alignés avec la criticité des systèmes ou leur exposition aux menaces. Les journaux suivants doivent notamment être activés : - Authentification des utilisateurs sur les systèmes et applications ; - Navigation internet et flux de messagerie ; - Activité des administrateurs et opérateurs ; - Évènements issus des solutions de sécurité (EDR ...). 2. Les journaux doivent contenir lorsque c'est pertinent : - Les identifiants de l'utilisateur, du terminal et son emplacement ; - La date et l'heure ; - Les tentatives d'ouverture de sessions, d'accès aux systèmes et aux données réussies ou avortées ; - Les modifications apportées à la configuration des systèmes et aux données ; - L'activation ou la désactivation des systèmes de sécurité. La politique de journalisation doit être stockée dans la GED du SILA ; 3. Les événements de sécurité doivent produire une alerte de sécurité à destination des administrateurs systèmes et réseaux ou au RSSI (cf. PSSI-EXP-03 : Opérations) ;	

4. Les informations journalisées doivent être conformes aux exigences légales applicables, notamment sur le stockage des données personnelles ;
5. Un système de journalisation centralisé devrait être mis en place ;
6. Les utilisateurs doivent être informés des différentes mesures de journalisation (cf. PSSI-RH-03 : Charte).

PSSI-EXP-14	Protection des journaux	
1. Les informations journalisées doivent être protégées contre les manipulations et les accès non autorisés ; 2. Les journaux ne doivent être accessibles qu'en lecture et aux seules personnes autorisées par le RSSI. Ces personnes doivent être sensibilisées à la protection de ces données (non-divulgaration, stockage dans un espace chiffré, destruction après utilisation) ; 3. Des mesures particulières doivent être appliquées pour que les administrateurs ne puissent pas effacer ou désactiver les journaux concernant leur activité. <i>Les événements de sécurité doivent être protégés à des fins d'investigation.</i>		

PSSI-EXP-15	Synchronisation des horloges	
1. Les horloges des SI doivent être synchronisées sur un serveur ayant une fonctionnalité dédiée au temps.		

11 - Sécurité des communications (RES) / (ISO 13)

11.1. Sécurité réseau

Le cloisonnement des réseaux permet de contrôler les flux d'informations en se basant sur les besoins d'accès des personnes, des fonctions et des processus. Ces objectifs sont :

- De faciliter le contrôle d'accès ;
- De mieux se protéger contre les intrusions ;
- De limiter les risques de fuites d'informations.

PSSI-RES-01	Cloisonnement et sécurité des réseaux internes	
1. Le réseau interne doit être cloisonné entre différents sous-réseaux ou VLAN ; 2. L'accès entre les différents domaines du réseau doit se faire par un pare-feu permettant de filtrer les flux ; 3. A minima, le cloisonnement doit se faire avec : - Des réseaux cloisonnés entre les sites distants ; - Un sous-réseau pour les systèmes industriels pour limiter les accès au système industriel aux seules personnes ou équipements autorisés ; - Un sous-réseau pour isoler les postes d'administration des équipements administrés et restreindre les flux vers les équipements administrés aux seuls flux initiés depuis les postes d'administration ;		

- Un sous-réseau de management pour isoler les équipements à administrer ;
 - Un sous-réseau pour l'AD ;
 - Un sous-réseau de sauvegarde et un sous réseau pour les journaux ;
 - Un sous-réseau pour les autres applications techniques ou d'exploitation (antivirus, patch management, gestion des configurations...) ;
 - Un sous-réseau pour les serveurs hébergeant les applications et bases de données. Ce réseau peut éventuellement être segmenté par services ou métiers pour limiter l'exposition des ressources aux seules personnes autorisées ;
 - Un sous-réseau bureautique pour les utilisateurs des équipements bureautique. Ce réseau peut éventuellement être segmenté par services ou métiers pour limiter l'exposition des ressources aux seules personnes autorisées ;
 - Un sous-réseau pour les imprimantes ;
 - Un sous réseau Wi-Fi professionnel dit interne et un sous réseau Wi-Fi Invité ;
 - Un sous-réseau DMZ pour les services nécessitant d'être accédés depuis l'extérieur et isoler le réseau interne d'internet.
4. Une politique de filtrage doit être mise en place afin de limiter les flux au strict minimum et assurer un filtrage sur les protocoles autorisés. La politique doit permettre de justifier la nécessité de chaque règle ;
 5. Les demandes d'ouverture de flux doivent être validées par le RSSI si la politique de filtrage ne permet pas de les justifier ;
 6. Une revue des règles en place doit être réalisée à minima semestriellement, documentée et stockée dans la GED ;
 7. L'utilisation de protocoles sécurisés devrait être privilégiée sur le réseau interne par rapport aux protocoles non sécurisés ;
 8. Une solution de contrôle d'accès au réseau (NAC) doit être installée et configurée

PSSI-RES-02
Sécurité sur les réseaux externes

1. Les services, applications et passerelles d'interconnexion exposés sur internet doivent être durcis et sécurisés correctement pour assurer leur robustesse vis-à-vis des attaques basiques. Des mesures de sécurité telles que des solutions PROXY, WAF, IDS/IPS doivent être envisagées suivant les cas ;
2. Une architecture spécifique basée sur le concept de DMZ doit être mise en place pour sécuriser les services nécessitant d'être accédés depuis l'extérieur et isoler le réseau interne d'internet ;
3. La sécurité de ces services doit être régulièrement contrôlée avec une solution de scan de vulnérabilités telle que proposée par l'ANSSI et corrigé le cas échéant-(PSSI-EXP-10 : Mise à jour) ;

Les informations transférées sur les réseaux publics doivent être protégées en intégrité et en confidentialité (chiffrement des communications).

PSSI-RES-03
Sécurité des réseaux sans fil

1. Le réseau sans fil invité doit être isolé du réseau interne (cf. PSSI-RES-01 : Cloisonnement) ;
2. Le réseau sans fil interne doit être isolé sur un sous-réseau dédié afin de filtrer les flux (ports et protocoles) venant de ce réseau et limiter strictement les accès vers les ressources nécessaires (cf. PSSI-RES-01 : Cloisonnement) ;

3. Pour les accès au réseau sans fil interne, l'authentification et le chiffrement doivent prendre en compte les pratiques à l'état de l'art ;
4. Les accès au réseau sans fil interne doivent être tracés.

11.2. Transfert et partage d'information

PSSI-RES-04	Sécurité des accès à internet
1. L'accès à Internet doit être réservé aux personnes ayant besoin d'en utiliser ; 2. Tout accès, d'un utilisateur depuis un équipement des SI, ou, d'un équipement des SI à Internet, doit s'effectuer via un proxy mis à disposition par la DSIN. 3. Des règles de filtrage doivent être appliquées sur le proxy Internet afin de protéger les SI des menaces externes (cf. PSSI-EXP-09 : Code malveillant) et de n'autoriser que les sites nécessaires à l'activité de la collectivité.	

PSSI-RES-05	Sécurité des flux de messagerie et des outils collaboratifs
1. Tout courrier électronique relayé, entrant ou sortant, doit faire l'objet d'une recherche de code malveillant dans son enveloppe, son message et ses pièces-jointes (cf. PSSI-EXP-09 : Code malveillant) ; 2. Les mesures de protection suivantes doivent être appliquées sur les outils collaboratifs : - Les comptes utilisateurs invités doivent être soumis à une authentification double facteur - Les partages extérieurs doivent être limités dans le temps ; 3. Seules les plateformes validées par la DSIN sont autorisées pour échanger des fichiers volumineux vers l'extérieur, sauf exception explicite du RSSI (cf. PSSI-PSI-02 : Dérogation) ; 4. Les utilisateurs doivent être tout particulièrement sensibilisés aux risques liés à l'usage d'internet et de la messagerie (cf. PSSI-RH-03 : Charte).	

11.3. Opérations de télémaintenance

PSSI-RES-06	Opérations de télégestion, télémaintenance ou télédiagnostic
1. Lorsque des opérations de télégestion, télémaintenance ou télédiagnostic sont nécessaires, les règles suivantes doivent être appliquées : - Les mesures d'accès à distance et aux solutions Cloud doivent être respectées (cf. PSSI-AAC-05 : Accès à distance) ; - La journalisation doit être activée, pour conserver la trace des interventions et des modifications apportées sur les systèmes (PSSI -EXT-13 ; PSSI-EXT-14) - Après un délai précis d'inactivité, la connexion doit être fermée ; - Les opérations de télémaintenance ne doivent être réalisées qu'à l'aide de protocoles sécurisés (notamment sur internet), assurant notamment l'intégrité et l'authenticité des échanges ; - Toutes ces opérations doivent être réalisées au travers d'un bastion d'administration ; - Seuls les flux requis pour les opérations à distance doivent être autorisés ; - Les comptes d'accès distants doivent être nominatifs ; - Les mots de passe de connexion doivent être changés régulièrement.	

2. De plus, pour les accès distants prestataires, leur utilisation doit être limitée au strict nécessaire. Pour cela les règles complémentaires suivantes doivent être appliquées :
 - La solution VPN utilisée pour accéder aux SI interne du SILA par le prestataire doit permettre d'authentifier l'utilisateur par l'activation d'une solution multi-facteur ;
 - Les comptes doivent être activés suite à la validation par le propriétaire de l'actif et/ou d'un administrateur systèmes et réseaux ;
 - Les comptes doivent être activés sur une période définie ;
 - Les comptes doivent être désactivés lorsqu'ils ne sont plus utilisés, ou lorsque le délai est dépassé.

Si un accès distant prestataire nécessite d'être ouvert en permanence, celui-ci doit être justifié et cadré (systèmes accessibles, protocoles utilisés, plage ou période d'intervention, etc.).
3. Les opérations de télégestion, télémaintenance ou télédiagnostic réalisées par des prestataires doivent faire l'objet d'exigences de sécurité encadrées contractuellement (cf. PSS-EXT-01 : Clauses de sécurité).

PSSI-RES-07	Engagements de niveaux de service	
1. Des engagements de niveaux de service répondant aux besoins de disponibilité, de performances et de continuité doivent être intégrés dans les contrats avec les fournisseurs de services réseaux.		

12 - Gestion des incidents de sécurité (INC) / (ISO 16)

PSSI-INC-01	Signalement et détection des incidents de sécurité	
1. Les sources permettant d'identifier les incidents de sécurité doivent être identifiées et surveillées. Ces sources peuvent être : - Les utilisateurs, les agents et contractant qui doivent être informés de leur devoir de signaler tout événement de sécurité ou comportement anormal, ainsi que les contacts et les moyens à utiliser pour remonter les signalements (cf. PSSI-RH-03 : Charte / cf. PSSI-RH-04 : Sensibilisation) ; - Les équipements de surveillance du système d'information (supervision ou autres alertes automatiques, cf. PSSI-EXP-03 : Opérations) ; 2. Les équipements de surveillance concernés par cette détection doivent être, à minima, les solutions de sécurité décrites ci-dessous : - Les solutions d'authentification utilisateurs ; - Les équipements participant à la protection périmétrique des sites (firewall, VPN) ; - Les solutions participant au filtrage de la navigation internet des utilisateurs. - Les solutions de protection type anti-virus (EDR) des postes de travail et serveurs.		

PSSI-INC-02	Réponse aux incidents de sécurité	
1. Une procédure de réponse doit être définie. Cette procédure doit notamment prendre en compte : - La qualification des incidents impactant la sécurité pour leur apporter une réponse et une investigation spécifique : - o Identification de la cause de l'incident avant toute action de correction ;		

- Mesures de confinement pour éviter la propagation d'une infection ;
 - Planification et mise en œuvre d'actions correctives et, le cas échéant, d'actions pour prévenir la résurgence (actions pour récupérer des informations ou corriger les systèmes, devant être effectuées avec rigueur, pour éviter la restauration d'informations infectées ou corrompues) ;
 - Communication vers les personnes concernées par l'incident ;
 - Collecte de preuves pour analyse ou dans le cadre d'une action judiciaire ou disciplinaire ;
 - Si nécessaire, déclaration de l'incident aux autorités compétentes.
- Les procédures d'escalade afin de réagir rapidement aux situations d'urgence et éventuellement activer les procédures de continuité ou de reprise d'activité.

La production de fiches réflexes est encouragée pour formaliser les meilleures réactions à adopter face à des incidents types (dysfonctionnement système, perte de service, virus, rançongiciel, déni de service, fuite de données, etc.). Ces fiches peuvent être complétées au fur et à mesure des réponses à incident pour enrichir la base et améliorer les prochaines réactions.

PSSI-INC-03	Capitalisation
1. Suite à la réponse à incident, les informations recueillies peuvent être capitalisées pour améliorer la sécurité du système informatique et la gestion des incidents. Cela peut inclure : - Des statistiques sur les incidents (indicateurs de suivi, communication) ; - La création ou la mise à jour de fiches réflexes ; - La correction de failles pouvant être généralisée sur d'autres équipements. - L'évolution du système d'information pour éviter des incidents récurrents ou à fort impact.	

13 - Sécurité des systèmes industriels (IND)

Bien qu'utilisant de plus en plus des technologies standardisées du système d'information traditionnel (ou IT), les systèmes industriels (OT) se différencient par le fait qu'ils pilotent des installations physiques (chaînes de production, énergie), mais n'ont pas été conçus pour faire face aux vulnérabilités qu'elles introduisent. Le SILA est classé comme Entité importante (EI) au regard de la norme européenne NIS 2, ajoutant des règles de sécurité informatiques spécifiques à son système industriel. A date, la directive n'est pas complètement retranscrite dans le droit français, aussi le présent document ne peut contenir l'ensemble des exigences de sécurité attendues au regard de cette norme.

PSSI-IND-01	Principes généraux sur la sécurité des systèmes industriels
La sécurité des systèmes industriels s'appuie sur les mêmes principes que ceux présentés pour le système d'information. Les principes essentiels à prendre en compte sont : 1. Les installations industrielles présentes dans les bâtiments doivent être cartographiées et les procédures de maintenance formalisées [cf. source] ; 2. La documentation doit être régulièrement mise à jour pour partager la connaissance de ces systèmes ; 3. Les différents utilisateurs des systèmes industriels et les privilèges qui leur sont accordés doivent être identifiés précisément ;	

4. Les équipements industriels doivent être durcis (cf. PSSI-EXP-08 : Durcissement) ;
5. Les réseaux industriels doivent être cloisonnés des réseaux du système de gestion (cf. PSSI-RES-01 : Cloisonnement) ;
6. La gestion des intervenants externes sur les systèmes industriels doit prendre en compte :
 - L'encadrement de la prestation par des clauses spécifiques dans les contrats en complément des exigences de la règle « PSSI-EXT-01 : clauses et engagement de sécurité ».
 - La traçabilité des actions réalisées sur les équipements industriels en complément des exigences de la règle « PSSI-EXT-05 : Maîtrise des interventions externes »,
 - Le contrôle des interventions externes à distance en complément des exigences de la règle « PSSI-RES-06 : Télégestion »

PSSI-IND-02
Sauvegarde et reprise des systèmes industriels

1. Des sauvegardes régulières doivent être réalisées sur les données nécessaires à la reconstruction du système après un sinistre (exemple : programmes, fichiers de configuration, firmware, paramètres de procédé, etc.) ;
2. Les sauvegardes doivent être externalisées en lieu sûr, pour se prémunir des risques physiques (incendies, intrusions physiques, etc.) ;
3. Les sauvegardes doivent être réalisées avant et après toute modification, y compris lorsque celles-ci ont été apportées « à chaud » ;
4. Les sauvegardes doivent être testées régulièrement pour contrôler les sauvegardes et entraîner les équipes à la restauration des équipements.

PSSI-IND-03
Sécurité des consoles de programmation

1. Les consoles de programmation sont des équipements nomades dédiés à la maintenance des équipements du système industriel. Les consoles de programmation doivent :
 - Être dédiées aux activités de maintenance et d'exploitation des systèmes industriels ;
 - Ne pas être connectées à Internet ;
 - Ne pas être connectées à d'autres systèmes que le système industriel ;
 - Appliquer les règles pour les terminaux mobiles ;
 - Appliquer les règles de durcissement de configuration et de renforcement des protections ;
 - Être stockées dans un local sécurisé ;
 - Être facilement identifiables (marquage visuel par exemple).
 - Être éteintes lorsqu'elles ne sont pas utilisées.

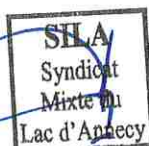
PSSI-IND-04
Supports amovibles sur les équipements industriels

1. Les supports amovibles (clés USB, disques durs externes, etc.) non maîtrisés ne doivent pas être connectés aux équipements industriels.

18 MARS 2026

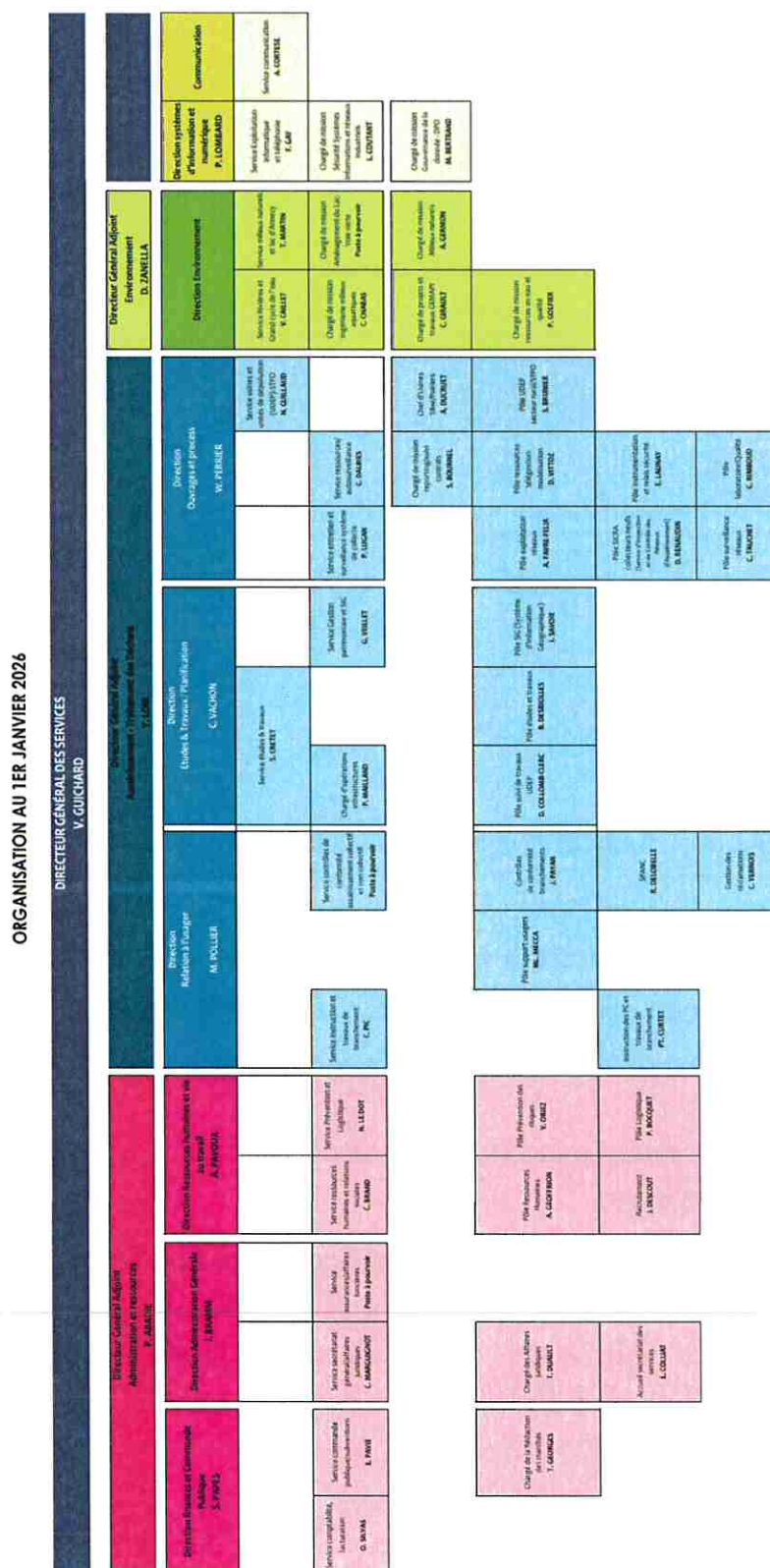
Fait à Annecy, le :

Le Président, Pierre Bruyère

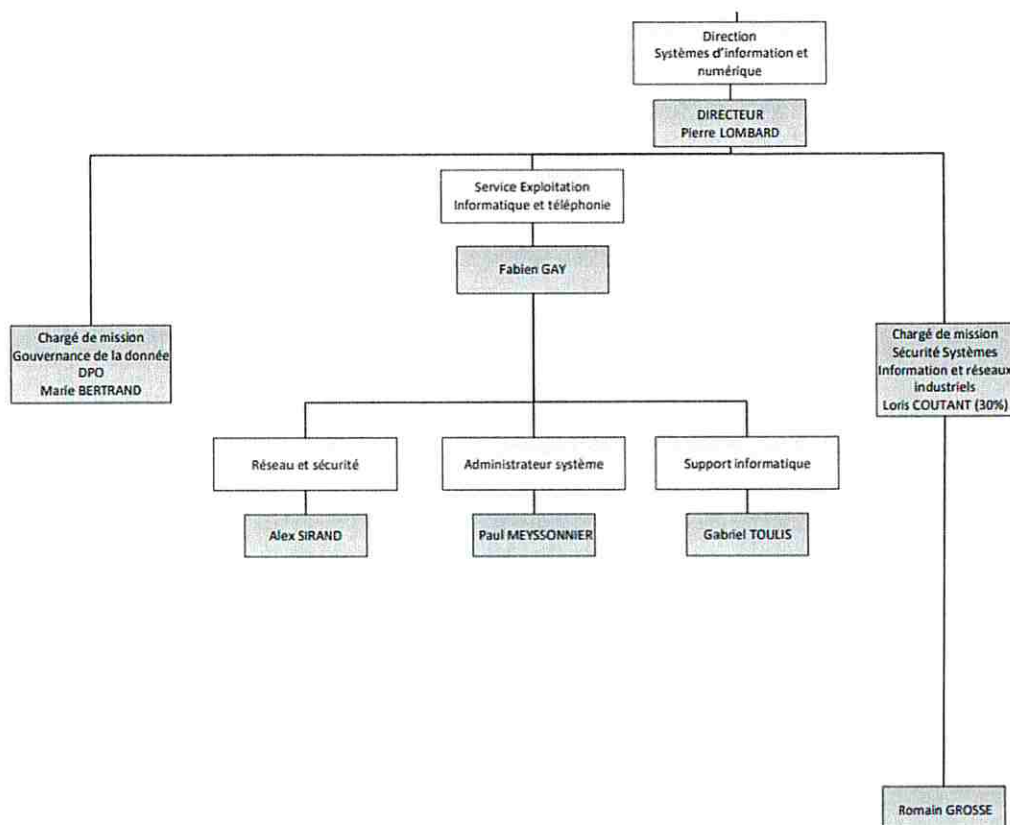


ANNEXES

1.1. ORGANIGRAMME GENERAL DES SERVICES DU SILA (01/2026)



1.2. ORGANIGRAMME DE LA DSIN (01/2026)



2. CADRE LEGAL REGLEMENTAIRE ET NORMATIF

[1] - Règlement et bonnes pratiques de l'ANSSI

<https://cyber.gouv.fr/guides-essentiels-et-bonnes-pratiques-de-cybersecurite-par-ou-commencer>

[2] – Guide d'hygiène informatique – renforcer la sécurité de son système d'information en 42 mesures , de l'ANSSI

https://messervices.cyber.gouv.fr/documents-guides/guide_hygiene_informatique_anssi.pdf

[3] - Normes ISO de la série 27000

- ISO/IEC 27001:2013 Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information – Exigences

- ISO/IEC 27002:2013 Technologies de l'information -Code de bonnes pratiques pour la gestion de la sécurité de l'information

<https://www.iso.org/fr/standard/iso-iec-27000-family>

[4] - Loi sur la protection des données (RGPD)

<https://www.cnil.fr/fr/reglement-europeen-protection-donnees>

[5] – Directive NIS2 sécurité des réseaux et des systèmes d'Information

<https://monespacenis2.cyber.gouv.fr/directive/>

[6] – Code du Patrimoine, Livre II

https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006074236/LEGISCTA000006129161/

[7] – Norme ISO 15489 -1 : Information et documentation – Gestion des documents d'activité

<https://www.iso.org/fr/standard/62542.html>

[8] – Norme ISO 14721 : Pratiques des systèmes de données spatiales -modèle de référence pour un système ouvert d'archivage d'information (SOAI) adaptation du modèle OAIS (Open Archival Information System)

<https://www.iso.org/fr/standard/87471.html>

[9] – LOI n° 2008-696 du 15 juillet 2008 relative aux archives

<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000019198529>



Bordereau d'acquittement de transaction

Collectivité : SILA D'ANNECY CRAN GEVRIER
Utilisateur : sila sila

Paramètres de la transaction :

Numéro de l'acte :	060_26
Objet :	Politique générale de sécurité des systèmes d'information du SILA
Type de transaction :	Transmission d'actes
Date de la décision :	2026-03-02 00:00:00+01
Nature de l'acte :	Délibérations
Documents papiers complémentaires :	NON
Classification matières/sous-matières :	5.7 - Intercommunalite
Identifiant unique :	074-247400013-20260302-060_26-DE
URL d'archivage :	Non définie
Notification :	Non notifiée

Fichiers contenus dans l'archive :

Fichier	Type	Taille
Enveloppe métier Nom métier : 074-247400013-20260302-060_26-DE-1-1_0.xml	text/xml	1 Ko
Document principal (Délibération) Nom original : 060-26_Politique générale sécurité systèmes information.pdf Nom métier : 99_DE-074-247400013-20260302-060_26-DE-1-1_1.pdf	application/pdf	172.4 Ko
Annexe (Projet de contrat avec l'organisme retenu) Nom original : PGSSI.pdf Nom métier : 73_CO-074-247400013-20260302-060_26-DE-1-1_2.pdf	application/pdf	1.4 Mo

Cycle de vie de la transaction :

Etat	Date	Message
Posté	16 mars 2026 à 16h19min12s	Dépôt initial
En attente de transmission	16 mars 2026 à 16h19min15s	Accepté par le TdT : validation OK
Transmis	16 mars 2026 à 16h19min17s	Transmis au MI
Acquittement reçu	16 mars 2026 à 16h19min24s	Reçu par le MI le 2026-03-16