Envoyé en préfecture le 26/12/2024
Reçu en préfecture le 26/12/2024
Publié le
ID : 017-211704150-20241219-2024_177-DE

SAINTES

CONSEIL MUNICIPAL DU JEUDI 19 DECEMBRE 2024

Délibération
DSIT/DD

2024 – 177 MISE EN PLACE DE LA POLITIQUE DE SECURITE DU SYSTEME D'INFORMATION AU SEIN DE LA VILLE DE SAINTES

Président de séance : DRAPRON Bruno, Maire

Etaient présents : 19
DRAPRON Bruno, CHEMINADE Marie-Line, CALLAUD Philippe, PARISI Evelyne, CREACHCADEC Philippe, TOUSSAINT Charlotte, BARON Thierry, CAMBON Véronique, DEREN Dominique, EHLINGER François, JEDAT Günter, CHANTOURY Laurent, ABELIN-DRAPRON Véronique, AUDOUIN Caroline, BENCHIMOL-LAURIBE Renée, MAUDOUX Pierre, ARNAUD Dominique, ROUDIER Jean-Pierre, CATROU Rémy

Excusés ayant donné pouvoir : 11
BERDAÏ Ammar à CAMBON Véronique, BUFFET Martine à PARISI Evelyne, CARTIER Nicolas à DRAPRON Bruno, DAVIET Laurent à JEDAT Günter, DEBORDE Sophie à TOUSSAINT Charlotte, DIETZ Pierre à BENCHIMOL-LAURIBE Renée, GUENON Delphine à ABELIN-DRAPRON Véronique, TERRIEN Joël à CHEMINADE Marie-Line, TORCHUT Véronique à BARON Thierry, MACHON Jean-Philippe à ROUDIER Jean-Pierre, MARTIN Didier à MAUDOUX Pierre

Absents excusés : 5
BETIZEAU Florence, CHABOREL Sabrina, DELCROIX Charles, MELLA Florent, VIOLLET Céline

Secrétaire de séance : JEDAT Günter

Date de la convocation : 12/12/2024

Le Conseil Municipal,

Vu le règlement européen 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,

Vu la directive européenne « Sécurité des réseaux et de l'information dite directive NIS1 » du 6 juillet 2016,

Vu la directive européenne « Sécurité des réseaux et de l'information dite directive NIS2 » du 27 décembre 2022,

Vu la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique,

Chaîne d'intégrité du document : C1 80 7A 35 34 83 43 BC BD CD 01 6F A2 3C 27 D4
Publié le : 26/12/2024
Par : Bruno DRAPRON
Document certifié conforme à l'original
https://publiact.fr/documentPublic/503922

Envoyé en préfecture le 26/12/2024
Reçu en préfecture le 26/12/2024
Publié le
ID : 017-211704150-20241219-2024_177-DE

SAINTES

Vu la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique,

Vu l'ordonnance n°2005-1516 du 8 décembre 2005 dite « ordonnance RGS » relative aux échanges électroniques entre les usagers et les autorités administratives et prévoyant le référentiel général de sécurité,

Vu la délibération n° CC_2024_151 du Conseil communautaire en date du 4 juillet 2024 par lequel Saintes Grandes Rives L'Agglo a approuvé la mise en place de de la Politique de Sécurité du système d'information,

Vu l'information transmise au Comité Social Territorial du mardi 26 novembre 2024,

Considérant les préconisations formulées par l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) pour renforcer le niveau de cybersécurité des administrations, des collectivités et des organismes au service des citoyens, tout en dynamisant l'écosystème industriel français dans le cadre du Plan France Relance,

Considérant que Saintes Grandes Rives, l'Agglo a souhaité s'inscrire dans cette démarche et a bénéficié du Parcours Cybersécurité avec l'accompagnement de l'ANSSI et du prestataire Terrain, la société ORNISEC,

Considérant que pour mener à bien les objectifs de protection des systèmes d'information de la Ville, il est nécessaire de mettre en place une Politique de Sécurité des Systèmes d'Information (PSSI) qui est le reflet de la vision stratégique de la direction en matière de sécurité des systèmes d'information,

Considérant que la PSSI se décline en deux documents :
- La PSSI Générale qui définit le cadre, l'organisation, les objectifs, les enjeux en matière de sécurité.
- La PSSI Opérationnelle, précisant les actions à mener dans le but de renforcer le niveau de protection des systèmes d'information.

Considérant que pour permettre une meilleure prise en compte par les utilisateurs de la PSSI, une charte informatique va être mise en place qui précisent notamment les droits, devoirs et obligations des utilisateurs vis-à-vis de l'utilisation des systèmes d'information de la Ville : Elus, Agents, Stagiaires, Administrateurs du Système d'Information (SI), Prestataires du SI,

Considérant qu'il appartient à l'assemblée délibérante de valider la politique de sécurité des systèmes d'information (générale et opérationnelle),

Considérant que les crédits nécessaires seront inscrits au budget principal,

Après consultation de la Commission « Ressources » en date du jeudi 5 décembre 2024,

Chaîne d'intégrité du document : C1 80 7A 35 34 83 43 BC BD CD 01 6F A2 3C 27 D4
Publié le : 26/12/2024
Par : Bruno DRAPRON
Document certifié conforme à l'original
https://publiact.fr/documentPublic/503922

Envoyé en préfecture le 26/12/2024
Reçu en préfecture le 26/12/2024
Publié le
ID : 017-211704150-20241219-2024_177-DE

SAINTES

Il est proposé au Conseil Municipal de délibérer :

- Sur l'approbation de la mise en place de la politique de sécurité des systèmes d'information (générale et opérationnelle),

- Sur l'autorisation donnée à Monsieur le Maire ou son représentant à signer tout document à cet effet.

Le Conseil Municipal,

Après en avoir délibéré,

ADOPTE à l'unanimité ces propositions.

Pour l'adoption : 30
Contre l'adoption : 0
Abstention : 0
Ne prend pas part au vote : 0

Les conclusions du rapport,
mises aux voix, sont adoptées.
Pour extrait conforme,

Le Maire,

MAIRIE DE SAINTES (Charente Maritime)

Bruno DRAPRON

Le secrétaire de séance,

Günter JEDAT

En application des dispositions des articles R.421-1 à R.421-5 du code de justice administrative, cette décision peut faire l'objet d'un recours en annulation par courrier ou par l'application Télérecours citoyens accessible à partir du site www.telerecours.fr devant le Tribunal Administratif de Poitiers dans un délai de deux mois à compter de sa publication.

SAINTES

Politique de la sécurité du système d'information de la Ville de Saintes

- PSSI-G -

Référence : VILLE_SAINTES_PSSI-G_V0r4

Date : Le 31 mai 2024

FICHE D'EVOLUTIONS

DIFFUSION

Récepteur	Entité ou Organisation	Nombre	Pour Action	Pour info
L'ensemble des collaborateurs de la DSIT de Saintes Grandes Rives, l'Agglo	**Ville de Saintes**			

MISE A JOUR

Version	Date	Auteur	Motifs
V0r1	04/03/2024	Marianne MILLOUR m.millour@ornisec.com	Initialisation
V0r2	14/03/2024	Marianne MILLOUR m.millour@ornisec.com	Modification
V0r3	09/04/2024	DSIT	Modification
V0r4	31/05/2024	DSIT	Modification

TABLE DES MATIERES

1. PREAMBULE

1.1. OBJECTIF DU DOCUMENT

Ce document constitue la Politique de Sécurité des Systèmes d'Information Générale (PSSI – G) de La Ville de Saintes. Il fixe les objectifs, l'organisation en matière de sécurité et les principes de sécurité applicables de façon transverse à tous les systèmes d'information de la Ville de Saintes.

Cette politique générale est rédigée et maintenue à jour par le Responsable de la Sécurité des Systèmes d'Information (RSSI) de la Ville de Saintes. Elle s'appuie sur les orientations stratégiques de la direction générale ainsi que sur la stratégie de traitement des risques qui pèsent sur les Systèmes d'Information de la Ville de Saintes.

La PSSI – G fait partie intégrante du référentiel cybersécurité de la Ville de Saintes.

1.2. PERIMETRE D'APPLICATION

La PSSI – G s'applique de façon transverse à toutes les directions et tous les systèmes d'information de la Ville de Saintes. Elle s'applique à l'ensemble des utilisateurs des systèmes d'information disposant d'un accès autorisé au système d'information.

1.3. ÉVOLUTION

La présente PSSI – G doit évoluer pour tenir compte des changements qui peuvent affecter les systèmes d'information et l'environnement, notamment en termes d'enjeux et de menaces. Elle doit en conséquence être mise à jour en fonction :

- Des évolutions de la réglementation ;
- Des nouvelles menaces et risques liés à l'évolution des technologies des systèmes d'information et à leur complexification ;
- Des évolutions des Systèmes d'Information ;
- Des résultats des audits concernant sa mise en application ;
- Des conclusions tirées des rapports de traitement des incidents.

La révision de la PSSI – G est réalisée, au minimum une fois tous les 3 ans, par le RSSI puis proposée à la Direction Générale pour validation.

1.4. DIFFUSION

La politique de Sécurité est un document interne de la Ville de Saintes. Il est communiqué à ses agents, ses administrés, fournisseurs et partenaires, lorsque c'est nécessaire et dès lors qu'ils sont acteurs des systèmes d'information.

Elle peut également être communiquée par le RSSI au cas par cas et sur demande écrite et justifiée à d'autres tiers extérieurs (exemple : organisations officielles, auditeurs externes, prestataires, etc.).

1.5. ENTREE EN VIGUEUR

La politique de sécurité est validée par la direction générale. Elle entre en vigueur dès diffusion à l'ensemble des agents.

Toutes les directions de la Ville de Saintes respectent les principes fondamentaux édictés dans cette politique générale ainsi que dans les différentes politiques de sécurité opérationnelles associées. Elles sont également contractuellement imposées aux partenaires et prestataires de la Ville de Saintes. Une charte leur sera transmise qu'ils devront signer puis retourner à la DSIT.

2. ENJEUX ET OBJECTIFS DE LA SECURITE DE LA VILLE DE SAINTES

2.1. LES ENJEUX EN MATIERE DE SECURITE

2.1.1. Sécuriser les SI : une nécessité

Les technologies de l'information pénètrent chaque jour un peu plus au sein de la Ville de Saintes, apportant autant de nouveaux services, de croissance, de progrès, de simplification et d'efficacité.

Le patrimoine informationnel manipulé par les systèmes d'information de la Ville de Saintes prend de plus en plus de valeur et le bon fonctionnement des services informatiques devient de plus en plus critique. Les incidents affectant la sécurité du système d'information sont de facto de plus en plus redoutés, d'autant plus que la menace est réelle, et que la surface d'exposition des SI aux cyberattaques augmente (exposition sur internet, nomadisme, interconnexions avec des tiers et prestataires, services accédés et déportés dans le nuage, etc.).

L'absence ou le manque de sécurisation du système d'information pourrait entraîner des conséquences sérieuses pour la Ville de Saintes :

- Dégâts matériels ;
- Perturbation, voire indisponibilité, des processus de l'établissement ;
- Fuite de données personnelles relatives aux agents et aux administrés ;
- Impact financier important suite à une manipulation frauduleuse des processus financiers de la Ville de Saintes ;
- Arrêt ou dysfonctionnement de certains process internes de la Ville de Saintes à des périodes critiques entraînant un impact opérationnel important sur les activités internes de la Ville de Saintes ;
- Divulgation de données sensibles internes, manipulées par les différentes directions de la Ville de Saintes et ses partenaires ;
- Atteinte à l'image de la Ville de Saintes ;
- Fuite de données personnelles relatives aux agents et aux administrés.

Il est donc nécessaire de protéger et de sécuriser les systèmes d'information de la Ville de Saintes, et ce à la hauteur des enjeux qu'ils représentent et en cohérence avec les risques et les menaces qui pèsent sur eux.

2.1.2. Sécuriser les SI : une obligation

Sécuriser les systèmes d'information de la Ville de Saintes est également une obligation pour s'aligner avec les évolutions du cadre juridique et réglementaire notamment :

- Le Règlement Général sur la Protection des Données (**RGPD**) relatif à la protection des données à caractère personnel ;
- Les engagements contractuels.

Dans la présente politique, le terme « loi, réglementation et engagements contractuels » fait référence aux lois et aux réglementations citées ci-dessus.

2.1.3. Sécuriser les SI : une opportunité

La sécurité des systèmes d'information est également appréhendée par la Ville de Saintes comme une opportunité lui permettant, d'une part, d'adopter sereinement les avancées technologiques, et d'autre part de renforcer la relation de confiance avec ses clients et partenaires.

Lorsque la sécurité est traitée en amont des projets, précisément gérée par des acteurs identifiés et avec l'engagement de la Direction, son coût peut être rationalisé et son retour sur investissement, certes indirect, peut être maximisé.

Le RSSI de la Ville de Saintes veille à la prise en compte de la présente PSSI dans les projets des systèmes d'information, en faisant mener les analyses de risques nécessaires, en décidant des mesures de sécurité techniques ou organisationnelles à mettre en place et en contrôlant leur application.

2.2. LES OBJECTIFS STRATEGIQUES EN MATIERE DE SECURITE

Afin de répondre aux enjeux de sécurité précédents, la Ville de Saintes a défini des objectifs stratégiques qui constituent la cible à atteindre en matière de sécurité des systèmes d'information :

- Permettre aux différentes directions d'assurer, même de façon dégradée, les activités métiers ;
- Être en mesure d'anticiper et de contribuer à la gestion coordonnée des situations de crise relatives aux systèmes d'information et celles susceptibles d'interrompre les activités de la Ville de Saintes ou de nuire à son image ;
- Respecter les lois, réglementations et engagements contractuels auxquelles sont assujetties les différentes directions de la Ville de Saintes ;
- Ne pas constituer une menace/un point de vulnérabilité pour le SI des partenaires ou de l'écosystème qui gravite autour de la Ville de Saintes ;
- Protéger son personnel, ses actifs, ses partenaires et ses clients contre toute forme de menaces, accidentelles ou intentionnelles ;
- Contribuer à la performance globale de la Ville de Saintes et préserver sa réputation et son image en tant qu'établissement public ;
- Faire de la sécurité un facteur d'opportunité et de croissance dans la création de nouveaux systèmes, notamment en anticipant les évolutions (nouvelles menaces, nouvelles technologies...) et en répondant aux attentes des directions, des élus et des partenaires.

Afin de satisfaire ses objectifs stratégiques, la Ville de Saintes définit un ensemble de politiques de sécurité opérationnelles qui proposent des règles et des mesures techniques. Ces politiques opérationnelles visent à garantir une protection efficace, rationalisée, proportionnée aux enjeux et améliorée dans le temps des activités et des processus de la Ville de Saintes.

Les politiques de sécurité opérationnelles sont élaborées sur la base des fonctions de sécurité ci-dessous :

- **L'Anticipation** : Anticiper l'occurrence de menaces et de risques, notamment les non-conformités réglementaires (Gestion des risques, Gestion de la conformité réglementaire, Gestion de la conformité avec les exigences contractuelles des partenaires, etc.) ;

- **La Protection** : Mettre en place des mécanismes de protection adaptés (Protection des actifs, Protection des biens supports, Protection des informations reçues de la part des partenaires, etc.) ;
- **La Détection** : Détecter les événements de sécurité pour se donner la capacité de réagir (Journalisation, Corrélation, Détection, etc.) ;
- **La Réaction** : Réagir face à des incidents de sécurité et reconstruire les actifs pour assurer une reprise d'activité dans les plus brefs délais (Gestion des incidents, Reprise d'activité, Retour à la normale, etc.) ;
- **L'Amélioration** : S'inscrire dans une logique d'adaptation dynamique des postures de sécurité et d'amélioration continue.

Le respect des politiques de sécurité opérationnelles est une obligation de tous les acteurs – internes et externes – de la Ville de Saintes, en lien direct ou indirect avec les systèmes d'information.

3. LE REFERENTIEL CYBERSECURITE DE LA VILLE DE SAINTES

Le référentiel cybersécurité de la Ville de Saintes est composé de trois niveaux :

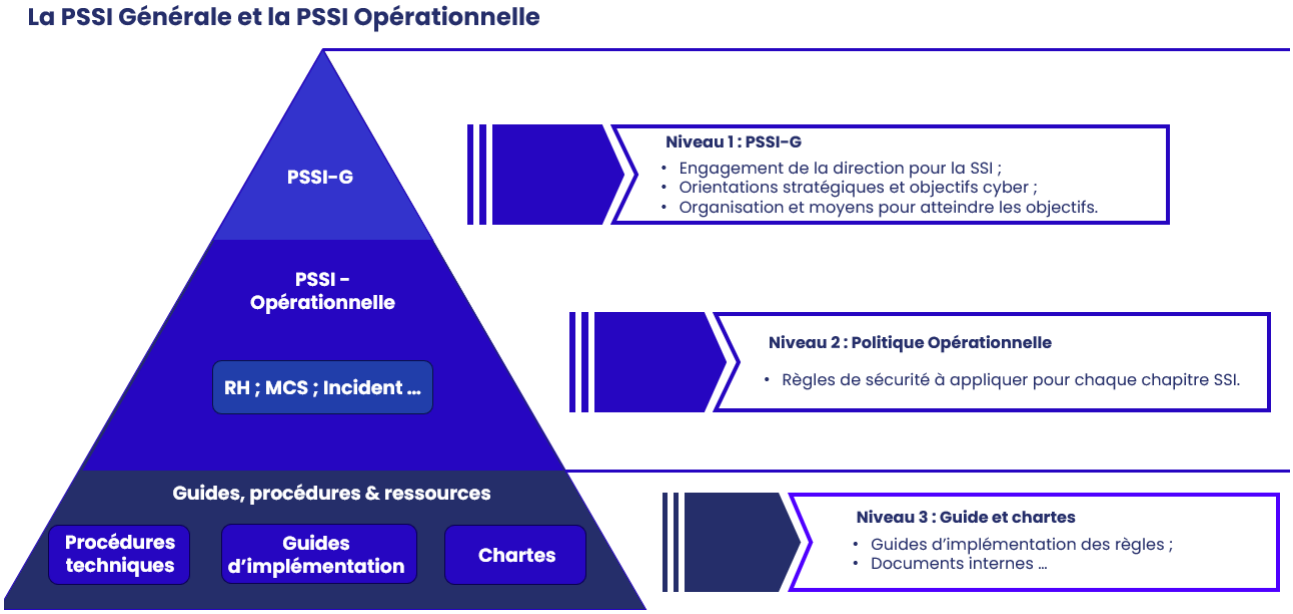

Figure 1 : Éléments constitutifs du référentiel cybersécurité

- **Niveau 1** : Définit la Politique de Sécurité des Systèmes d'information Générale applicable de façon transverse à l'ensemble des systèmes d'information de la Ville de Saintes (le présent document) ;
- **Niveau 2** : Définit les déclinaisons opérationnelles des objectifs stratégiques de la Ville de Saintes. Cette politique opérationnelle (PSSI – Opérationnelle) formalise les règles de sécurité applicables pour l'ensemble des systèmes d'information de la Ville de Saintes afin d'atteindre les objectifs stratégiques ;
- **Niveau 3** : Définit les guides et les méthodes proposées pour un déploiement correct et cohérent des règles de sécurité.

Ces politiques et procédures de sécurité sont issues d'une analyse des risques cybersécurité réalisée et régulièrement mise à jour par le Responsable de Sécurité des Systèmes d'Information.

Elles constituent le cadre de référence conçu pour atteindre les objectifs en matière de sécurité des SI. Elles traduisent la feuille de route que la Ville de Saintes entend suivre et faire prendre en compte par toutes les parties prenantes afin d'atteindre la cible définie en matière de sécurité.

4. ORGANISATION ET MANAGEMENT DE LA SECURITE DES SI

4.1. ROLES EN MATIERE DE SECURITE

4.1.1. Direction générale

La maîtrise et la gestion de la sécurité globale relèvent de la responsabilité première de l'autorité territoriale. Elle porte ainsi la responsabilité de la gestion des risques cybersécurité et des travaux de mise en conformité réglementaire. En effet, une délégation de pouvoirs à ce propos a été signée entre le Maire et la direction générale.

Cette responsabilité lui incombe de se doter des moyens et de l'organisation les plus adaptés pour gérer les risques et la conformité réglementaire relatifs aux systèmes d'information de la Ville de Saintes. À ce titre, la Direction Générale réalise, sur la base des travaux effectués par le RSSI, un arbitrage sur l'acceptation des risques et sur la conformité réglementaire et contractuelle, et décide les budgets et les moyens mis à disposition pour le programme sécurité.

La Direction Générale exprime son engagement en faveur du programme sécurité de la Ville de Saintes en :

- S'assurant que la politique et les objectifs sécurité sont établies et qu'ils sont compatibles avec l'orientation stratégique de la Ville de Saintes ;
- S'assurant que les ressources nécessaires pour la mise en place du programme sécurité sont disponibles ;
- Communicant sur l'importance d'une continuité d'activité efficace et de se conformer aux exigences de la politique de sécurité ;
- S'assurant que la politique de sécurité atteint les résultats et les objectifs escomptés ;
- Orientant et soutenant les personnes pour qu'elles contribuent à l'efficacité du programme sécurité et au respect des règles de la politique de sécurité ;
- Promouvant l'amélioration continue ;
- Aidant les autres directions et responsables concernés à démontrer leur engagement dès lors que cela s'applique à leurs domaines de responsabilité.

4.1.2. Responsable de la Sécurité des Systèmes d'Information (RSSI)

Le RSSI a la responsabilité, au sein de la direction des systèmes d'information, de conseiller et d'accompagner la Direction Générale dans la définition d'un programme sécurité, conformément aux risques identifiés, aux obligations légales et contractuelles, aux objectifs stratégiques, et d'en contrôler le respect tout en exerçant un rapport régulier pour assurer le suivi au plus haut niveau du programme.

Cette responsabilité se décline en missions d'expertise, de pilotage et de support :

- Concevoir la gouvernance et le cadre de référence de la sécurité (Politiques et Procédures de sécurité) et veiller à son déploiement ainsi qu'à sa bonne application au sein de toutes les directions de la Ville de Saintes ;
- Identifier et fournir la visibilité sur les risques / impacts majeurs ainsi que sur l'efficacité des capacités mises en œuvre pour les traiter ;

- Constituer un pôle d'expertise à même d'assister et de conseiller les directions sur les nouveaux usages et risques sécurité sur leur périmètre d'activité et les projets de la Ville de Saintes, pour leur permettre de répondre aux enjeux métiers en réalisant des analyses de risques, en proposant des mesures de sécurité pour traiter les risques identifiés et en contrôlant la bonne application des mesures de sécurité ;
- S'assurer de la correcte mise en œuvre des règles de la politique de sécurité, et de la prise en compte des aspects sécurité dans les actions et les projets menés au sein de chaque direction de la Ville de Saintes ;
- Contribuer au suivi et à la gestion des incidents de sécurité de la Ville de Saintes ;
- Gérer les évolutions des Politiques de Sécurité des Systèmes d'Information et de l'analyse des risques ;
- Participer à la sensibilisation et la formation des agents de la Ville de Saintes à la sécurité des SI ;
- Assurer le suivi régulier de l'application de la politique de sécurité vis-à-vis de la direction générale.

4.1.3. Délégué à la protection des données (DPO)

Le DPO a la responsabilité, au sein de la direction juridique, de conseiller et d'accompagner la Direction Générale dans la définition d'un programme de mise en conformité avec les exigences juridiques, techniques et sécurité du RGPD.

Le DPO a la responsabilité de contrôler le respect du programme de mise en conformité et d'exercer un suivi régulier à destination de la direction générale.

En particulier, le DPO a la responsabilité de réaliser, avec l'appui de la DSI et du RSSI, les analyses d'impact relatives à la protection des données (AIPD) et de contrôler l'application du plan de traitement des risques identifiés.

4.1.4. Directeurs et responsables de services

Chaque directeur et/ou chaque responsable de service a la responsabilité, au sein de son équipe, de sensibiliser les agents sur la nécessité de respecter les règles de la politique de sécurité des systèmes d'information.

Cette responsabilité se décline en mission d'appui et de support du RSSI :

- Reconnaître et soutenir le RSSI : intervenir pour légitimer le rôle du RSSI vis-à-vis de la direction ou du service ;
- Sensibiliser les agents pour l'application du référentiel de sécurité (PSSI, procédure, charte, etc.) ;
- Adopter un comportement ayant valeur d'exemple en respectant les mesures de sécurité de la PSSI ;
- Exercer une surveillance permanente et informer le RSSI de toute situation anormale ou présomption d'incident ou de comportement à risque ;
- Participer aux arbitrages réalisés par le RSSI en cas de contrainte organisationnelle ou technique au sein d'une équipe.

Les directeurs et/ou responsables de services sont également responsables des risques au niveau de leur périmètre. Ils valident le niveau de risques SI acceptable de chaque activité dont ils ont la charge, valident la mise en œuvre et font appliquer les mesures de sécurité des SI adéquates, en allouant les ressources en cohérence avec les objectifs et la PSSI.

Pour cela, les directeurs et/ou responsables de services s'appuient sur les travaux réalisés par le RSSI et le Délégué à la protection des données (DPO) pour obtenir les informations nécessaires afin de décider du caractère acceptable ou non des risques.

4.1.5. Utilisateurs internes

Chaque utilisateur interne du système (agents, prestataires, stagiaires, CDD, intérimaires …) respecte les règles de sécurité édictées par la PSSI et par la charte informatique, respecte les dispositifs et les mesures de sécurité, informe le RSSI de tout incident ou anomalie constatée.

4.1.6. Direction des systèmes d'information (DSI)

Les équipes de la DSI assurent le développement et le fonctionnement des ressources informatiques et de télécommunication. Ils mettent en œuvre les services de sécurité des SI et de contrôle, en conformité avec la PSSI et pour répondre aux exigences formulées par les directions et les départements métiers.

Ils définissent et mettent en application les plans d'action techniques pour :

- L'intégration des règles et mesures de sécurité des SI dans leurs activités ;
- L'intégration des mesures de sécurité en phase de conception de chaque projet (Security By Design) ;
- La détection et la réaction en cas d'incident informatique.

Les équipes de la DSI respectent les procédures internes, communes à toute la DSI, afin de garantir :

- Une cohérence des activités au sein de la DSI ;
- Un niveau de sécurité homogène entre les différents composants du SI, quel que soit l'équipe en charge de la mise en place et de l'exploitation en sein de la DSI ;
- Le respect des mesures de sécurité de la PSSI.

Par défaut, la DSI est le garant de l'application des mesures de sécurité pour tous les composants du système d'information de la Ville de Saintes. Lorsqu'un périmètre est géré par une autre direction pour des raisons organisationnelles ou techniques, un transfert de responsabilité est formalisé sous forme d'une attestation signée par les acteurs concernés.

Cette attestation précise :

- Le périmètre concerné : Description détaillée des composants du système concerné ;
- Les raisons justifiant le transfert de responsabilité ;
- Le responsable qui aura la charge du respect des règles de la PSSI : Le correspondant sécurité ;
- Les modalités de contrôle par le RSSI ;

Les signatures et leurs rôles/responsabilités : au minimum, le RSSI/DSI, le responsable de la direction concerné, et le « correspondant sécurité » désigné.

4.2. LE PILOTAGE DE LA SECURITE

4.2.1. Comité de pilotage de la sécurité des SI (COPIL)

Un comité stratégique de la sécurité des systèmes d'information se réunit une fois tous les 6 mois. Ce comité réunit le RSSI et le Directeur Général ou tout autre membre du comité de direction. Il permet d'assurer :

- Le suivi et l'amélioration continue de la sécurité au niveau de la Ville de Saintes ;
- Le suivi des règles de la politique de sécurité ;
- Le suivi des travaux de mise en conformité réglementaire et contractuelle ;
- Le suivi du niveau de risque qui pèse sur la Ville de Saintes ;
- La mise à disposition des ressources nécessaires pour assurer la conformité aux règles de la Politique de Sécurité des Systèmes d'Information ;

Le suivi et la revue des processus de sécurité (Gestion des risques, Gestion d'incident, Gestion de la continuité d'activité, etc.).

4.2.2. Comité technique de la sécurité des SI (COTECH)

Le comité de pilotage de la sécurité des systèmes d'information se réunit tous les mois. Ce comité réunit le RSSI et les éventuels acteurs de la Ville de Saintes concernés par les thématiques abordées. Les sessions de ce comité de pilotage sont l'occasion de :

- Suivre l'avancement et l'exécution des plans d'action de la sécurité des systèmes d'information ;
- Valider les mesures de sécurité proposées pour la gestion des risques ;
- Obtenir les arbitrages et orientations dans les choix concernant la sécurité des systèmes de la Ville de Saintes ;
- Assurer le suivi des indicateurs sécurité ;
- Discuter des contrôles et audits relatifs à la sécurité des systèmes d'information.

4.2.3. Tableaux de bord de suivi

Le pilotage de la sécurité implique la mise en place d'une structure de suivi et induit la mise en place de tableaux de bord. Ces tableaux de bord sont réalisés par le RSSI et sont présentés au comité de pilotage et doivent intégrer des indicateurs relatifs :

- Aux risques de sécurité ;
- Au niveau de déploiement de la politique de sécurité ;
- Aux incidents de sécurité rencontrés.

4.3. RELATIONS AVEC LES AUTORITES

Des relations appropriées avec les autorités compétentes sont entretenues par le RSSI et le DPO. Des procédures définissent :

- Quand et comment contacter les autorités compétentes ;
- Comment signaler dans les meilleurs délais les incidents liés à la sécurité de l'information (telles qu'une tentative d'intrusion ou une fuite des données à caractère personnel).

Les utilisateurs ne sont pas autorisés à contacter par eux-mêmes les autorités, sauf à y être autorisé du fait de leur fonction, à condition d'informer immédiatement leur responsable hiérarchique qui feront remonter l'information aux RSSI et DPO.

5. PRINCIPES & PROCESSUS DE SECURITE

La Ville de Saintes appuie la sécurité de ses systèmes d'information sur des processus permettant leur amélioration continue et leur ajustement à l'évolution des missions, du cadre réglementaire et des menaces pesant sur ses environnements numériques. Les principaux processus sont décrits ci-dessous.

Les processus de la présente politique, fixant un cadre général, se valent indépendants des technologies et des mécanismes de sécurité. Elles sont donc complétées par des instructions et mesures de sécurité, sous forme de politiques opérationnelles, qui déclinent au niveau opérationnel les principes fondamentaux.

5.1. GESTION DES RISQUES ET CONFORMITE

La Ville de Saintes prend en compte les risques pouvant affecter ses systèmes d'information à différents niveaux :

- **Risques stratégiques :** Une analyse des risques globale, qui couvre tous les périmètres de la Ville de Saintes, est élaborée et maintenue à jour. Elle propose une vision macro des risques qui pèsent sur les systèmes d'information et permet de formaliser les règles de la politique de sécurité de la Ville de Saintes ;
- **Risques propres à un système :** Si nécessaire, chaque sous-système d'information de la Ville de Saintes peut fait l'objet d'une analyse des risques spécifiques en prenant en compte le contexte et l'écosystème du périmètre étudié ;
- **Risques projets informations « Security By Design » :** Chaque projet doit faire l'objet d'une appréciation des risques SSI afin d'élaborer les objectifs sécurité du projet. Ces objectifs sont traduits en exigences sécurité, intégrées dans le cahier des charges et dont le bon respect est contrôlé par le RSSI.

La Ville de Saintes élabore et maintient à jour une étude de conformité avec les lois, réglementations et engagements contractuels. Les non-conformités sont identifiées, partagées avec la Direction Générale et associées à des plans d'action SSI.

Pour le cas particulier du Règlement Général sur la Protection des Données (**RGPD**), le RSSI maintient à jour l'étude de conformité conjointement avec le Délégué à la Protection des Données (DPO) de la Ville de Saintes.

5.2. SELECTION ET APPLICATION DES MESURES DE SECURITE

Les mécanismes de sécurité mis en place au sein de la Ville de Saintes sont issus :

- Du processus de gestion des risques ;
- Du processus de conformité avec les lois, réglementations et engagements contractuels ;
- Des politiques de sécurité internes.

Ces mécanismes sont sélectionnés par le RSSI conformément aux objectifs de sécurité fixés, en prenant en compte le contexte de la Ville de Saintes.

Les mesures de sécurité retenues, qu'elles soient de nature technique ou organisationnelle, sont alors applicables par toutes les parties prenantes des systèmes d'information de la Ville de Saintes.

La mise en place des mesures de sécurité techniques et organisationnelles est suivie par le RSSI au moyen de plan d'action SSI, régulièrement présentées à la Direction Générale lors des instances décisionnelles et de pilotage.

5.3. GESTION DES INCIDENTS DE SECURITE

Les incidents de sécurité sont identifiés, détectés, traités, évalués et leurs causes recherchées. Cette gestion est indispensable à l'amélioration continue de la sécurité ; elle est assurée par le RSSI, avec le concours des acteurs de la DSI et des parties prenantes des directions concernées.

5.4. AUDIT ET AMELIORATION CONTINUE

L'activité d'audit est primordiale pour vérifier la bonne mise en œuvre des démarches et mesures de sécurité décrites dans les différentes politiques de sécurité des systèmes d'information de la Ville de Saintes.

Des audits de sécurité sont réalisés tous les trois ans, particulièrement sur les activités essentielles de la Ville de Saintes.

Les audits de sécurité sont préparés, pilotés et analysés par le RSSI, en concertation avec les acteurs du système d'information concernés par le périmètre de chaque audit.

Les plans d'action d'audits sont proposés par l'auditeur en concertation avec le RSSI et validés par la Direction Générale. Le RSSI assure le suivi de la mise en place des plans d'action issues de chaque audit.

5.5. SENSIBILISATION ET FORMATION

Dans la sécurité, les comportements et la vigilance des personnes sont toujours un facteur majeur de succès ou d'échec. C'est un élément majeur de prévention de la survenue d'incidents et de limitation de ses impacts en cas de survenance.

La Ville de Saintes mène donc des actions de sensibilisation et de formation sous l'égide du RSSI.

5.6. ACCES PAR DES TIERS ET SOUS-TRAITANCE

Tout accès, qu'il soit physique ou logique, local ou à distance, aux ressources et informations de la Ville de Saintes par des tiers est accordé dans un cadre strict en fonction des besoins de la mission.

Les accès sont formellement approuvés par le collaborateur de la Ville de Saintes auquel ils sont rattachés et le RSSI, et fait l'objet d'un encadrement contractuel via la signature de la charte de sécurité informatique et la charte des prestataires pour les prestataires extérieurs.

Les intervenants externes travaillent sous la responsabilité d'un collaborateur de la Ville de Saintes.

5.7. POLITIQUE BYOD (BRING YOUR OWN DEVICE)

La connexion d'équipements personnels des collaborateurs au réseau interne de la Ville de Saintes n'est pas autorisée. Seuls les ordinateurs, les smartphones, les tablettes professionnel(le)s de la Ville de Saintes peuvent être connecté(e)s sur le réseau interne pour accéder aux ressources.

Politique opérationnelle de la sécurité du système d'information de la Ville de Saintes

- PSSI-O -

Référence : VILLE_SAINTES_PSSI-O_V0r3

Date : Le 31 mai 2024

FICHE D'EVOLUTIONS

DIFFUSION

Récepteur	Entité ou Organisation	Nombre	Pour Action	Pour info
DSIT de Saintes Grandes Rives, l'Agglo	**Ville de Saintes**			

MISE A JOUR

Version	Date	Auteur	Motifs
V0r1	04/03/2024	Marianne MILLOUR m.millour@ornisec.com	Initialisation
V0r2	09/04/2024	DSIT	DSIT
V0r3	31/05/2024	DSIT	DSIT

Table des matières

1. INTRODUCTION

1.1. OBJECTIF DU DOCUMENT

Ce document constitue la Politique de Sécurité des Systèmes d'Information – Opérationnelle (PSSI-O) appliquée aux systèmes d'information de La Ville de Saintes. Il propose une déclinaison opérationnelle des objectifs stratégiques de sécurité, représentés au niveau de la politique générale de sécurité des systèmes d'information, sous forme de mécanismes de sécurité applicables sur tous les systèmes d'information manipulés par la Ville de Saintes.

Cette politique est rédigée et maintenue à jour par le Responsable de la Sécurité des Systèmes d'Information (RSSI). Elle s'appuie sur les orientations stratégiques de la direction générale ainsi que sur des normes et réglementations nationales et internationales sur la sécurisation des Systèmes d'Information.

La PSSI-O fait partie intégrante du référentiel cybersécurité de la Ville de Saintes. Elle s'intègre au niveau 2 du référentiel suivant (Règle de sécurité opérationnelle) :

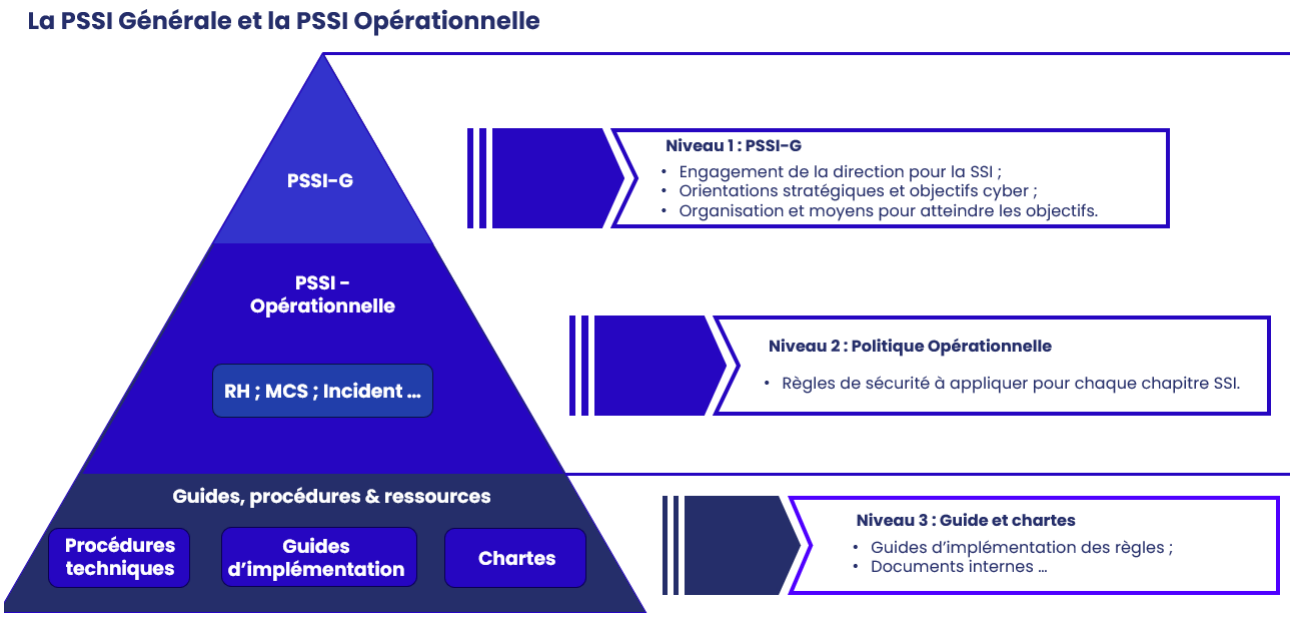

Figure 1 : Eléments constitutifs du référentiel cybersécurité

1.2. PERIMETRE D'APPLICATION

La PSSI s'applique de façon transverse à toutes les directions et tous les systèmes d'information de la Ville de Saintes. Elle s'applique à l'ensemble des utilisateurs des systèmes d'information de la Ville de Saintes disposant d'un accès autorisé au système d'information.

Le périmètre d'application de la PSSI-O inclut sans s'y limiter :

- L'ensemble des données, qu'elles soient sous forme électronique ou sous forme papier, y compris celles nécessaires à la DSI pour exploiter le système d'information (documentations, procédures, configurations),
- Les technologies incluant les systèmes d'exploitation, les logiciels, les supports stockage de données (clés USB, disques externes…), les serveurs, les réseaux, les appareils (PC, tablettes, smartphones, imprimantes, photocopieurs, systèmes permettant de convertir et de stocker les données…)

Les obligations des prestataires externes en matière de sécurité des systèmes d'information sont décrites dans :

- La charte de sécurité informatique de la Ville de Saintes pour les prestations extérieures, et dans les clauses contractuelles, et son annexe charte de confidentialité
- Les clauses sécurité SI intégrées dans les documents contractuels (CCAP, CCTP, CCP, marché publics, etc…)

1.3. EVOLUTION

La présente PSSI évolue pour tenir compte des changements qui peuvent affecter les systèmes d'information et l'environnement, notamment en termes d'enjeux et de menaces. Elle est mise à jour en fonction :

- Des évolutions de la réglementation ;
- Des nouvelles menaces et risques liés à l'évolution des technologies des systèmes d'information et à leur complexification ;
- Des évolutions des Systèmes d'Information ;
- Des résultats des audits concernant sa mise en application ;
- Des conclusions tirées des rapports de traitement des incidents.

La révision de la PSSI est réalisée, au minimum une fois tous les 3 ans, par le RSSI puis proposée à la Direction Générale pour validation.

1.4. DIFFUSION

La PSSI-O est un document interne de la Ville de Saintes. Il est communiqué aux agents, aux administrés et partenaires, lorsque c'est nécessaire et dès lors qu'ils sont acteurs des systèmes d'information.

Elle peut également être communiquée par le RSSI, au cas par cas et sur demande écrite et justifiée, à d'autres tiers extérieurs (exemple : organisations officielles, auditeurs externes, prestataires, etc.).

1.5. ENTREE EN VIGUEUR

La politique de sécurité est validée par le RSSI. **Elle entre en vigueur dès diffusion à l'ensemble des agents.**

Toutes les directions, départements et services de la Ville de Saintes doivent respecter les principes fondamentaux édictés dans cette politique ainsi que dans les différents guides et procédures de sécurité

associés. Elles doivent également être contractuellement imposée aux partenaires et prestataires de la Ville de Saintes quand cela est jugé nécessaire par le RSSI.

1.6. GESTION DES DEROGATIONS

Tout écart par rapport aux règles de la présente PSSI-O doit faire l'objet d'une demande de dérogation justifiée auprès du RSSI et accompagnée d'un plan d'action.

Après analyse, le RSSI émet un avis sur la demande de dérogation qui sera ensuite validée ou non par le Directeur Métier du périmètre concerné. Pour qu'elle soit applicable, une demande de dérogation est formellement validée par un membre de la direction de la Ville de Saintes, qui sera porteur du risque.

La durée de vie d'une dérogation ne doit pas dépasser 12 mois, et est revue à l'échéance pour :

- Valider sa mise en conformité ;
- La renouveler si nécessaire.

Lorsque l'écart ne peut pas être corrigé, une fiche d'acceptation de risque doit être formalisée par le RSSI et signée par le Directeur du périmètre concerné, qui sera porteur du risque.

2. SECURITE LIEE AUX RESSOURCES HUMAINES

Règle RHU-1	**Charte informatique** Tout utilisateur interne des systèmes d'information reçoit et signe la charte informatique dès son arrivée au sein de la Ville de Saintes

Cette charte est signée par tout utilisateur qui dispose d'un accès à une ressource de la Ville de Saintes. Cela concerne en particulier les collaborateurs, les prestataires et les stagiaires.

Elle précise en particulier les règles et clauses de sécurité des systèmes d'information au niveau de la Ville de Saintes que les utilisateurs doivent respecter, aussi bien pendant la durée du contrat qu'après leur départ.

Elle fait également référence **au processus disciplinaire** applicable en cas de violation de ces règles.

En termes de règles à respecter, la charte prend en compte les exigences des politiques de sécurité de la Ville de Saintes.

Règle RHU-2	**Charte des administrateurs** Tout administrateur des systèmes d'information reçoit et signe la charte des administrateurs.

La charte des administrateurs précise le devoir de respect de la confidentialité des données de la Ville de Saintes, du respect de la vie privée et plus généralement le cadre d'utilisation des privilèges d'administration.

Cette charte est signée par tous les agents prestataires ou stagiaires qui disposent des privilèges d'administration :

- Les administrateurs techniques qui disposent des droits d'administration sur les équipements d'infrastructure de la Ville de Saintes ;
- Les administrateurs métiers qui disposent des droits d'administration métier sur les applications de la Ville de Saintes.

Règle RHU-3	**Sensibilisation des utilisateurs du système d'information** Les utilisateurs des systèmes d'information de la Ville de Saintes sont régulièrement sensibilisés aux questions de sécurité des systèmes d'information, aux bons comportements à tenir.

Les utilisateurs sont au courant des menaces relatives aux mauvais usages et au non-respect des règles de base de la sécurité des systèmes d'information, en rapport avec leur utilisation quotidienne des moyens informatiques mis à leur disposition. Ils sont également informés des comportements à adopter en cas d'incident de sécurité, suspecté ou avéré.

Cela se traduit, en pratique, par :

- Des sessions de sensibilisation dispensées par le RSSI ou un expert sécurité ;
- Des campagnes d'e-learning de sensibilisation et de test des connaissances ;
- Des affiches de sensibilisation ;
- La diffusion des livrets ou des bulletins d'information ;
- L'identification des points de contact pour toute demande d'information relative à la sécurité ;
- Des moments d'échanges informels avec le RSSI ou tout autre membre de la Direction des systèmes d'information (DSI) ;
- La réalisation de tests de phishing.

Règle RHU-4	**Gestion des arrivées et des départs** Une procédure de gestion des arrivées et des départs des agents est formalisée et appliquée. Elle précise les responsabilités et les actions à réaliser en termes de sécurité des systèmes d'information.

Cette procédure liste l'ensemble des actions à mener en cas d'arrivée ou de départ d'un agent. Ces actions comprennent en particulier :

- Contrôle du casier judiciaire – B2 avant l'embauche : Pour les collaborateurs et les stagiaires ;
- Le processus d'accueil avec une sensibilisation sécurité ;
- La signature de la charte informatique ;
- La mise à disposition de la PSSI générale de la Ville de Saintes ;
- L'attribution ou la restitution des outils informatiques mis à sa disposition ;
- L'ouverture, la modification, la fermeture ou la désactivation de comptes informatiques et des droits associés ;
- La fourniture ou la restitution de moyens d'accès physique (clés, …) ;
- La restitution de documents sensibles au responsable hiérarchique.

Règle RHU-5	**Gestion des longues absences** Les accès aux ressources de la Ville de Saintes (Application, messagerie, etc.) sont désactivés pour les agents en longue absence.

En cas d'absence prolongée, d'au moins un mois, d'un agent d'au moins un mois et en fonction du contexte et du profil concerné, une étude est réalisée en concertation avec le département des ressources humaines pour analyser le besoin de désactiver temporairement ou non les accès aux ressources de la Ville de Saintes (Internes ou accessibles depuis internet, comme les services SAAS).

Les managers et le département des ressources humaines doivent notifier le RSSI pour les départs prolongés, d'au moins un mois (long congé payé, congé maladie prolongé, congé sans solde, la mise à disposition, etc.).

Règle RHU-6	**Processus disciplinaire** Un processus disciplinaire est défini et appliqué en cas de non-respect des obligations en matière de sécurité des systèmes d'information. Sera appliqué le processus disciplinaire prévu pour les agents de droits public et privé, se référant aux statuts de la fonction publique territoriale.

Au cas où il s'avèrerait qu'un agent a failli de manière délibérée à une ou plusieurs règles de sécurité dont il a pris connaissance à son arrivée, des sanctions seront prises à son encontre.

Règle RHU-7	**Formation des acteurs IT** Les agents de la DSIT sur le système d'information sont régulièrement formés aux bonnes pratiques sécurité liées à leurs activités.

Les agents de la DSIT pourront suivre différentes formations en fonction de leurs profils :

- Profil RSSI : Formation à la gestion de la sécurité des systèmes d'information sur le volet technique et organisationnel ;
- Profil administrateur système / réseau : Formation aux bonnes pratiques d'administration SI, principes d'architecture sécurité, défense en profondeur, durcissement des équipements sécurité et réseau, etc. ;
- Profil équipe support et poste de travail : Formation aux bonnes pratiques de sécurisation d'un parc informatique, durcissement des postes de travail, sécurisation via l'Active Directory, etc. ;
- Profil développement et projet : Security By Design, bonnes pratiques de développement sécurisé, les failles applicatives les plus connues et les mesures de protection (TOP10 OWASP - Open Web Application Security Project), etc.

3. SECURITE DE L'INFORMATION ET DES BIENS DES SYSTEMES D'INFORMATION

3.1. CARTOGRAPHIE ET CLASSIFICATION DES BIENS

Règle SIB-1	**Cartographie des biens** Tous les biens des systèmes d'information sont clairement identifiés et enregistrés dans une cartographie des systèmes d'information. Cette cartographie est mise à jour une fois par an et met en exergue les relations entre les biens. Un inventaire des composants matériels et logiciels est mis en place via un gestionnaire de parc informatique.

Conformément aux recommandations de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), la cartographie de la Ville de Saintes présente les quatre niveaux d'architecture :

- Architecture métier : Présentation des processus et informations métiers de chaque direction et service, présentation des blocs fonctionnels ;
- Architecture applicative : Présentation des blocs applicatifs, présentation du lien entre les blocs applicatifs et les processus / informations métiers associés ;
- Architecture logique : Présentation des zones réseau (LAN, VLAN, Interconnexion, Accès internet), présentation des équipements logiques, présentation des machines virtuelles, présentation du lien entre les machines virtuelles et les blocs applicatifs ;
- Architecture physique : Présentation des composants physiques du système d'information, présentation des sites, présentation des locaux techniques et salles serveur, présentation des interconnexions physiques entre les équipements, présentation des liens entre les équipements physiques et les équipements logiques.

Les biens comprennent :

- Les informations ;
- Les processus métier ;
- Les systèmes, les applications et les logiciels ;
- Les composants d'infrastructure : postes client, équipements mobiles, supports amovibles, équipements réseaux, serveurs, baies de stockage, etc. ;
- Les locaux.

Cette cartographie met en avant les relations entre ces biens afin de pouvoir :

- Classifier les biens supports selon les données et processus manipulés ;
- Identifier les vulnérabilités et les scénarios de menaces applicables à chaque bien.

Les relations types illustrées dans l'inventaire sont les suivantes :

- Une donnée est manipulée au sein d'un processus métier ;

- Un processus est rendu par des applications et systèmes au sein d'une direction ;
- Les applications et systèmes communiquent ensemble ;
- Les applications et systèmes s'appuient sur une infrastructure sous-jacente ;
- Les infrastructures sont hébergées physiquement dans des locaux.

Le rôle de « gestionnaire d'inventaire » est donné à un agent au sein de la Ville de Saintes pour s'assurer de la mise à jour régulière des informations sur les actifs.

Un inventaire des licences utilisées pour les composants matériels et logiciels existe et maintenu à jour par la DSI.

Un schéma réseau détaillé est tenu à jour et rendu accessible aux personnes habilitées.

L'inventaire des équipements matériels et logiciels et mis en place via un outil de gestion automatique de parc. Cet outil permet de collecter les informations sur les différents composants (en mode connecté, via un agent sur les Postes de travail et les serveurs, ou via le protocole SNMP pour les équipements réseaux) :

- Identifiant ;
- Adresse IP ;
- Marque ;
- Version ;
- Caractéristiques matérielles ;
- Information sur les firmwares et les systèmes d'exploitation ;
- Localisation de l'équipement.

Règle SIB-2	**Identification d'un responsable fonctionnel pour chaque bien** Un responsable fonctionnel est formellement identifié pour chaque bien essentiel (données et processus métier) des systèmes d'information.

Le responsable fonctionnel a pour responsabilité de :

- Classifier le bien et d'exprimer les besoins de sécurité associés ;
- S'assurer que le bien est inventorié ;
- Garantir l'exactitude des informations transmises au gestionnaire de l'inventaire ;
- S'assurer d'une gestion correcte des droits d'accès au bien.

Règle SIB-3	**Identification d'un correspondant sécurité pour chaque bien support** Un correspondant sécurité est formellement identifié pour chaque bien support non géré par la DSI.

Lorsque la gestion opérationnelle et sécurité (Maintien en Condition opérationnelle et Maintien en Condition de Sécurité) d'un composant du système d'information n'est pas sous la responsabilité de la DSI, un correspondant sécurité est formellement identifié lors de la mise en production du système.

Ce correspondant sécurité est désigné par le RSSI en concertation avec les équipes DSI, l'équipe utilisatrice et le responsable du département concerné.

Le correspondant sécurité a pour responsabilité de :

- Décliner les règles de la politique de sécurité de la Ville de Saintes au niveau du composant en prenant en compte les spécificités et les contraintes techniques et opérationnelles du composant ;
- Coordonner le déploiement des mesures de sécurité au niveau du composant ;
- Prendre en charge les mesures de sécurité opérationnelles (Durcissement, mise à jour de sécurité, analyser des alertes, gérer les incidents, contrôler les droits d'accès, etc.)
- Classifier le bien et d'exprimer les besoins de sécurité associés ;
- S'assurer que le bien est inventorié ;
- Garantir l'exactitude des informations transmises au gestionnaire de l'inventaire.

Règle SIB-4	**Classification des biens** Les données et processus, notamment les traitements des données à caractère personnel, sont identifiés et classifiés par rapport à leurs besoins en termes de confidentialité, d'intégrité et de disponibilité. Les autres types de biens héritent de cette classification selon leurs interdépendances avec les données et processus concernés (cf. SIB-1).

Les données et processus métiers font l'objet d'une analyse des risques dont le but est d'identifier leur criticité sur les critères de confidentialité, d'intégrité et de disponibilité.

Quatre niveaux de classification sont utilisés au sein de la Ville de Saintes :

Définition de l'échelle de classification	
01- Public	Le bien essentiel peut être communiqué publiquement.
02- Interne	Le bien essentiel peut être communiqué aux employés, tiers, partenaires, et autorités.
03- Confidentiel	Le bien essentiel ne peut être communiqué qu'à des personnes nominativement désignées et ayant le besoin d'en connaître.
04- Secret	Le bien essentiel ne peut être communiqué qu'en interne à des personnes habilitées.

Le niveau de classification est attribué par le responsable fonctionnel de chaque bien.

3.2. SECURISATION DES BIENS DES SYSTEMES D'INFORMATION

Règle SIB-5	**Mesures de sécurité adaptées au niveau de classification** Des mesures sont mises en œuvre pour assurer la confidentialité, l'intégrité et la disponibilité des biens essentiels. Ces mesures sont adaptées au niveau de classification définie dans la règle SIB-4.

La Ville de Saintes élabore et met en place un guide de sécurisation des biens essentiels, à destination des équipes de la DSI et des services particuliers (SIG…). Ce guide propose des mesures de sécurité de protection graduées en fonction de la classification des biens et du traitement réalisé.

Règle SIB-6	**Marquage des documents** Les supports d'informations portent de manière visible l'indication de leur niveau de confidentialité.

Les supports concernés par cette exigence sont les suivants :

- Les documents sous format électronique ou papier (.doc, .pdf, .ppt, etc.) ;
- Les supports de stockage (clés USB, disques durs, etc.) ;
- Les Interfaces Homme Machine des applications métiers.

En l'absence de marquage, le support est considéré de niveau « Interne ».

4. SECURITE DES ACCES AUX SYSTEMES D'INFORMATION

4.1. AUTHENTIFICATION ET AUTORISATION

Règle AUT-1	**Comptes personnels délivrés aux agents** Des comptes personnels sont fournis aux agents de la Ville de Saintes. Ils leur permettent de déverrouiller leurs postes de travail et d'accéder aux systèmes d'information dans la limite des droits d'accès qui leur sont alloués. L'utilisation de comptes génériques est interdite, dans la mesure du possible.

Conformément à l'état de l'art de la sécurité, aux lois et aux réglementations, tout compte d'accès aux ressources de la Ville de Saintes est nominatif afin d'assurer la non-répudiation des actions entreprises. L'utilisation des comptes génériques est interdite, dans la mesure du possible.

Règle AUT-2	**Maîtriser l'utilisation des comptes de service** Les comptes de service, attribués à des systèmes, des composants techniques ou des applications, sont gérés conformément à une procédure bien définie.

Cette procédure prend en compte les règles suivantes :

- Gérer de façon sécurisée les informations d'authentification relatives aux comptes de service ;
- Sécuriser le stockage des informations d'authentification : via un gestionnaire de mot de passe collaboratif ;
- Respecter la politique de mot de passe ;
- Respecter le principe du moindre privilège lors de l'attribution des droits aux comptes de service ;
- Établir un inventaire des comptes de services et des droits d'accès associés ;
- Réaliser des revues périodiques des droits attribués aux comptes de service ;
- Révoquer les droits associés à des comptes de service obsolètes.

Règle AUT-3	**Authentification et autorisation des utilisateurs** Tout accès non public à une ressource est protégé par une authentification et un contrôle de droit d'accès.

Aucune ressource, non publique, n'est exposée en interne ou en externe, sans authentification et contrôle d'habilitation.

Règle AUT-4	**Authentification double facteur** Les accès aux applications et services sensibles exposés sur internet sont protégés via un mécanisme d'authentification double facteur.

À titre d'exemple, l'interface d'administration des services cloud sensibles et les accès VPN sont protégés par une authentification double facteur.

Règle AUT-5	**Sécurité des mots de passe** Les mots de passe des utilisateurs, des comptes de service et des administrateurs respectent des règles minimales de complexité et sont gérés de manière sécurisée. Des mécanismes permettant la mise en œuvre et le contrôle automatique de ces règles sont mis en place.

Trois politiques de mot de passe sont formalisées et respectées au sein de la Ville de Saintes :

- Une politique de mot de passe pour les comptes utilisateurs ;
- Une politique de mot de passe pour les comptes administrateurs ;
- Une politique de mot de passe pour les comptes de service.

Règle AUT-6	**Gestion centralisée des comptes, de l'authentification et du contrôle d'accès** Un annuaire centralisé est utilisé pour gérer les comptes, les droits d'accès et l'authentification des agents de la Ville de Saintes.

Chaque application et système, interne ou externe, de la Ville de Saintes doit être connecté à l'annuaire central afin de :

- Gérer les comptes (Provisionning) : Ajout / Modification / Suppression d'un compte utilisateur ;
- Déléguer l'authentification : Authentification l'utilisateur, Gestion d'un mot de passe unique, mise en place du Single Signe On (SSO) ;
- Gérer le contrôle d'accès : Utilisation de groupe et de profil utilisateur, attribution des droits d'accès à une ressource en fonction des groupes/profils de l'utilisateur.

4.2. GESTION DES HABILITATIONS

Les droits d'accès aux ressources sont gérés suivant les principes suivants :

- **Besoin d'en connaître** : chaque utilisateur n'est autorisé à accéder qu'aux ressources nécessaires à l'accomplissement de ses missions ;
- **Moindre privilège** : chaque utilisateur accède aux ressources avec le minimum de privilèges lui permettant de conduire les actions nécessaires à ses missions ;
- **Séparation des tâches** : les droits d'accès incompatibles sont séparés en vue de limiter les impacts des mauvais usages, accidentels ou délibérés.

Règle GSH-1	**Procédure de contrôle d'accès** Une procédure de contrôle d'accès est formalisée et revue sur la base des exigences métiers et de sécurité de l'information afin de protéger la confidentialité, l'intégrité et la disponibilité des actifs.

Cette procédure concerne les accès aux systèmes, aux applications et aux répertoires réseau.

Règle GSH-2	**Définition d'une matrice des droits d'accès** Une matrice des droits d'accès est définie au niveau de chaque direction. Cette matrice est maintenue à jour par les responsables fonctionnels.

Cette matrice, basée dans la mesure du possible sur le modèle RBAC (Role Based Access Control), associe les profils métiers des agents aux droits d'accès nécessaires pour la réalisation de leurs fonctions.

Elle respecte le principe des moindres privilèges et de séparation des tâches.

Règle GSH-3	**Procédure d'attribution des droits d'accès** Toute attribution de droit d'accès à un utilisateur est effectuée dans le cadre d'un processus formel.

Le processus d'entrée des agents prévoit une attribution des droits d'accès aux systèmes d'information, conformément à la matrice et la procédure de contrôle des accès.

Toute attribution de droits supplémentaires est soumise au minimum à la validation du responsable de l'agent et du responsable fonctionnel du bien en question.

Règle GSH-4	**Revue régulière des droits d'accès** Une revue des droits d'accès aux systèmes d'information est réalisée au minimum une fois par an. Tout écart par rapport à la matrice des accès est supprimé ou justifié auprès du Responsable de la Sécurité des Systèmes d'Information.

En ce qui concerne les applications métiers, chaque responsable fonctionnel est tenu de réaliser annuellement une revue des droits sur les applications utilisées par son application. Cette revue des droits permet :

- De supprimer les comptes inutiles ;
- De supprimer les comptes dormants ;
- D'adapter les droits applicatifs des utilisateurs à leur mission.

Règle GSH-5	**Réexamen des droits d'accès en cas de changement de fonction** Tout changement de fonction ou de direction donne lieu à un réexamen systématique des droits d'accès à l'égard de la matrice des accès.

Règle GSH-6	**Suppression des droits d'accès** Le départ d'un agent donne lieu à une suppression de tous ses droits d'accès aux systèmes d'information et une désactivation de son compte.

4.3. GESTION DES COMPTES ADMINISTRATEURS ET DROITS A PRIVILEGE

Règle GSH-7	**Identification des droits à privilège** La liste des droits d'accès « à privilège » est définie, maintenue à jour et régulièrement vérifiée.

Ces droits correspondent aux accès jugés sensibles, dont un abus aurait un impact important sur la Ville de Saintes (ex. droits administrateurs, droits d'accès à des données confidentielles, etc.).

Règle GSH-8	**Comptes d'administration dédiés et nominatifs** Chaque administrateur, technique ou métier, dispose d'un compte d'administration dédié aux activités d'administration. Les comptes génériques d'administration ne sont pas utilisés.

Cela concerne :

- Les administrateurs métiers : Chaque administrateur métier d'une application de la Ville de Saintes dispose d'un compte dédié aux opérations d'administration. Ce compte est différent du compte utilisateur de l'agent, qui ne dispose pas de privilège d'administration. En fonction du besoin (utilisation de l'application ou administration), l'utilisateur utilise un compte ou l'autre.
  Les deux comptes de l'utilisateur sont deux comptes distincts au niveau de l'annuaire et chaque compte dispose d'un mot de passe différent.
- Les administrateurs techniques (DSI, IT, etc.) : Les administrateurs techniques des composants du SI disposent de plusieurs comptes d'administration en fonction de l'action réalisée :
  - Un compte dédié pour l'administration des postes de travail ;
  - Un compte dédié pour l'administration des serveurs, des équipements réseaux et des équipements d'infrastructure ;
  - Un compte dédié pour l'administration du contrôleur de domaine.

  Ces comptes d'administration sont propres à chaque administrateur, et sont distincts des comptes utilisateurs.

Règle GSH-9	**Attribution des droits à privilège** L'attribution des droits à privilège respecte le principe du moindre privilège.

Toute attribution de droits à privilège fait l'objet d'une vérification et d'une validation par le Responsable de la Sécurité des Systèmes d'Information.

Cette attribution respecte les principes suivants :

- Les administrateurs disposent du minimum de privilèges nécessaires pour la réalisation de leurs tâches ;
- Une revue régulière (tous les ans) de l'attribution des droits d'accès à privilège est réalisée.

5. SECURITE DES RESEAUX ET DES COMMUNICATIONS

5.1. SECURITE DES RESEAUX

Règle RES-1	**Disponibilité des ressources réseau** La disponibilité et la performance des ressources réseau sont garanties, surveillées et optimisées en adéquation avec les besoins métiers.

- Les besoins métiers sont définis pour chaque système et application ;
- Les capacités et l'utilisation du réseau de la Ville de Saintes sont surveillés afin de prévenir tout arrêt de service lié à une surcharge ou saturation ;
- Le réseau est optimisé en termes de bande passante et de redondance des connexions ;
- Les exigences de sécurité sont prises en compte dans les engagements contractuels avec les fournisseurs d'accès réseau.

Règle RES-2	**Contrôle d'accès des équipements sur le réseau** Un contrôle d'accès réseau (ex. 802.1x) est mis en œuvre pour interdire la connexion de tout équipement non fourni ou non expressément validé et configuré par la Ville de Saintes au réseau interne.

Seuls les équipements maîtrisés par la Ville de Saintes peuvent être reliés au réseau interne. Le raccordement sur le réseau de tout équipement informatique non maîtrisé est interdit.

Règle RES-3	**Cloisonnement des réseaux de la Ville de Saintes** Le réseau de la Ville de Saintes est découpé en zones cloisonnées physiquement ou logiquement. Ce découpage prend en considération la criticité des ressources concernées et les menaces auxquelles elles sont exposées.

Le découpage en zone est basé sur les trois critères ci-dessous :

- La sensibilité des composants de la zone (poste de travail, périmètre critique, base de données, serveur métier, réseau d'administration, etc.) ;
- L'exposition des composants de la zone (équipement accessible par une population non maîtrisée, équipement accessible depuis un espace public, équipement accessible en interne, équipement accessible depuis un local technique, etc.).

Règle RES-4	**Filtrage des communications** Tous les flux entre les zones sont filtrés et contrôlés par un dispositif de filtrage (Pare-feu). Une politique de filtrage est formalisée et mise en place pour contrôler et filtrer les accès entre les différentes zones réseau de la Ville de Saintes.

Seuls les flux strictement nécessaires sont autorisés. Les flux non explicitement autorisés sont bloqués par défaut.

Règle RES-5	**Sécurité des réseaux sans-fil** La Ville de Saintes met en place des règles de durcissement réduisant les risques inhérents à l'usage des réseaux sans fil.

Ces règles incluent en particulier :

- Mettre en place une authentification et un contrôle d'accès pour les communications sans fil ;
- Chiffrer les communications sans fil de manière à garantir une protection en matière de confidentialité et d'intégrité ;
- Limiter la puissance du signal des points d'accès des réseaux sans fil internes ;
- Cloisonner les différents réseaux sans fil et empêcher tout accès aux actifs internes de la Ville de Saintes :
    - SSID pour le wifi des visiteurs ;
    - SSID pour le wifi des agents ;
- Mettre en place une authentification, une journalisation et une demande de consentement pour les accès au réseau sans fil public conformément à la réglementation en vigueur.

Règle RES-6	**Sécurité des interconnexions avec les réseaux externes** Toute interconnexion entre les systèmes d'information de la Ville de Saintes et un réseau externe est maitrisée, sécurisée, surveillée et contrôlée.

- Une cartographie est établie en précisant les interconnexions avec les réseaux tiers, les mesures de sécurité et l'architecture mise en place ;
- Des audits de la sécurité de ces points d'interconnexion (avec internet et avec les réseaux des tiers) sont régulièrement menés ;
- Des outils de surveillance et de détection d'intrusion sont utilisés pour contrôler ses interconnexions;
- Les flux réseau sont limités au strict nécessaire ;
- Des pares-feux applicatifs peuvent être mis en place au besoin.

5.2. SECURITE DU RESEAU D'ADMINISTRATION

Règle RAD-1	**Mise en place d'un système d'information d'administration** L'administration des composants des systèmes d'information de la Ville de Saintes est effectuée depuis un réseau d'administration maîtrisé et cloisonné logiquement.

Le système d'information d'administration est composé de trois zones :

- Une ou plusieurs zones pour les ressources administrées en fonction de leur criticité. Ce découpage en zones de ressources administrées peut être déterminé conformément aux critères de cloisonnement présentés dans la règle RES-3 ;
- Une zone pour les postes d'administration.

Règle RAD-2	**Utilisation des postes d'administration dédiés** L'administration des composants des systèmes d'information de la Ville de Saintes est effectuée exclusivement depuis des postes de travail durcis et dédiés aux taches d'administration.

Chaque administrateur de la DSI dispose d'un poste de travail dédié aux opérations d'administration, qui est différent du poste de travail utilisé pour la bureautique.

Le poste de travail d'administration est :

- Utilisé exclusivement pour réaliser des opérations d'administration ;
- Durcis et sécurisé ;
- Déployé sur un VLAN dédié qui n'a pas accès à internet.

5.3. SECURITE DES COMMUNICATIONS RESEAUX

Règle COM-1	**Choix et dimensionnement des mécanismes de chiffrement** Les algorithmes utilisés ainsi que la longueur des clés sont définis et appliqués conformément à l'état de l'art et aux recommandations de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).

Règle COM-2	**Gestion des clés de chiffrement** Pour tout mécanisme de chiffrement, une procédure opérationnelle est formalisée pour préciser comment les clés sont demandées, générées, affectées, introduites dans les systèmes d'information, stockées, utilisées, renouvelées, recouvrées, détruites, voire archivées.

Règle COM-3	**Sécurité des communications réseaux** Les flux de communication sont protégés en fonction de la classification des données véhiculées et des menaces auxquelles elles sont exposées.

- Tout échange de données sur un réseau tiers (Internet en particulier) fait l'objet d'un chiffrement en vue d'assurer la confidentialité, l'intégrité et l'authenticité ;
- Les accès distants sont protégés en confidentialité et en intégrité via la mise en place d'un lien VPN / IPSec ;
- Tout flux ou échange de données confidentielles est chiffré ;
- Tout flux ou échange d'information d'authentification est chiffré ;
- Tout échange par email de données confidentielles est chiffré ;
- Tout flux d'administration est chiffré ;
- Les certificats auto-signés ne sont pas utilisés.

Règle COM-4	**Sécurité des échanges avec les tiers** Seuls les modes et les protocoles de transfert d'information sécurisés (SFTP, HTTPS, etc.) sont employés pour les échanges de données avec les clients et les tiers. Si ces canaux sécurisés ne sont pas disponibles, les informations échangées sont chiffrées.

La solution Zed ! est utilisée pour chiffrer les données.

5.4. SECURITE DES ACCES DISTANTS

Règle SAD-1	**Administration à distance des ressources internes** Les flux d'administration qui transitent sur un réseau tiers sont protégés en confidentialité et en intégrité via un tunnel VPN/IPSec.

Ceci concerne à la fois les accès des administrateurs internes et des prestataires.

6. SECURITE LIEE A L'EXPLOITATION DES SYSTEMES D'INFORMATION

6.1. PROCEDURES OPERATIONNELLES D'EXPLOITATION

Règle POE-1	**Documentation des procédures d'exploitation** Les procédures d'administration et d'exploitation des composants des systèmes d'information sont formalisés et régulièrement mises à jour par la DSI.

Des procédures documentées (procédures d'exploitation, d'administration des serveurs et des applications, de gestion des connexions réseau, etc.) sont rédigées par les membres de l'équipe DSI, pour une meilleure gestion des opérations et une meilleure administration des systèmes.

Ces procédures sont également utilisées pour :

- Faciliter le transfert de compétence en cas de recrutement d'un nouveau collaborateur ;
- Garantir une continuité d'activité en cas de départ d'un collaborateur.

6.2. SECURITE DES EQUIPEMENTS

Règle SEQ-1	**Durcissement des configurations** Une configuration de référence est définie et appliquée pour chaque type de composant informatique (Firmware, Systèmes d'exploitation, Logiciels, Applications), intégrant des règles de durcissement du niveau de sécurité.

Ces équipements comprennent en particulier :

- Les postes de travail ;
- Les imprimantes et copieurs ;
- Les serveurs ;
- Les middlewares (serveur d'application, base de données, etc.) ;
- Les équipements réseaux (routeurs, commutateurs, etc.) ;
- Les équipements de sécurité (firewall, antivirus, etc.) ;
- Les environnements de virtualisation ;
- Les services d'infrastructure et applicatifs (AD, WSUS, etc.).

En particulier, l'installation des serveurs et des postes de travail est effectuée depuis un master sécurisé.

Règle SEQ-2	**Droits des utilisateurs sur les postes de travail**

	Les agents de la Ville de Saintes ne disposent pas des droits d'administration sur leurs postes de travail.
Règle SEQ-3	**Mise au rebut des supports informatiques** Les supports qui ne sont plus utilisés sont mis au rebut de manière sécurisée en suivant une procédure formelle. Les données contenues sur des supports informatiques devant être mis au rebut sont détruites de manière irréversible.

Tout matériel contenant des supports de stockage est vérifié pour s'assurer que toute donnée confidentielle a bien été supprimée et que tout logiciel sous licence a bien été désinstallé de façon sécurisée.

En particulier, les mesures suivantes sont respectées :

- Suppression des données via des techniques irréversibles avant mise au rebut des supports ;
- Stockage des supports mis au rebut dans un local sécurisé ;
- Extraction des disques dur et de la RAM avant la récupération d'un matériel par un tiers (prestataire, association, revendeur, etc.).

Règle SEQ-4	**Utilisation des supports amovibles** L'utilisation des supports amovibles au sein de la Ville de Saintes est cadrée en vue de se protéger des menaces associées.

En particulier, les règles suivantes sont respectées :

- Distribuer, dans la mesure du possible, des supports amovibles à l'ensemble des agents ;
- N'autoriser que l'utilisation des supports amovibles gérés et référencés par la Ville de Saintes ;
- Désactiver l'exécution automatique des supports amovibles sur les postes de travail et effectuer une analyse antivirus et antimalware forcée ;
- Limiter l'utilisation des supports amovibles au transfert des données et éviter le stockage permanent;
- Sécuriser la restitution, la réaffectation et la mise au rebut des supports amovibles.

Règle SEQ-5	**Chiffrement des postes de travail** Les disques durs des postes de travail sont chiffrés pour protéger leur contenu en cas de vol ou de perte.

Règle SEQ-6	**Changement des mots de passe locaux** Les mots de passe d'administration locale des postes de travail et des serveurs sont régulièrement mis à jour via des solutions automatisées (Windows et Linux).

Règle SEQ-7	**Blocage des sites malveillant** Les modules de blocage des sites malveillant sont activés au niveau du pare-feu, pour les postes de travail internes.

Règle SEQ-8	**Mise en place de LAPS** Les postes de travail intègrent le module de sécurité LAPS.

6.3. SECURITE DES APPAREILS MOBILES

Règle MOB-1	**Sécurité des téléphones portables professionnels** Les ressources de la Ville de Saintes accessibles depuis un téléphone portable professionnel sont protégées en confidentialité et en intégrité.

Les téléphones portables utilisés dans un contexte professionnel (consultation des emails) intègrent des mécanismes de sécurité adaptés :

- Utiliser un mot de passe pour déverrouiller les téléphones ;
- Activer un verrouillage automatique du téléphone après une période d'inactivité ;
- Activer le chiffrement du téléphone ;

Ces mécanismes sont renforcés par l'utilisation d'une solution de gestion des terminaux mobiles.

6.4. TRAÇABILITE DES ACTIONS ET JOURNALISATION

Règle JOU-1	**Journalisation des accès** Toute activité d'exploitation ou d'administration fait l'objet d'une traçabilité afin d'assurer la non-répudiation des actions. Une stratégie de collecte est définie et mise en œuvre sur la base d'une analyse des risques.

Règle JOU-2	**Centralisation et sécurisation des traces** Les traces produites sur chacun des composants du système sont systématiquement déportées vers un serveur de collecte et de centralisation sécurisée des traces.

Règle JOU-3	**Corrélation et exploitation des journaux** Les traces font l'objet d'une revue régulière selon une procédure formelle, et ce en vue d'identifier tout comportement anormal.

Un outil d'analyse et de corrélation des logs est utilisé à cet effet.

Règle JOU-4	**Conservation des journaux** Les traces sont archivées pendant un an, hors contraintes légales et réglementaires.

6.5. GESTION DES SAUVEGARDES

Règle SVG-1	**Réalisation des sauvegardes** Des sauvegardes sont réalisées régulièrement pour faire face à un sinistre. Une politique de sauvegarde et de restauration est définie pour toutes les données des systèmes d'information.

La politique de sauvegarde précise :

- Les fréquences et l'étendue de sauvegarde nécessaire conformément aux exigences métiers et aux contraintes règlementaires ;
- Les exigences de sécurité applicables aux informations sauvegardées.

Règle SVG-2	**Protection des sauvegardes** Les données sauvegardées sont conservées de manière à garantir leurs confidentialité, intégrité et disponibilité.

Les règles suivantes, issue du principe 3,2,1, sont respectées :

- Placer les sauvegardes dans un endroit suffisamment distant du site principal ;
- Doter l'information sauvegardée d'une protection physique et environnementale adéquate ;
- Définir et mettre en place une solution de sauvegarde en mode *offline* ;
- Chiffrer les sauvegardes des données confidentielles.

Règle SVG-3	**Procédure de restauration des sauvegardes** Une procédure de restauration des sauvegardes est formalisée et régulièrement testée.

Règle SVG-4	**Tests réguliers des sauvegardes** Des tests de restauration sont réalisés annuellement sur une plateforme de test pour s'assurer du bon fonctionnement du dispositif de sauvegarde.

6.6. GESTION DES VULNERABILITES ET DES MISES A JOUR

Règle VLN-1	**Veille sur les vulnérabilités et mises à jour des systèmes** La Ville de Saintes s'informe régulièrement sur les vulnérabilités techniques et les menaces qui concernent les composants en production des systèmes d'information.

Les moyens suivants sont considérés lors de l'identification des vulnérabilités :

- Suivre les dernières mises à jour sécurité qui concernent des composants en production des systèmes d'information, et identifier toute nouvelle vulnérabilité ;
- S'abonner à des services de vieille sécurité des systèmes d'information (ex. CERT-FR) ;
- Participer à des groupes de travail et échanger les informations sur les menaces et vulnérabilités ;
- Avoir accès à une assistance technique par les éditeurs des solutions utilisées ;
- Utiliser un gestionnaire de vulnérabilité qui scanne l'ensemble du réseau en permanence et détecte la présence de toute vulnérabilité non corrigée :
    - Scan de vulnérabilité interne : permets d'identifier les vulnérabilités critiques en interne.
    - Scan de vulnérabilité externe : permets d'identifier les vulnérabilités critiques exposées sur internet.

Règle VLN-2	**Évaluation des vulnérabilités et application des correctifs** Pour chaque vulnérabilité identifiée, il convient d'évaluer l'exposition de la Ville de Saintes à ces vulnérabilités et d'entreprendre, dans les meilleurs délais, les actions appropriées pour traiter le risque associé.

En particulier, tous les postes de travail et les serveurs les plus exposés aux risques sont à jour de leurs correctifs de sécurité.

Pour une gestion efficace du déploiement des mises à jour, des outils d'automatisation sont mis en place afin de :

- Collecter automatiquement les mises à jour depuis internet ;
- Télécharger et installer automatiquement les mises à jour sur les composants concernés : Poste de travail, Serveur (Linux et Windows), application métier et logiciel ;
- Redémarrer automatiquement les composants non critiques : les équipements critiques sont redémarrés manuellement ;
- Lancer automatiquement des services après redémarrage.

Règle VLN-3	**Gestion des obsolescences** L'ensemble des logiciels utilisés sur les systèmes d'information sont dans une version supportée par l'éditeur ou par la communauté le cas échéant.

Un inventaire des composants obsolètes est maintenu à jour par la DSI.

Pour chaque composant obsolète, un projet de mise à niveau de sécurité est proposé. Ce projet peut consister :

- Soit à réaliser une montée de version du composant en déployant une version supportée par l'éditeur ;
- Soit à définir et appliquer des mesures de sécurité compensatoires pour limiter l'exposition du composant obsolète (Mise en quarantaine, limiter l'accès réseau, désactiver les services obsolètes, Patch virtuel, etc.).

6.7. LUTTE CONTRE LES CODES MALVEILLANTS

Règle VIR-1	**Protection antimalware** Un antimalware est installé et maintenu à jour sur l'ensemble des serveurs et des postes de travail (Windows et Linux).

La configuration de l'antimalware prend en compte les mesures de sécurité suivantes :

- Analyser en temps réel les processus actifs, les fichiers importés, les pages web, les courriels, les supports amovibles et les comportements au niveau local ;
- Réaliser une analyse complète des disques locaux de façon hebdomadaire ;
- Mettre à jour régulièrement les bases de signature ;
- Isoler du réseau tout équipement infecté ou soupçonné.

Ceci concerne à la fois les systèmes d'exploitation Linux et Windows.

La protection anti-malware au niveau des postes de travail est mise en place à travers d'un :

- **Antivirus** : Basé sur le contrôle des signatures pour la détection des malwares. C'est la première ligne de défense sur les postes de travail, permettant de détecter les logiciels malveillants de base ;
- **Antivirus Next-Génération** : Effectue une analyse comportementale des processus au niveau de la machine pour détecter la présence d'un malware. Cela permet de détecter et neutraliser les malwares non connus par la base antivirale ;
- **EDR (EndPoint Detection & Response)** : Effectue une corrélation des journaux de chaque machine pour détecter les modes opératoires d'attaque et neutraliser les machines infectées. Cette brique est la plus importante dans la chaîne de protection antimalware, car elle permet de détecter les activités de compromission réalisées par un attaquant ayant réussi de compromettre le système.

Règle VIR-2	**Interdire l'utilisation des composants non maîtrisés (Shadow IT)** La Ville de Saintes détecte et interdit l'utilisation des logiciels, équipements et solutions non autorisés et non validés par la DSI. La Ville de Saintes fournit, dans la mesure du possible, des solutions alternatives aux agents pour répondre à leurs besoins.

L'installation spontanée de toute infrastructure informatique technique, qu'elle soit physique ou logique, est strictement interdite. Seule la DSI est habilitée à mettre en œuvre des infrastructures.

6.8. NOMADISME

Les équipements informatiques « nomades » fournis par la Ville de Saintes sont par essence perdables et ne bénéficient pas des mêmes mesures de sécurité, étant donnée l'environnement dans lequel ils sont utilisés (Avion, hôtel, maison …), que les équipements fixes et installés dans les locaux de la Ville de Saintes.

Des mesures spécifiques doivent être appliquées et respectées.

Règle NOM-1	**Sécurité des accès distants au système d'information** L'accès distant aux systèmes d'information internes de la Ville de Saintes est effectué à travers une solution VPN/IPSec qui assure la confidentialité et l'intégrité des données échangées.

Les règles ci-dessous sont respectées en cas d'accès distant :

- Une protection en confidentialité et en intégrité du canal sur lequel transitent les flux *via* une solution VPN ;
- Une authentification forte pour protéger les accès contre toute attaque d'usurpation d'identité : Authentification par login/mot de passe utilisateur et par un certificat machine ;
- Une traçabilité (côté réseau, équipement et serveur) des échanges pour assurer la non-répudiation des actions entreprises ;
- Une inspection et filtrage des flux internet pour détecter et bloquer les sites malveillants.

Les accès distants regroupent la télémaintenance, le télétravail et l'accès en mobilité.

Règle NOM-2	**Protection des données manipulées** Les données de la Ville de Saintes manipulées en dehors des locaux sont protégées contre le vol.

Cette protection est garantie par :

- L'implémentation d'un mécanisme de chiffrement des disques durs des postes de travail ;
- La distribution de film de protection d'écran ;
- La mise à disposition de poste de travail dédié aux déplacements à l'étranger pour ne pas exposer les données sensibles de la Ville de Saintes.

6.9. IMPRIMANTES ET COPIEURS

Règle IMP-1	**Impression en mode privé** Les copieurs de la Ville de Saintes mettent en place un mécanisme d'authentification permettant aux utilisateurs d'imprimer en mode privé.

Les mesures ci-dessous sont mises en place au niveau des imprimantes de la Ville de Saintes :

- L'utilisateur doit s'authentifier sur l'imprimante avant de pouvoir récupérer le document imprimé ;
- Les utilisateurs sont sensibilisés pour retirer immédiatement les documents imprimés ;
- Les flux de données envoyées vers les imprimantes sont protégés en confidentialité et en intégrité ;
- Les interfaces d'administration des imprimantes sont protégées par une authentification et un accès sécurisé via HTTPs.
- Les documents scannés sont envoyés par mail aux destinataires ;

Règle IMP-2	**Suppression des données au niveau des imprimantes mises au rebut** Les mécanismes de suppression sécurisés proposés par les imprimantes sont utilisés pour supprimer les données de la Ville de Saintes avant mise au rebut ou retour de location des imprimantes.

6.10. PROTECTION DE LA MESSAGERIE

Règle MES-1	**Protection de la messagerie** La Ville de Saintes met en place des solutions de détection et de blocage des attaques ayant comme vecteur d'intrusion la messagerie interne.

Les mesures ci-dessous sont mises en place au niveau des services de messagerie ou via des services tiers :

- Activation des filtres anti-spam, anti-malware, anti-phishing
- Blocage des adresses email/IP suspectes.

6.11. PROTECTION DES EQUIPEMENTS BYOD

Règle BYOD-1	**BYOD pour le personnel de la Ville de Saintes** La connexion d'ordinateurs ou de smartphones personnels des collaborateurs au réseau interne de la Ville de Saintes n'est pas autorisée. Seuls les ordinateurs et les smartphones professionnels de la Ville de Saintes peuvent être branchés sur le réseau interne pour accéder aux ressources de la Ville de Saintes.

7. SECURITE DANS LES PROJETS

7.1. PROJETS INFORMATIQUES

Règle SPI-1	**Intégration de la sécurité dans les projets – « Security By Design »** Tout projet ayant une dimension informatique intègre systématiquement la sécurité dans son processus de management et ceci dès la phase de conception.

Chaque direction de la Ville de Saintes ayant comme objectif de lancer un projet qui nécessite un changement dans les systèmes d'information doit se référer systématiquement au RSSI, pour réaliser une étude de sécurité.

La consultation du RSSI doit se faire en phase de conception et d'élaboration du cahier des charges.

Un changement des systèmes d'information peut être à titre d'exemple :

- Une demande exprimée par une direction métier sous la forme d'une fiche navette ;
- Modification/changement d'une application ou d'un système existant ;
- Ajout d'une nouvelle application ou d'un nouveau système (interne ou externe) ;
- Développement d'une nouvelle application en interne ou via un prestataire externe ;
- Modification des composants techniques du système d'information (Changement de matériels, etc.) ;
- Modification de la topologie réseau (Cloisonnement, filtrage, interconnexion, etc.) ;
- Externalisation d'un service ou d'une application ;
- Etc.

Règle SPI-2	**Étude des risques et identification des exigences de sécurité** Le RSSI réalise, en concertation avec le métier, une analyse des risques sécurité relatifs au changement introduit par le projet. Un plan de traitement de risques qui découle de cette analyse est formalisé sous forme « d'expression de besoin en matière de sécurité » et est intégré au cahier des charges du projet.

Les objectifs de l'analyse de risques sont les suivants :

- Prendre en compte les règles de sécurité de la présente PSSI ;
- Prendre en compte les contraintes légales et réglementaires applicables au projet (Protection des données classifiées, protection des données à caractère personnel – RGPD) ;
- Identifier les risques liés au projet en prenant en compte le contexte, l'écosystème, les parties prenantes, les changements apportés aux systèmes d'information de la Ville de Saintes ;
- Proposer les mesures de sécurité à mettre en place pour réduire les risques identifiés ;

- Identifier les risques résiduels formellement acceptés par la direction concernée.

À l'issue de l'analyse des risques, les mesures de sécurité à mettre en place dans le cadre du projet sont formalisées et intégrées dans le cahier des charges sous forme d'exigences sécurités.

Règle SPI-3	**<u>Vérification du respect des exigences de sécurité</u>** À l'issue de la phase de réalisation de chaque projet, le RSSI réalise un audit du système et vérifie que les exigences de sécurité ont bien été prises en compte. Un avis d'un point de vue sécurité est ensuite formalisé par le RSSI en fonction des résultats de l'audit. Dans le cas d'un avis non favorable, il revient à la Direction concernée d'autoriser ou non la mise en production du système en question.

L'audit de sécurité permet de vérifier que le projet a bien pris en compte les contraintes opérationnelles de sécurité établies en phase de conception, que les exigences de sécurité sont bien satisfaites, que les risques résiduels sont maîtrisés, et que le système en question est donc apte à entrer en service.

L'arbitrage de la direction est nécessaire uniquement en cas d'avis non favorable. Dans ce cas précis, les risques résiduels sont présentés à la direction qui décide ensuite de les accepter ou de les refuser. En cas de refus, un plan d'action de remédiation est proposé et mis en place, et ce avant l'entrée en service du système en question.

8. SECURITE DANS LES RELATIONS AVEC LES TIERS

8.1. PRESTATAIRES EXTERIEURS

La Ville de Saintes recourt à des prestataires externes dans le cadre des activités réalisées par ses directions. Elle reste néanmoins responsable en toute circonstance de la protection des informations et des processus métiers, y compris sur les périmètres sous-traités ou externalisés auprès des tiers.

Il est donc fondamental de respecter des règles strictes dans les phases de sélection, de contractualisation et de suivi de l'exécution des prestations des tiers.

Règle SRT-1	**Expression des exigences sécurité** Toute réflexion d'externalisation de service fait l'objet d'une étude sécurité et d'une expression des besoins de sécurité conformément à la règle SPI-2.

Le RSSI, en liaison avec le responsable de la prestation, a la charge de la réalisation d'une analyse des risques liés à la prestation.

L'objectif de cette analyse est d'exprimer les besoins de sécurité relatifs à la prestation, et ce dès la phase de cadrage. Ces besoins de sécurité sont intégrés dans le cahier des charges de la prestation.

Un clausier sécurité et RGPD (Règlement général sur la protection des données) est intégré aux contrats signés avec les prestataires.

Règle SRT-2	**Sélection des tiers** L'expression des besoins de sécurité donne lieu à des exigences qui sont intégrées au cahier des charges de la consultation et font partie des critères de sélection des tiers.

Le cahier des charges fourni aux soumissionnaires inclut un questionnaire relatif aux exigences de sécurité issues de l'expression de besoins (SRT-1).

Pour chaque exigence, les candidats décrivent les mesures qu'ils mettent en œuvre pour y répondre dans un Plan d'Assurance Sécurité (PAS).

Règle SRT-3	**Engagement des tiers et clauses de sécurité** Le prestataire sélectionné s'engage à respecter les exigences de l'expression de besoin sécurité (SRT-1). Cet engagement se matérialise par des clauses dans le contrat de prestation.

Chaque prestation externe intègre des clauses de sécurité génériques, fournies par le service juridique avec l'appui du RSSI, et des clauses de sécurité spécifiques à la prestation. Les clauses de sécurité spécifiques sont issues de l'analyse des risques, élaborée en phase de cadrage.

Les clauses de sécurité couvrent, a minima, les thématiques suivantes :

- Des clauses garantissant le respect des exigences de l'expression de besoin sécurité ;
- Des clauses autorisant la conduite d'audits par la Ville de Saintes ou de contrôles de conformité des services opérés ;
- Des clauses exigeant un respect strict de la réglementation applicable ;
- Des accords de confidentialité signés par le prestataire ;
- Les conditions de restitution et/ou de destruction des données en fin du contrat ;
- Les règles de gestion et de notification des incidents ;
- Des clauses et conditions de réversibilité de la prestation.

Règle SRT-4	**Suivi des prestations et des contrats** Les services rendus par les tiers avec lesquels des contrats ont été signés sont suivis par rapport aux exigences sécurité des systèmes d'information.

Ceci implique en particulier de :

- Vérifier le respect des clauses de sécurité ;
- Vérifier le respect des exigences de sécurité ;
- Réaliser des contrôles de sécurité avant l'entrée en production et à fréquence régulière des services proposés par les tiers ;
- Contrôler et limiter les accès des prestataires externes aux ressources et données de la Ville de Saintes.

Règle SRT-5	**Gestion des accords de non-divulgation (NDA)** Tout prestataire externe de la Ville de Saintes reçoit et signe l'accord de non-divulgation avant le début de la prestation.

Les accords de non-divulgation sont systématiquement imposés à tous les prestataires externes qui traitent, stockent ou collectent des données internes de la Ville de Saintes.

Règle SRT-6	**Charte des prestataires externes** Tout prestataire intervenant, localement ou à distance, sur les ressources des systèmes d'information de la Ville de Saintes reçoit et signe la charte des prestataires avant le début de la prestation.

La charte des prestataires est systématiquement signée par tous les prestataires externes qui bénéficient, dans le cadre de leur mission, d'un accès privilégié - local ou distant - aux systèmes d'information de la Ville de Saintes.

9. SURVEILLANCE ET GESTION DES INCIDENTS

Règle SGI-1	**Procédure de gestion des incidents de sécurité** Une procédure de gestion des incidents de sécurité est définie et mise en œuvre. Elle identifie les responsabilités et les actions à respecter afin de permettre une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité des systèmes d'information.

Règle SGI-2	**Détecter et remonter les incidents de sécurité** Un dispositif de surveillance continue et permanente des systèmes d'information et de remontée des incidents de sécurité informatique est mis en place.

Les moyens suivants sont utilisés :

- Le personnel : les agents sont sensibilisés à remonter tout évènement ou faille de sécurité informatique, constaté ou suspecté. Un moyen de communication est mis à leur disposition ;
- Alertes remontées par les mécanismes de contrôle de la sécurité : Pare-feu, détecteur d'intrusion, filtre antispam, filtre antimalware, antivirus, etc. ;
- Revue régulière des traces et des journaux d'évènement : Une procédure est définie et mise en œuvre pour exploiter les journaux et détecter tout acte malveillant ;
- Veille de sécurité en vue d'être notifié des nouvelles menaces auxquelles il convient de réagir de manière préventive.

Règle SGI-3	**Qualification des incidents sécurité** Une qualification des incidents détectés est élaborée en vue de déclencher une réponse appropriée.

Chaque évènement lié à la sécurité des systèmes d'information est apprécié et catégorisé le cas échéant comme incident lié à la sécurité des systèmes d'information, conformément à la procédure de gestion des incidents.

Règle SGI-4	**Réponse aux incidents sécurité** La procédure de gestion des incidents prévoit une réponse aux incidents en fonction de leur niveau de classification.

Une équipe de réponse et de réaction, en cas d'incidents liés à la sécurité des systèmes d'information, est composée.

Cette équipe a comme mission de :

- Répondre aux incidents signalés ;
- Limiter les dommages et réduire les impacts des incidents de sécurité ;
- Communiquer auprès des parties intéressées (en interne, les autorités nationales, les tiers, etc.) ;
- Collecter les preuves ;
- Journaliser toutes les actions effectuées ;
- Réduire la probabilité de survenue d'incidents répétitifs.

Des fiches réflexes sont formalisées pour améliorer le temps de réaction aux incidents sécurité.

Règle SGI-5	**Apprentissage des incidents sécurité** La procédure de gestion des incidents de sécurité intègre, en fonction des cas, une étude post incidents en vue d'identifier les éventuelles mesures qui permettraient de réduire la probabilité d'occurrence des futurs incidents ou de réduire leurs impacts.

Cette règle s'inscrit dans une démarche d'amélioration continue des politiques de sécurité de la Ville de Saintes. Elle consiste à analyser les incidents survenus afin de :

- Améliorer les mesures de sécurité existantes ;
- Proposer de nouvelles mesures de sécurité ;
- Mettre à jour l'analyse des risques (réévaluer les vraisemblances, ajouter de nouvelles menaces, etc.).

10. REPRISE D'ACTIVITE DES SYSTEMES D'INFORMATION

Règle PCA-1	**Identification des besoins en termes de disponibilité des services** Les besoins en termes de disponibilité sont identifiés par le responsable fonctionnel de l'actif pour chaque composant des systèmes d'information.

Les besoins de disponibilité sont exprimés en RPO et RTO :

- RTO (Recovery Time Objective) : durée maximale d'interruption admissible ;
- RPO (Recovery Point Objective) : durée maximum d'enregistrement des données qu'il est acceptable de perdre.

Règle PCA-2	**Plan de Continuité d'activité** Un plan de continuité (PCA) est élaboré et mis à jour régulièrement en accord avec les exigences de disponibilité de la Ville de Saintes. Les responsabilités liées à la continuité de l'activité sont clairement définies.

Le plan de continuité d'activité permet de remettre en service les applications les plus sensibles dans un délai raisonnable, en cas de sinistre majeur impactant les systèmes d'information.

La mise en place du PCA prend en compte tous les périmètres de la Ville de Saintes.

Règle PCA-3	**Test du Plan de Continuité d'activité** Il convient de s'assurer de la bonne mise en œuvre des dispositions prévues dans le plan de continuité d'activité. Cela s'effectue par des tests et exercices annuels.

11. SECURITE PHYSIQUE ET ENVIRONNEMENTALE

11.1. PROTECTION PHYSIQUE DES LOCAUX

Règle PPL-1	**Identification des zones de sécurité physique** La Ville de Saintes identifie les zones de sécurité physique et les classifie selon leurs niveaux de sensibilité : • Zone publique ; • Zone interne ; • Zone sensible.

Règle PPL-2	**Contrôle d'accès physique aux zones de sécurité physique :** Tout accès à une zone sensible des locaux de la Ville de Saintes fait l'objet d'un dispositif de contrôle d'accès physique.

Mettre en place des mesures de protection physique adéquates pour sécuriser les locaux et les zones sensibles :

- Zone interne : accessible aux agents ;
- Zone sensible : accessible aux personnes explicitement autorisées. Exemple : salle serveur, etc.

Tenir à jour une liste des personnes autorisées à pénétrer dans chaque zone.

Les zones sensibles sont protégées par une solution de contrôle d'accès par badge.

Règle PPL-3	**Gestion des droits d'accès physique** La délivrance des moyens et des droits d'accès physiques respecte une procédure formelle de gestion des habilitations d'accès physique. Cette procédure prévoit notamment la récupération des moyens d'accès physique en cas de départ d'un agent.

Règle PPL-4	**Procédure d'accueil et d'accès des visiteurs** Une procédure d'accueil et d'accès des visiteurs est formalisée et appliquée au sein de la Ville de Saintes.

Cette procédure intègre les règles suivantes :

- Réception du visiteur au niveau de l'accueil de la Ville de Saintes pour tout accès à une zone non-publique ;
- Accompagnement des visiteurs dans les zones non publiques. Les visiteurs sont accompagnés depuis leur entrée, pendant leur visite puis raccompagnés à la sortie par un agent de la Ville de Saintes.
- Attribution d'un badge pour les visiteurs qui sont amenés à circuler sans accompagnement dans les locaux. Ce badge est porté de façon visible par le visiteur ;
- Remontée d'alerte en cas d'un visiteur non accompagné dans une zone sensible.

Règle PPL-5	**Protection des équipements en salle serveur** Un contrôle d'accès est mis en place pour accéder à la salle d'hébergement des serveurs. De plus cette salle est constamment sous vidéoprotection. Tout matériel présent dans cette salle se trouve dans une baie fermée à clefs. Ces clefs sont sous la responsabilité de la DSI.

11.2. PROTECTION PHYSIQUE DU MATERIEL

Règle PPM-1	**Protection des équipements informatiques** Les équipements informatiques sont mis dans des emplacements sécurisés de manière à limiter les dangers environnementaux et les possibilités d'accès non autorisés, et ce en fonction de la criticité des équipements.

Les précautions suivantes sont considérées :

- Stocker les équipements de secours, les serveurs et les équipements réseaux dans des locaux techniques sécurisés et adaptés ;
- Mettre en place des mesures de protection contre le vol, l'incendie, les fuites d'eau et les pannes d'électricité ;
- Mettre en place des systèmes de climatisation et de contrôle d'humidité, fiables et surveiller les conditions ambiantes.

Règle PPM-2	**Maintenance des matériels**

	La Ville de Saintes définit et met en œuvre une procédure de maintenance des matériels informatiques.

La procédure de maintenance respecte les règles ci-dessous :

- Appliquer les recommandations des fournisseurs ;
- Contrôler les activités de maintenance réalisées par des externes ;
- Maintenir un dossier de journalisation de toutes les pannes, de toutes les actions de maintenance et de prévention.

Règle PPM-3	**Procédure de bureau propre** Une procédure de bureau propre et d'écran vide est formalisée et communiquée afin de protéger les informations sensibles.

Mettre à disposition des agents :

- Des armoires verrouillables à clé ;
- Des déchiqueteuses au niveau de chaque bâtiment ;
- Une solution de verrouillage automatique de leur poste de travail en cas d'absence.

12. CONFORMITE

12.1. CONFORMITE LEGALE, REGLEMENTAIRE ET CONTRACTUELLE

Règle CLR-1	**Référentiels d'exigences applicables** Un référentiel d'exigences légales, réglementaires et contractuelles, impactant les systèmes d'information, est mis en place et tenu à jour avec l'appui de la direction juridique.

Règle CLR-2	**Conformité avec le référentiel d'exigences applicables** Un plan de conformité est élaboré et mis en œuvre afin d'assurer la conformité vis-à-vis des exigences légales, réglementaires et contractuelles.

Règle CLR-3	**Contrôle du respect du référentiel d'exigences applicables** Un processus d'audit de conformité est défini et mis en œuvre par le RSSI en concertation avec la direction générale et la direction juridique afin de contrôler la mise en conformité vis-à-vis des exigences légales, réglementaires et contractuelles.

Règle CLR-4	**Conformité RGPD - Règlement général sur la protection des données** Un groupe de travail qui réunit : le DPO, le RSSI, et un membre de la direction générale est formé pour suivre les travaux de mise en conformité RGPD. Un comité stratégique se réunit une fois tous les 6 mois pour suivre les travaux et réaliser les arbitrages nécessaires à la mise en conformité RGPD.

12.2. CONFORMITE A LA POLITIQUE DE SECURITE

Règle CPS-1	**Contrôle du respect de la PSSI** Un processus d'audit de sécurité des systèmes d'information est défini et mis en œuvre en vue d'évaluer la conformité des systèmes d'information aux règles de la présente Politique de Sécurité des Systèmes d'Information.

- L'audit est réalisé sous la responsabilité du RSSI ;
- Le processus décrit les méthodes d'évaluation pour chaque règle de la présente Politique de Sécurité des Systèmes d'Information et du référentiel d'exigences présenté dans la règle CLR-1 ;
- L'audit doit identifier les éventuelles non-conformités et élaborer un plan d'action correctif ;
- L'audit doit avoir lieu une fois tous les deux ans ;
- Les résultats des évaluations sont consolidés dans un tableau de bord régulièrement mis à jour ;
- Une synthèse des audits est présentée et communiquée à la direction générale.

Règle CPS-2	**Audit technique des applications et systèmes** Une procédure d'audit technique régulier est définie et mise en place pour tous les systèmes et applications internes et externes de la Ville de Saintes.

Les audits techniques de sécurité sont déroulés périodiquement pour les applications internes et externes et ceci pour tous les systèmes d'information gérés par la Ville de Saintes.

Une procédure décrivant cette démarche d'audit est formalisée et partagée avec toutes les directions.

En particulier, les services sensibles exposés sur internet sont régulièrement audités pour vérifier leur résistance aux menaces extérieures.

13. ANNEXE

13.1. GLOSSAIRE

Bien essentiel : Information ou processus jugé comme important.

EDR : Endpoint Detection and Response

Firmware : Un programme intégré dans un matériel informatique pour qu'il puisse fonctionner.

Homologation : Il s'agit d'un processus d'information et de responsabilisation qui aboutit à une décision, prise par le responsable de l'organisation. Cette décision constitue un acte formel par lequel il :

- Atteste de sa connaissance des systèmes d'information et des mesures de sécurité (techniques, organisationnelles ou juridiques) mises en œuvre ;
- Accepte les risques qui demeurent, qu'on appelle risques résiduels.

HTTPS : HyperText Transfer Protocol Secure, un protocole de communication sécurisée.

Incident de sécurité : tout évènement ou ensemble d'évènements indésirables ou inattendus, susceptibles de compromettre les opérations liées à l'activité de l'organisation, et de menacer significativement la sécurité de ses informations et de ses ressources. Les incidents de sécurité peuvent être d'origine humaine (interne ou externe) ou naturelle, par négligence ou délibérée.

Infrastructure de Gestion des Clés (IGC) : Un ensemble de composants, de procédures et de logiciels utilisés pour gérer les certificats des chiffrements asymétriques d'une organisation.

Menace : Cause potentielle d'un incident indésirable pouvant nuire à un système ou à un organisme

Non-Disclosure Agreement (NDA) : c'est un Accord de Non-Divulgation, une clause de confidentialité, entre deux parties.

Role Based Access Control (RBAC) : un modèle de contrôle d'accès dans lequel chaque décision d'accès à une ressource est basée sur le rôle de l'utilisateur ayant demandé l'accès.

SAAS : Le software as a service ou logiciel en tant que service, est un type de service accessible par les utilisateurs depuis internet et installés sur des serveurs distants plutôt que sur la machine de l'organisation.

Sécurité de l'information : La sécurité de l'information représente l'ensemble des moyens organisationnels, techniques et procéduraux ayant pour objectif d'assurer la disponibilité, l'intégrité, la confidentialité des systèmes et des données :

- *La disponibilité* : assurer la continuité des services, l'accès aux données et aux applications, dans le respect des objectifs de performance ;
- *L'intégrité* : garantir l'exhaustivité et la validité des informations ; se prémunir des modifications, par accident ou malveillance ;
- *La confidentialité* : réserver les accès aux données, applications et systèmes aux seules personnes habilitées.

Security By Design : Il s'agit d'une approche de développement des systèmes et des applications, qui consiste à prendre en compte la sécurité des systèmes d'information dès la phase de conception et d'expression de besoin.

SFTP : Secure File Transfer Protocol, un protocole d'échange de données sécurisé.

Shadow IT : C'est un terme utilisé pour désigner toutes les solutions, les applications, les logiciels et les services web, utilisés par les agents sans approbation de la direction.

SNMP : Simple Network Management Protocol, est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.

Système d'information : Le système d'information est considéré dans son ensemble, c'est-à-dire comme la totalité des moyens matériels, logiciels et organisationnels visant à créer, acquérir, traiter, stocker, diffuser ou détruire de l'information sous quelque forme que ce soit : électronique, papier, oral, etc. Il inclut toutes les solutions informatiques sous maîtrise directe et tout ce qui est contractualisé avec des tiers.

VPN (Virtual Private Network ou Réseau Privé Virtuel) : Réseau permettant de travailler en toute sécurité, à travers un réseau tiers comme Internet. Le protocole IPsec est l'une des méthodes permettant de créer des VPN

802.1x : Un standard lié à la sécurité des réseaux informatiques. Il permet d'authentifier, de contrôler et de journaliser les accès réseau des machines et des postes de travail.

Envoyé en préfecture le 10/01/2025
Reçu en préfecture le 10/01/2025
Publié le
ID : 017-211704150-20241219-2024_177A-DE

SAINTES

SAINTES
CENTRE COMMUNAL
D'ACTION SOCIALE

Charte utilisateur de la Ville et du CCAS de Saintes

Table des matières

1. DEFINITIONS

Charte informatique : Document, généralement annexe au protocole du temps de travail rédigé par la Ville et le CCAS de Saintes dans le but de réglementer l'usage des systèmes d'information de ses agents, membres ou adhérents (entreprise, association, administration…).

Système d'information : Ensemble de moyens informatiques et de télécommunications ayant pour finalité d'élaborer, traiter, stocker, acheminer, présenter ou détruire des données.

2. PREAMBULE

La Ville et le CCAS de Saintes met en œuvre un système d'information et de communication nécessaire à l'exercice de son activité, comprenant notamment un réseau informatique et téléphonique, ainsi que des outils mobiles.

Les agents, dans l'exercice de leurs fonctions, sont conduits à accéder et à utiliser lesdits équipements informatiques, ainsi que le système d'information et de communication mis à leur disposition. L'utilisation du système d'information et de communication doit être effectué exclusivement à des fins professionnelles, sauf exception prévue dans la présente charte.

Aussi, dans un but de transparence à l'égard des utilisateurs, de promotion d'une utilisation loyale, responsable et sécurisée du système d'information et des équipements informatiques, la présente charte pose les règles relatives à l'utilisation de ces ressources.

Elle définit aussi les moyens de contrôle et de surveillance de cette utilisation mise en place, non seulement pour la bonne exécution du contrat de travail des agents, mais aussi dans le cadre de la responsabilité pénale et civile de l'employeur. Elle dispose d'un aspect réglementaire et doit être signée par chaque utilisateur.

Elle ne remplace en aucun cas les lois en vigueur, que chacun est censé connaître.

3. CHAMP D'APPLICATION

3.1. SYSTEME D'INFORMATION ET TELECOMS

Le système d'information et de communication de la Ville et du CCAS de Saintes est notamment constitué des éléments suivants :

- Ordinateurs portables et fixes ;
- Accessoires (câbles, chargeurs, clé USB…) ;
- Connexions réseau ;
- Imprimantes et Scanners, Photocopieurs Multifonctions ;
- Messagerie électronique ;
- Téléphones portables et fixes ;
- Logiciels utiles à l'activité du CCAS de Saintes.

3.2. CENTRE DE SERVICES

La Ville et le CCAS de Saintes dispose d'un centre de services au sein de la Direction des Systèmes d'Information et Télécoms (DSIT). C'est par lui que sont centralisées toutes les demandes ou déclarations d'incident des utilisateurs qui sont ensuite transmises aux différentes équipes. Le centre de services assure également un soutien technique à chaque agent détenteur d'une ressource numérique (Réf 3.1).

3.3. UTILISATEURS CONCERNES

Sauf mention contraire, la présente charte s'applique à l'ensemble des utilisateurs du système d'information et télécoms de la Ville et du CCAS de Saintes, quel que soit leur statut : Elus, dirigeants, agents, stagiaires…

Le service des ressources humaines veille à faire accepter les règles posées dans la présente charte à tout nouvel utilisateur qui demandera d'accéder au système d'information et télécoms, soit sur l'un des sites de la Ville et du CCAS de Saintes, soit à partir de tout lieu de travail déporté et notamment en situation de télétravail.

Sont exclus de ce champ les utilisateurs ou tous les intervenants extérieurs pour lesquels un contrat de confidentialité ou bien une charte spécifique devra être signée, notamment pour les prestataires de service, les partenaires.

4. CONFIDENTIALITE

4.1. CONFIDENTIALITE DES PARAMETRES D'ACCES

L'accès à certains éléments du système d'information comme la messagerie électronique, la téléphonie, les sessions sur les postes de travail, le réseau, certaines applications ou services interactifs sont protégés par des paramètres de connexion (identifiant, mot de passe). Ces paramètres ne doivent pas être transmis à des tiers ou se retrouver aisément accessibles.

Ces paramètres sont personnels à l'utilisateur, ils doivent être gardés confidentiels et ne pas être communiqués.

Lors de la première utilisation de ces identifiants, l'utilisateur devra modifier le mot de passe qui lui aura été communiqué, par un mot de passe personnel qui devra respecter un certain degré de complexité et devra être modifié tous les 6 mois.

Aucun utilisateur ne doit se servir d'un autre compte que celui qui lui a été attribué pour accéder au système d'information de la Ville et du CCAS de Saintes. Il ne doit pas non plus déléguer à un tiers les droits d'utilisation qui lui sont attribués.

4.2. CONFIDENTIALITE DES DONNEES

Les personnes ayant accès à des données confidentielles, du fait de leur activité, sont assujetties à une obligation de confidentialité sur les informations qu'elles sont amenées à détenir, consulter ou utiliser.

L'utilisateur s'engage à prendre toutes les précautions utiles pour éviter que ne soient divulguées de son fait, ou du fait de personnes dont il a la responsabilité, ces informations confidentielles. Encore plus particulièrement lors de déplacements professionnels.

En cas d'absence momentanée de son poste de travail, bien que le verrouillage se réalise au bout de 10 min, il est impératif que l'utilisateur verrouille l'accès au matériel.

Tout matériel n'appartenant pas à la Ville et au CCAS de Saintes (clé USB ou disque dur externe) est proscrit, néanmoins l'utilisateur pourra obtenir une autorisation préalable et écrite (manuscrite ou électronique) auprès de la DSIT. Un formulaire de demande et un matériel d'analyse seront mis à disposition.

5. SECURITE

5.1. ROLE DU CCAS DE SAINTES

La Ville et le CCAS de Saintes se doivent de mettre en œuvre les moyens humains et techniques appropriés pour assurer la sécurité matérielle et logicielle du système d'information et Télécoms.

À ce titre, il lui appartient de limiter les accès aux ressources sensibles ou d'obtenir les autorisations nécessaires à l'utilisation des ressources mises à disposition des utilisateurs.

La Ville et Le CCAS de Saintes sont responsables de la mise en œuvre et du contrôle du bon fonctionnement du système d'information et Télécoms. Ils veillent à l'application des règles de la présente charte. Ils sont assujettis à une obligation de confidentialité sur les informations qu'ils sont amenés à connaître.

5.2. ROLE DE L'UTILISATEUR

Il appartient à l'utilisateur de veiller à la sécurité du matériel utilisé en faisant preuve de prudence et de vigilance. L'utilisateur s'engage à prendre soin du matériel informatique et des locaux mis à sa disposition dans le cadre de l'exercice de ses fonctions.

Il informe la DSIT de toute anomalie, incident ou dysfonctionnement repéré. Une anomalie peut être l'indice d'une infection par un virus ou d'un problème de sécurité. L'accès au système d'information avec du matériel (PC, Tablettes, smartphones) n'appartenant pas à la Ville et au CCAS de Saintes, est formellement interdit.

L'utilisateur doit veiller à enregistrer tous les fichiers sur lesquels il travaille sur le réseau d'entreprise car tout document stocké hors du réseau n'est pas sauvegardé (Bureau, mes documents, mes images, téléchargement). Il doit régulièrement supprimer les données devenues inutiles sur les espaces communs du réseau.

Le vol ou la perte de matériel doit être signalé aussi rapidement que possible au supérieur hiérarchique ainsi qu'à la DSIT, en fournissant le nom de l'utilisateur directement concerné, le modèle de l'appareil, la nature des informations contenues, la date du vol ou de la perte, ainsi que toutes autres informations pertinentes.

L'utilisateur ne doit pas installer de logiciels sans la validation de la DSIT, ni copier ou installer des fichiers susceptibles de créer des risques portant atteinte à la sécurité de la Ville et du CCAS de Saintes.

L'utilisateur veille au respect de la confidentialité des informations en sa possession. Notamment dans le cadre de ses déplacements professionnels, peu importe leur durée ou leur fréquence, l'utilisateur se doit d'adopter une attitude de prudence et de réserve au regard des informations et des ressources du système

d'information qu'il pourrait être amené à accéder, manipuler ou échanger. En particulier, il est déconseillé d'utiliser les systèmes de connexion wifi dans les lieux publics.

L'utilisateur s'oblige en toutes circonstances à se conformer à la législation, qui protège notamment les droits de propriété intellectuelle, le secret des correspondances, les données personnelles, les systèmes de traitement automatisé de données, le droit à l'image des personnes, l'exposition des mineurs aux contenus préjudiciables. Il ne doit en aucun cas se livrer à une activité susceptible de causer un quelconque préjudice en utilisant le système d'information et Télécoms.

6. USAGES PROFESSIONNEL ET PERSONNEL DES EQUIPEMENTS

6.1. USAGE PROFESSIONNEL

Les outils de communication et les ressources informatiques (internet, téléphonie, messagerie, postes de travail) sont mis à disposition des utilisateurs pour un usage professionnel, en tant que moyens utiles à l'accomplissement des missions qui leur sont confiées par la Ville et le CCAS de Saintes.

Toutes données contenues dans ces moyens informatiques (fichiers, mails, images, etc.) sont considérées comme étant professionnelles et demeurent la propriété du CCAS de Saintes. Dans certaines conditions avec l'accord de l'agent, la Ville et le CCAS de Saintes pourront accéder à certaines données (Continuité de services).

6.2. USAGE A TITRE PRIVE OU PERSONNEL

Il est rappelé que l'usage reste professionnel mais de manière ponctuelle et marginale une tolérance est acceptée pour une utilisation plus personnelle de l'outil numérique en conformité avec les lois en vigueur, il est notamment interdit :

- D'utiliser son adresse mail professionnelle à des fins d'usages personnelles (création de profils, compte sur internet),
- D'effectuer des téléchargements illicites ou d'accéder à des sites illégaux, jeux et commerce en ligne,
- De porter préjudice à l'image de la Ville et du CCAS de Saintes,
- De perturber son activité professionnelle ou celles des autres agents.

De façon exceptionnelle, l'enregistrement des données doit s'effectuer dans un dossier nommé « Personnel » ou « Privé ».

6.3. MESURES :

Dans l'hypothèse d'une utilisation des moyens informatiques non-conforme à la charte informatique, la responsabilité personnelle de l'utilisateur pourrait être engagée.

La DSIT sur instruction de la Direction Générale se réserve le droit de restreindre ou suspendre cette utilisation privée sans préavis, en cas de danger pour le système d'information (accès à des sites réputés dangereux ou illégaux, attaques virales, intrusions, etc.) et de prendre les mesures nécessaires pour rétablir les ressources informatiques à un niveau compatible avec l'activité de la Ville et du CCAS de Saintes.

7. UTILISATION DU SYSTEME D'INFORMATION ET DES OUTILS DE COMMUNICATION

7.1. LA MESSAGERIE ELECTRONIQUE

Chaque agent dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique attribuée par la Ville et le CCAS de Saintes. L'utilisateur doit savoir qu'elle a la même portée qu'un courrier postal. Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les agents sont invités à informer la direction informatique des dysfonctionnements qu'ils constateraient dans ce dispositif de filtrage.

Les utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits des tiers. Les correspondances ne doivent pas comporter d'éléments illicites, tels que des propos diffamatoires, injurieux. L'utilisateur se doit de contrôler les informations contenues lors de ses envois car elles ne doivent en aucun cas engager la responsabilité civile ou pénale de la Ville et du CCAS de Saintes.

Les messages à caractère personnel sont tolérés, à condition de respecter les principes posés dans la présente charte (cf. 6.2). En cas d'usage privé, les messages envoyés doivent être signalés par la mention « Privé » ou « Personnel » dans leur objet, et être classés dès l'envoi dans un dossier lui-même dénommé de la même façon. Les messages reçus doivent également être classés, dès réception, dans un dossier lui-même dénommé « Privé » ou « Personnel ». En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.

7.2. INTERNET

Dans le cadre de leur activité, les utilisateurs peuvent avoir accès à Internet. Pour des raisons de sécurité, l'accès à certains sites peut être limité ou prohibé. La Ville et le CCAS de Saintes sont habilité à imposer des configurations du navigateur et à restreindre le téléchargement de certains fichiers/sites. Toute trace sera exploitable à des fins de statistiques, contrôle et vérification dans les limites prévues par la loi, en particulier en cas de perte importante de bande passante, sur demande de la Direction Générale.

Il est rappelé aux utilisateurs que l'usage d'Internet est réservé à des fins professionnelles (réf : 6.2).

7.3. LA TELEPHONIE

Il est rappelé que l'usage des appels téléphoniques, reste professionnel mais l'utilisation à caractère personnel du téléphone, fixe ou mobile, est tolérée, à condition qu'elle reste dans des limites raisonnables en termes, tant de temps passé, que de quantité d'appels (Réf 6.2).

Il est rappelé que l'envoi de SMS est réservé aux échanges professionnels et qu'il engage la responsabilité de l'émetteur et donc de la Ville et du CCAS de Saintes, au même titre que l'envoi d'un courriel. Il est donc soumis aux mêmes règles rappelées plus haut.

7.4. L'ESPACE DE STOCKAGE

L'espace de stockage de chaque agent se partage en 3 répertoires distincts :

- L'espace de travail propre à l'agent ;
- L'espace de travail partagé avec son service (organisé par l'agent et son service) ;
- L'espace de travail et d'échange avec d'autres utilisateurs du réseau interne.

Seuls ces espaces sont sauvegardés par la DSIT. Tout autre répertoire hors de ces espaces ne pourra faire l'objet d'une demande de restauration.

L'espace de stockage dédié aux utilisateurs n'est pas illimité. Il est nécessaire de vous rapprocher de la DSIT pour tout volume supérieur à 2 Go.

7.5. LES DOCUMENTS ET DOSSIERS PAPIER

Chaque agent s'engage, pendant ses absences, à ranger les documents et les dossiers sensibles notamment ceux des usagers dans des espaces protégés (armoires ou bureau fermés à clé, etc…). Les documents et dossiers jugés sensibles (niveaux 1, 2 et 3 de la classification) ne doivent pas sortir des locaux de la Ville et du CCAS de Saintes à moins d'une validation de la hiérarchie. Lorsque l'agent est amené à emporter des documents contenant des données jugées sensibles, il s'engage à prendre toutes les mesures nécessaires pour éviter qu'ils ne soient perdus ou volés (sans surveillance dans une voiture, sans possibilité de lecture par des personnes non habilitées, etc…).

7.6. LES LOGICIELS

L'autorisation d'accès à un logiciel est soumise à une demande d'habilitation en complétant la fiche d'arrivée de l'agent transmise par sa hiérarchie ou bien dans le cadre des missions qui lui sont confiées et fait ainsi l'objet de restrictions (fonctionnalités du logiciel, périmètre d'accès aux données). Ce dernier ne doit pas utiliser ou tenter d'utiliser les logiciels en dehors du cadre d'habilitations, ou pour des finalités autres que celles pour lesquelles il a été autorisé.

7.7. UTILISATION DE NOUVELLES RESSOURCES

L'utilisateur n'est en aucun cas habilité à installer des logiciels, programmes ou nouveaux équipements. L'installation de logiciels sur des ordinateurs ou outils de mobilité reliés au réseau informatique de la Ville et du CCAS de Saintes est de la compétence exclusive de la DSIT. L'utilisateur se doit d'en faire la demande auprès du centre de services de la DSIT.

7.8. UTILISATION DES CERTIFICATS ELECTRONIQUES

L'utilisation d'un certificat électronique remis à l'utilisateur pour viser ou signer électroniquement les documents, a la même valeur probante qu'une signature manuelle, conformément à sa délégation de signature. À ce titre, un certificat représente personnellement son porteur.

Il est matérialisé par une clé d'authentification sur support USB, auquel est associé un code PIN. L'ensemble est placé sous l'entière responsabilité de son porteur qui doit en faire un usage strictement professionnel, et prendre toutes les précautions qui s'imposent pour sa sécurité. En cas de perte, de vol ou de départ,

l'utilisateur a obligation d'informer dans les plus brefs délais, la DSIT et le cas échéant le RSSI et le DPO afin qu'il soit procédé à une demande de révocation du certificat auprès de l'autorité de certification compétente.

7.9. LE TELETRAVAIL

Après autorisation à télétravailler, l'agent s'engage à utiliser le matériel dans le respect des règles de sécurité en matière d'informatique. L'agent est responsable du matériel mis à sa disposition. Il assure la mise en place des matériels et leur connexion au réseau à son domicile.

En cas de défaillance technique, l'agent devra contacter le centre de services et suivre les instructions. Les agents de la DSIT ne sont pas habilités à se déplacer au domicile de l'agent.

Le télétravailleur doit avoir une exigence particulière sur son environnement de travail pour s'assurer d'un niveau de sécurité identique à celui pratiqué à la Ville et au CCAS de Saintes. Dans tous les cas, il devra se conformer à l'engagement de confidentialité et de protection des données dans le cadre du télétravail en vigueur à la Ville et au CCAS de Saintes.

7.10. LES CONNEXIONS A DISTANCE ET LE NOMADISME

Par outil de mobilité (ou nomade), on entend tout support numérique permettant de travailler en dehors de son bureau (ordinateur portable, smartphone…). Les tablettes tactiles et les smartphones sont des outils attitrés individuellement à l'utilisateur dans le cadre de ses missions et pour un usage exclusivement professionnel.

La présente charte engage ce dernier à mettre en œuvre toutes les mesures possibles pour :

- S'assurer de ne pas laisser les équipements dans un endroit sans surveillance afin d'en prévenir le vol ;
- Protéger les équipements contre les chocs, et les manipuler avec le plus grand soin ;
- Ne jamais divulguer à quiconque son code PIN, ni son mot de passe de connexion au réseau et/ou aux applications métiers installées sur les appareils ;
- Avertir le centre de service de la DSIT, le RSSI ou le DPO, en cas de perte ou de vol, afin qu'il soit procédé, si possible, à un blocage ou à un effacement à distance des données présentes sur le matériel, ainsi qu'à une évaluation de l'impact lié à la perte des données concernées ;

7.11. L'IMPRIMANTE / LES PHOTOCOPIEURS MULTIFONCTIONS

L'utilisation d'imprimantes ou de photocopieurs multifonctions est destinée uniquement à l'usage professionnel. L'utilisation du mode noir et blanc, en recto/verso, doit être privilégié plutôt que l'usage du mode couleur dont le coût est 10 fois supérieur.

8. SUPPRESSION DES ACCES

Les autorisations d'accès au réseau seront supprimées ou suspendues dans les cas suivants :

- Départ définitif de la Ville et du CCAS de Saintes : Suppression de l'accès après le départ de l'agent et après information transmise par le service des ressources humaines (Procédures Arrivée et Départ de l'agent);

- Départ temporaire de la Ville et du CCAS de Saintes : Détachement dans une autre collectivité, mise à disposition, disponibilité, tout congé de maladie ou tout accident, après information transmise par le service des ressources humaines ou du service d'affectation ;
- En cas de sanction disciplinaire : En fonction des règles en vigueur et en concordance avec le service des ressources humaines de la Ville et du CCAS.

9. DROIT A LA DECONNEXION

Le droit à la déconnexion s'entend comme le droit pour tout agent de ne pas être connecté à un outil numérique professionnel en dehors de son temps de travail.

Ce droit, qui s'inscrit dans une démarche d'amélioration des conditions de travail et d'une meilleure conciliation entre la vie professionnelle et la vie personnelle, a pour objectif le respect des temps de repos et de congé.

Ainsi, ce droit permet aux agents de ne pas répondre aux sollicitations professionnelles en dehors des horaires de travail sans risque d'être sanctionnés.

Ce droit est inscrit à l'article L. 2242-17 du Code du travail, modifié par la LOI N°2021-1018 du 2 août 2021.

10. PROTECTION DES DONNEES A CARACTERE PERSONNEL

10.1. DISPOSITIONS GENERALES

Le Règlement n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, communément appelé Règlement Général sur la Protection des Données (RGPD) est entré en vigueur le 25 mai 2018 en France. Le RGPD, complété par la Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa version consolidée du 14 juin 2018, impose les conditions dans lesquelles les traitements de données à caractère personnel peuvent être réalisés.

La Ville et le CCAS de Saintes sont soumis de plein droit au RGPD et à la désignation d'un Délégué à la Protection des Données à caractère personnel (DPD appelé aussi DPO) qui a pour mission de veiller au respect des dispositions au RGPD. Il a notamment pour rôle de s'assurer de la conformité juridique des traitements des données à caractère personnel.

Selon l'article 2 de la Loi Informatique et Liberté du 6 janvier 1978, est considérée comme une donnée à caractère personnel « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne ».

Le « responsable de traitement » est celui qui détermine les finalités et les moyens du traitement, c'est celui qui a pris l'initiative du traitement. A ce titre, la Ville et le CCAS de Saintes sont responsables de traitement.

10.2. DROITS EN MATIERE DE PROTECTION DES DONNEES

La Loi Informatique et Libertés et le RGPD instituent des droits que la présente charte vient protéger et respecter, tant à l'égard des utilisateurs que des personnes concernées par le traitement.

A cet égard, la Ville et le CCAS de Saintes soumettent leurs utilisateurs à :

- Ne pas utiliser les données à caractère personnel auxquelles ils peuvent accéder à des fins autres que celles prévues par leurs attributions ;
- Ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication ;
- Ne faire aucune copie de ces données sauf si cela est nécessaire à l'exécution de leurs fonctions ;
- Prendre toutes les mesures conformes aux usages dans le cadre de leurs attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- Respecter les droits des personnes concernées, à savoir :
    - Le droit d'accès ;
    - Le droit de rectification ;
    - Le droit d'opposition ;
    - Le droit d'effacement ;
    - Le droit à la portabilité ;
    - Le droit à la limitation ;
    - Le droit à l'image.

Les utilisateurs sont également informés que les données à caractère personnel les concernant sont conservées par la Ville et le CCAS de Saintes pendant toute la durée de leur relation contractuelle et des délais en matière de prescription.

La Ville et le CCAS de Saintes s'engagent, et par voie de conséquence les utilisateurs, à respecter les principes fondamentaux de la protection des données à caractère personnel, à savoir notamment la minimisation de la collecte et la préservation de la confidentialité, de l'intégrité et de la sécurité des données à caractère personnel.

10.3. RESPECT DE LA PROTECTION INTELLECTUELLE

Les ressources mises à disposition par la Ville et le CCAS de Saintes (site Internet, logiciels, CD-Rom, etc...) contiennent des informations protégées, sauf mention explicitement contraire, par le droit d'auteur. Toute reproduction ou diffusion, totale ou partielle, sous quelque forme que ce soit, de ces informations est possible mais uniquement dans les conditions prévues par le code de la propriété intellectuelle (article L.122-4 du Code de la propriété intellectuelle française).

Seule une copie de sauvegarde des logiciels commerciaux est possible dans les conditions prévues par le code de la propriété intellectuelle et ne peut être effectuée que par le service en charge du système d'information.

De plus, lorsque des données venant de l'extérieur sont utilisées par un agent, la source doit être citée sur le document numérique (dans le cadre d'un diaporama ou du SIG par exemple).

11. ADMINISTRATION DU SYSTEME D'INFORMATION

L'administrateur système, membre de la DSIT, gère la sécurité des machines connectées au réseau informatique ainsi que les serveurs sur lesquels sont installés les différents services mis à la disposition des utilisateurs. Il veille à assurer le meilleur service rendu aux utilisateurs dans la limite des moyens alloués.

Il lui appartient d'entreprendre toute démarche nécessaire au bon fonctionnement des ressources informatiques dans la limite des dispositions légales relatives à la protection des données privées de l'utilisateur. Il doit informer, autant que possible, les utilisateurs de toute intervention nécessaire, susceptible de perturber ou d'interrompre l'utilisation habituelle des ressources informatiques.

Il doit, de plus, informer immédiatement le RSSI de toute tentative d'intrusion sur le système ou de tout comportement délictueux d'un utilisateur. Il ne doit pas porter atteinte à la vie privée des utilisateurs. Cette obligation de discrétion concerne aussi bien le contenu de tout message à caractère privé dont les dispositions sont couvertes par le secret des correspondances que de tout fichier à caractère privé dont les dispositions relèvent de la vie privée des utilisateurs.

12. PRISE DE MAIN A DISTANCE

Ces outils permettent d'accéder à distance à l'ensemble des données informatiques de tout poste de travail connecté au réseau informatique.

Seul le personnel de la DSIT peut utiliser ces outils assurant ainsi la confidentialité des données auxquelles il accède. Le recueil de l'accord oral de l'utilisateur est nécessaire avant chaque prise de contrôle à distance d'un poste de travail.

Enfin, le DPO se réserve le droit de contrôler que ces opérations de maintenance demeurent conformes aux principes édictés dans la présente charte et aux politiques de sécurité en vigueur à la Ville et au CCAS de Saintes.

13. MODALITES DE CONTROLE

13.1. CONTROLES AUTOMATISES

Le système d'information et de communication s'appuie sur des fichiers journaux, créées en grande partie automatiquement par les équipements informatiques et de télécommunication. Ces fichiers sont stockés sur les postes informatiques et sur les serveurs. Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations de la Ville et du CCAS de Saintes, en détectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des utilisateurs et des tiers accédant au système d'information.

Les utilisateurs sont informés que des traitements peuvent être effectués afin de surveiller l'activité du système d'information et de communication.

13.2. PROCEDURE DE CONTROLE MANUEL

En cas de dysfonctionnement constaté par la DSIT, un contrôle manuel et une vérification de toutes les opérations effectuées par un ou plusieurs utilisateurs peuvent être réalisés.

Il peut porter sur les fichiers contenus sur le disque dur de l'ordinateur, sur un support de sauvegarde mis à sa disposition ou sur le réseau de la Ville et du CCAS de Saintes, ou sur la messagerie. Sauf risque ou évènement particulier, la Ville et le CCAS de Saintes peuvent ouvrir les fichiers ou messages identifiés par l'utilisateur comme personnels conformément à la présente charte, qu'en présence de l'utilisateur.

14. INFORMATIONS ET SANCTIONS

La Ville et le CCAS de Saintes, la DSIT, le RSSI et le DPO sont à la disposition des agents pour leur fournir toute information concernant l'utilisation du système d'information.

Chaque utilisateur doit se conformer aux procédures et règles de sécurité édictées par la Ville et le CCAS de Saintes dans le cadre de la présente charte. En cas de besoin, les agents pourront être accompagnés par la Ville et le CCAS de Saintes pour se conformer aux règles prévues. Il est rappelé que la présente charte est un document à portée juridique.

En effet, le manquement aux règles et mesures de sécurité décrites dans la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entrainer à son encontre des avertissements, limitations ou suspensions d'utiliser tout ou partie du système d'information et Télécoms de la Ville et du CCAS de Saintes, voire des sanctions disciplinaires proportionnées à la gravité des faits concernés.

La Ville et le CCAS de Saintes se réservent également le droit d'engager ou de faire engager des poursuites pénales et/ou civiles, indépendamment des sanctions disciplinaires mises en œuvre, notamment en cas de fraude informatique ou de violation du secret des correspondances.

15. DIFFUSION ET MISE EN APPLICATION

La présente charte est communiquée à l'ensemble des utilisateurs à leur première utilisation du système d'information par la direction élargie et les chefs de service de la Ville et du CCAS de Saintes. La charte est consultable à tout moment sur l'Intracom ou sur demande auprès du responsable de sécurité des systèmes d'information ou du service des ressources humaines.

Elle est remise contre-signature à chaque utilisateur et dispose par conséquent d'une valeur d'acte réglementaire. Elle est ainsi applicable et opposable à tous les agents, que ces derniers soient déjà en fonction au sein de la Ville et du CCAS de Saintes, au moment de sa conclusion ou qu'ils soient recrutés a posteriori.

Le formulaire de la charte signé par l'utilisateur sera conservé dans le dossier de l'agent au service des ressources humaines.

16. ENTREE EN VIGUEUR

La présente charte est communiquée individuellement à chaque utilisateur Elus, dirigeants, agents, les stagiaires. Elle doit être signée par chacun d'eux sur le formulaire transmis à cet effet. Elle sera applicable à compter du 1er janvier 2025.