RÉPUBLIQUE FRANCAISE

EXTRAIT DU REGISTRE DES DÉLIBÉRATIONS DU CONSEIL MUNICIPAL

Séance du 18 décembre 2023 à 20h30

Systèmes d'information, numérique, communication

12. Politique de sécurité des SI

Corentin GOETHALS donne lecture du rapport suivant :

Mes Chers Collègues,

En septembre 2021, l'intercom de la Vire au Noireau a débuté le parcours de cyber sécurité que nous a proposé l'ANSSI (Agence Nationale de Sécurité de Systèmes d'Information) dans le cadre de France Relance. Ce parcours s'applique à nos systèmes d'information mutualisés et bénéficie donc aux 3 collectivités qui les partagent dans le cadre de la mutualisation.

Après un pré diagnostic permettant de nous situer, nous avons réalisé le « pack initial » financé à 100 % soit 40 000 € TTC, qui a permis d'évaluer notre indice de cyber sécurité et d'établir un plan de sécurisation.

En octobre 2022, nous avons initié les premières actions (packs Relais) pour un montant de 70 000 € TTC financé à hauteur de 50 000 € TTC par l'ANSSI. Ces packs comprenaient des actions techniques et des actions organisationnelles. Parmi ces actions, deux actions constituent donc le socle de nos actions en terme de sécurisation :

- La rédaction d'une politique de sécurité des Systèmes d'Information (PSSI) qui est notre feuille de route.
- La nomination, au sein de la DSI, d'un Responsable de la Sécurité des Systèmes d'Information (RSSI) pour, au minimum, 25 % d'un ETP et qui pilotera la mise en œuvre de notre PSSI.

La PSSI a été rédigée et les collectivités doivent maintenant y adhérer pour que cette politique de sécurité vive et soit appliquée dans notre quotidien.

Pour reprendre la définition de l'ANSSI, « La PSSI reflète la vision stratégique de la direction de l'organisme en matière de sécurité des systèmes d'information (SSI) ». Elle est un élément fondateur de la sécurité des SI définissant les objectifs à atteindre et les moyens accordés pour y parvenir.

Pour résumer, la PSSI est un document cadre nécessaire à sécurisation de notre système d'information, qui doit être connu de tous, partagé, et qui doit guider l'ensemble des actions qui ont un impact sur la sécurité de notre système d'information. C'est dans ce sens qu'il doit être approuvé pour le conseil Municipal.

La PSSI est composée d'annexes techniques, de procédures à mettre en œuvre et de chartes de sécurité. En effet, la PSSI énonce des mesures techniques générales qui constituent un socle minimal. Pour certaines applications, ce socle minimal ne devra pas être considéré comme suffisant. Une charte d'utilisation de l'informatique est donc aussi nécessaire pour définir le comportement adéquat de tous les acteurs qui interagissent avec le système d'information. Cette charte devient un élément du règlement interne de chaque

collectivité et son application ne peut être contestée. Une charte d'utilisation a donc été rédigée pour chaque collectivité afin de définir un usage responsable et sûr du système d'information.

Pour chaque aspect, les principes de la bonne utilisation sont décrits, puis les dispositions et obligations sous forme d'une liste de ce qui doit être fait et de ce qui ne doit pas être fait. La charte se termine par une section plus pédagogique présentée sous forme de questions et réponses.

La charte informatique, une fois qu'elle aura fait l'objet d'une délibération du conseil municipal ou communautaire, deviendra immédiatement applicable. Si l'objectif premier reste de guider chacun vers une utilisation responsable du système d'information, le non-respect de la charte, surtout s'il est répété, peut donc donner lieu à des sanctions disciplinaires.

Vu l'article L.2121-29 du CGCT, le Conseil Municipal règle par ses délibérations les affaires de la commune.

Considérant l'avis favorable de la Commission Systèmes d'information, numérique, communication du 26 avril 2023,

Considérant l'avis favorable du Bureau Municipal du 05 Décembre 2023,

Il est demandé au Conseil Municipal, après en avoir délibéré à l'unanimité :

- D'approuver la mise en œuvre de la Politique de Sécurité des Systèmes d'Information (PSSI) présentée en annexe ;
- D'adopter la charte d'utilisation de l'informatique présentée en annexe en tant que règlement interne de la collectivité ;
- D'autoriser à cet effet, M. le Maire ou son représentant, ainsi que le Directeur Général des Services, à signer Politique de Sécurité des Systèmes d'Information (PSSI).
- De donner tous pouvoirs à Monsieur le Maire pour mettre en œuvre la présente délibération.

VOTE : Unanimité		Dont pouvoirs
Votants	44	8
Vote Pour	44	8
Vote Contre	0	0
Abstention	0	0

Arrêté en séance les jour, mois et an ci-dessus et ont signé au registre les membres présents.

Le Secrétaire de Séance

Dimitri RENAULT

Signé le 21/12/2023

Signé et certifié par yousign

L'adjointe au Maire de VIRE NORMANDIE,

Nicole DESMOTTES

Accusé de réception - Ministère de l'Intérieur

014-200060176-20231221-12-DE

Accusé certifié exécutoire

Réception par le préfet : 21/12/2023

Publication : 21/12/2023

Le Maire de VIRE NORMANDIE informe que le présent acte peut faire l'objet d'un recours pour excès de pouvoir devant le Tribunal Administratif de CAEN dans un délai de deux mois à compter de sa notification ou de sa publication

REPUBLIQUE FRANÇAISE

Extrait du Registre des Délibérations du Conseil Municipal

Nombre de membres en exercice : 47

Nombre de membres présents : 36

Quorum (24) : Atteint

Nombre de membres excusés : 09

Nombre de membres excusés ayant donné pouvoir : 08

Nombre de membres absents: 02

Le 18 Décembre 2023, le Conseil Municipal de Vire Normandie s'est réuni Salle des Mariages à l'Hôtel de Ville, sous la présidence de Nicole DESMOTTES, adjointe au Maire de Vire Normandie.

Les convocations individuelles et l'ordre du jour ont été transmis par mail et par courrier aux conseillers municipaux le 12 Décembre 2023.

La convocation et l'ordre du jour ont été publiés sur le site internet de Vire Normandie le 12 Décembre 2023.

Dimitri RENAULT a été nommé Secrétaire de Séance.

NOMS DES CONSEILLERS	Présent	Excusé	Absent	A donné pouvoir à
ANDREU SABATER Marc		☒		Nicole DESMOTTES
DESMOTTES Nicole	☒			
MALOISEL Gilles	☒			
VELANY Guy	☒			
CHÉNEL Fernand	☒			
GALLIER Pierre-Henri	☒			
MAINCENT Lyliane	☒			
GOETHALS Corentin	☒			
ROSSI Annie	☒			
PICOT Régis	☒			
MADELAINE Catherine	☒			
OLLIVIER Valérie	☒			
DROULLON Joël	☒			
BAZIN Lucien	☒			
LEMARCHAND Marie-Claire	☒			
FOUBERT Françoise	☒			
BALLÉ Marie-Noëlle	☒			
CORDIER Marie-Ange	☒			
ROBBES Martine	☒			
LE DRÉAU Nathalie	☒			
DUMONT Eric		☒		
COIGNARD Cindy		☒		Marie-Claire LEMARCHAND
MALLÉON Philippe	☒			

LETELLIER Nadine	☒			
LELARGE Michel	☒			
RENAULT Dimitri	☒			
MOREL Marie-Odile	☒			
GOSSMANN Patrick	☒			
BLANC Meiggie		☒		Philippe MALLÉON
VIGIER Maud			☒	
COURTEILLE Jacques	☒			
MASSÉ Aurélie		☒		Régis PICOT
BINET Samuel	☒			
BEDEL Sandra		☒		Marie-Ange CORDIER
LEFOUR Tony		☒		Gilles MALOISEL
LEFEBVRE Yoann			☒	
MARTIN Pascal	☒			
PIGAULT Jane	☒			
COUASNON Serge	☒			
DUVAUX Maryse		☒		Roselyne DUBOURGUAIS
DUBOURGUAIS Roselyne	☒			
FAUDET Olivier	☒			
RENAULT Régine		☒		Pascal MARTIN
TOULUCH Jean-Claude	☒			
LABROUSSE Sabrina	☒			
LEVERRIER Rosine	☒			
ALLEGRE Gilles	☒			

Vire Normandie

11, rue Deslongrais - CS 70076 Vire
14500 Vire Normandie

PSSI

mercredi 26 avril 2023

Vire Normandie

PSSI

Politique de sécurité des systèmes d'information de Vire Normandie

TABLE DES MATIERES

I. PRÉAMBULE : DÉCLARATION DE LA DIRECTION

Le système d'information (SI) remplit des fonctions indispensables de support aux activités de l'intercom de la Vire au Noireau, de la commune de Vire Normandie, et de son CCAS. Sa disponibilité doit être assurée à tout moment et en toutes circonstances.

Certaines informations qu'il traite sont particulièrement sensibles, et doivent être protégées de manière adéquate. Le système d'information doit garantir que ces informations restent authentiques et confidentielles. Son ouverture vers l'extérieur doit se faire dans un cadre sécurisé et maîtrisé.

Ces mêmes données sont exposées à des menaces et des risques réels, notamment de vol et de négligence, pouvant engager la responsabilité de tous.

En regard de ces risques, l'intercom de la Vire au Noireau, la commune de Vire Normandie, et son CCAS ont la responsabilité vis-à-vis des missions qui lui sont conférées de garantir un niveau de sécurité suffisant pour protéger les données qui lui sont confiées.

Elus et Directions de l'intercom de la Vire au Noireau, de la commune de Vire Normandie, et de son CCAS mobiliserons les moyens nécessaires à la mise en place et au fonctionnement de l'organisation de la sécurité du système d'information.

Pour relever ce défi, une démarche a dernièrement été lancée pour identifier les améliorations à apporter, élaborer et mettre en œuvre un plan d'action visant à permettre de maîtriser les risques.

La présente politique de sécurité du système d'information constitue le cadre unique de référence de l'intercom de la Vire au Noireau, de la commune de Vire Normandie, et de son CCAS pour toutes les questions de sécurité du système d'information.

Chacun doit veiller personnellement à sa bonne mise en application, et faire preuve de vigilance dans son usage des moyens de traitement des informations. Chaque responsable de service doit communiquer cette politique et s'assurer que les règles sont respectées au sein de son service.

A cette fin, je délègue au comité d'homologation SSI (voir composition en Annexe) la responsabilité de mettre à jour les orientations de la politique de sécurité, et je désigne Jocelyn Helie comme responsable de la sécurité du système d'information.

L'intercom de la Vire au Noireau, la commune de Vire Normandie, et son CCAS partagent le même système d'information au travers d'une convention qui met en commun les moyens et la gestion. Ils partagent donc les règles d'usage de ce système et les risques associés. Cette politique de sécurité des Systèmes d'information (PSSI) est donc également applicable pour les 3 collectivités, leurs élus et leurs agents.

Vire Normandie, le **[date]**

Le Maire de Vire Normandie	Le DGS de Vire Normandie
Le Président du CCAS de Vire Normandie	Le DGS du CCAS de Vire Normandie
Le Président de l'Intercom de la Vire au Noireau	Le DGS de l'Intercom de la Vire au Noireau

II. OBJET DE LA PSSI

Compte tenu de la transformation digitale des organisations, la protection de l'information et la sécurité des systèmes, des réseaux, des applications et des données de la structure représente un enjeu hautement stratégique devant permettre de préserver et de garantir ses intérêts et ses activités.

La politique de sécurité du système d'information (PSSI) a ainsi pour objet de définir les directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection et la sécurisation du système d'information d'une organisation. La PSSI vise également à s'assurer de la conformité avec les bonnes pratiques et les recommandations des autorités compétentes (ANSSI, CNIL, ARCEP, etc.) et les obligations légales.

Ainsi, la PSSI de l'intercom de la Vire au Noireau, de la commune de Vire Normandie, et de son CCAS est un document de référence, validé et appuyé par les élus et la direction, qui doit être pris en compte pour l'ensemble des projets et par tous les acteurs et utilisateurs du système d'information.

La PSSI est aussi un instrument de sensibilisation qui doit être largement communiquée à l'ensemble des acteurs du SI, qu'ils soient utilisateurs internes, externes, sous-traitants, prestataires ou stagiaires.

Elle explicite les principaux enjeux de la sécurisation du système d'information pour la collectivité et fixe les exigences et les règles de sécurité qui permettent d'assurer cette sécurisation, dans une démarche d'amélioration continue, afin de pérenniser le niveau de sécurité.

Elle sert aussi de base à la factorisation des études de sécurité portant sur le même périmètre que la PSSI afin de garantir une cohérence globale.

Par ailleurs, la PSSI est composée d'annexes techniques, de procédures à mettre en œuvre et de chartes de sécurité. En effet, la PSSI énonce des mesures techniques générales, qui constituent un socle minimal. Pour certaines applications, ce socle minimal ne devra pas être considéré comme suffisant. Chaque direction s'appuiera sur la PSSI, sur les normes existantes et sur les guides techniques de l'ANSSI pour élaborer des mesures techniques détaillées.

Les différentes mesures qu'elle prévoit sont destinées à être mises en œuvre de manière graduelle, définie par un Plan d'Action Sécurité, afin de permettre une progression de la sécurité du système d'information soutenable par la structure et d'atteindre à terme les objectifs de sécurisation fixés

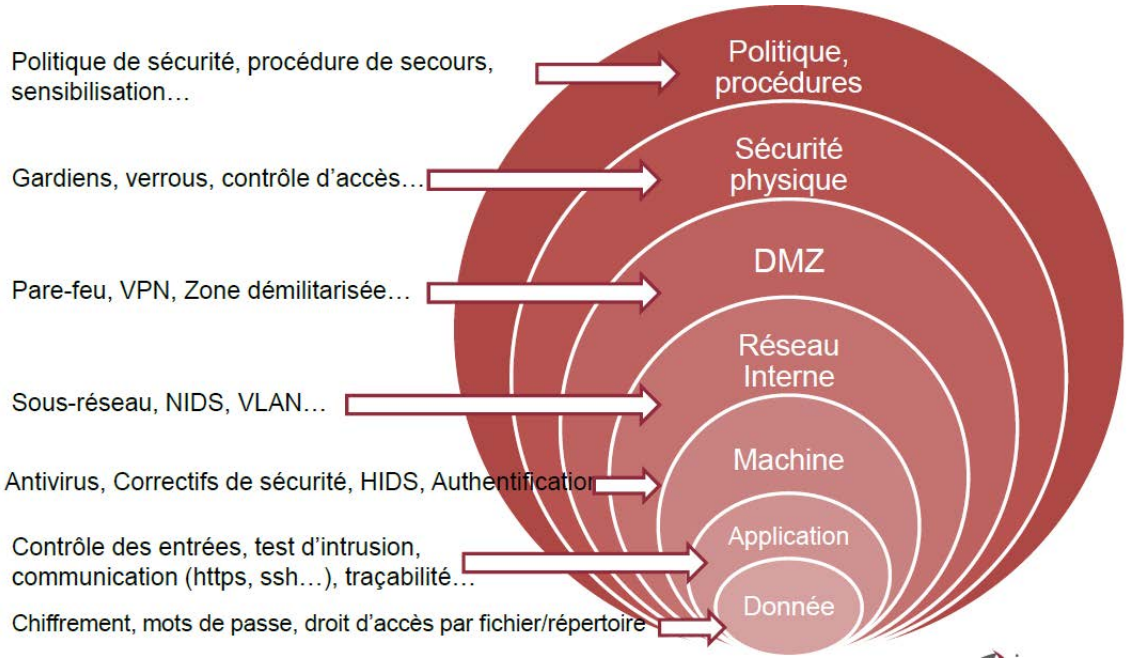
.

III. CHAMPS D'APPLICATION

Le périmètre d'application de la PSSI est le système d'information de l'intercom de la Vire au Noireau, de la commune de Vire Normandie, et de son CCAS et plus précisément :

- Les équipements mis à disposition des utilisateurs par la DSI (PC, terminaux mobiles, imprimantes, tablettes, supports de stockage externes, etc.) ;
- Les applicatifs métiers mis à disposition des utilisateurs par la DSI ;
- Les ressources transversales systèmes et réseaux locaux, distants et Internet, supports des services du SI ;
- Les utilisateurs du système d'information aussi bien personnel des collectivités (élus, agents titulaires, contractuels, stagiaires, saisonnier, ...) que les tiers utilisateurs (les associations, les élèves du conservatoire, les adhérents de la bibliothèque, etc.)
- Les organismes extérieurs (partenaires, prestataires, etc.) à la collectivité, susceptibles de se connecter, d'utiliser ou d'intervenir sur le SI ;
- Les bâtiments sensibles (cf. Annexe 4);
- Les locaux hébergeant les ressources informatiques (salles informatiques, baies de brassage, locaux techniques, etc.) (cf. Annexe 4) ;
- Les ressources numériques dédiés et isolées mises à disposition des communes, d'associations, entreprise, délégataire etc. ;
- Les ressources informatiques mises à disposition de tiers dans le cadre de prestations contractualisées.

Le dispositif de sécurisation s'appuie sur un modèle de défense en profondeur illustré ci-dessous :



IV. CONTEXTE

1. Enjeux de sécurité liés au SI

Le système d'information de l'intercom de la Vire au Noireau, de la commune de Vire Normandie, et de son CCAS devient de plus en plus :

- Connecté : ils intègrent la gestion des équipements informatiques et l'exploitation des informations qu'ils produisent, les demandes d'accès au système d'information se diversifient avec l'usage de terminaux « mobiles » (smartphones, tablettes, ordinateurs portables) ;
- Ouvert : pour favoriser la coordination entre directions et apporter plus de valeur ajoutée au travers de services du SI ;
- Mutualisé dans le cadre d'une offre de service potentiel auprès des communes ;
- Evolutif à l'image du dynamisme de la collectivité, il prend en compte la prise en charge de nouveaux bâtiments et compétences. Il se doit pour autant de rester homogène, performant et conforme à la règlementation,

Le système d'information s'appuie sur un ensemble de plus en plus grand de dispositifs, interconnectés ou cohabitants, au service des utilisateurs et usagers pour le bénéfice d'une meilleure prise en charge des attentes et d'amélioration du système d'information.

Levier d'amélioration de la qualité des services délivrés et d'efficience, il s'accompagne d'un accroissement significatif des vulnérabilités, des menaces et des risques d'atteinte aux informations conservées sous forme électronique et en conséquence aux processus s'appuyant sur le système d'information. L'origine de ces menaces peut être intentionnelle (développement de la cybercriminalité, acte de malveillance d'un utilisateur du système d'information), ou involontaire (faille technique, manque de sensibilisation des utilisateurs, etc.).

Dès lors, la sécurité du système d'information est une condition indispensable pour garantir une bonne prise en charge des attentes et une gestion intègre du SI de l'intercom de la Vire au Noireau, de la commune de Vire Normandie, et de son CCAS.

La maîtrise de la sécurité des systèmes d'information doit être intégrée tout au long du cycle de vie de ces systèmes. Elle doit s'appliquer aux dispositifs et applications en place, et accompagner l'intégration des nouvelles applications.

Elle doit prendre en compte l'évolution des facteurs, tant internes et qu'externes, qui sont susceptible de l'impacter : usage au quotidien des informations dématérialisées, stockage d'informations à caractère personnel rendu facilement accessible, responsabilité de l'organisme quant au respect du RGPD.

Elle doit en outre garantir la disponibilité des services du système d'information et offrir un socle de données fiables, intègres, et dont la confidentialité est protégée chaque fois que nécessaire.

La sécurité informatique doit s'inscrire dans une démarche « qualité » et de maîtrise globale des risques, en recherchant l'adhésion des utilisateurs. Il est important de conserver à l'esprit que la capacité de protection et de réaction repose bien souvent in fine sur l'utilisateur.

2. Textes et documents de référence applicables

A. Cadre législatif et réglementaire

Le système d'information de l'intercom de la Vire au Noireau, de la commune de Vire Normandie, et de son CCAS se doit de respecter les lois, codes et règlement en vigueur applicables aux collectivités.

Plus spécifiquement, le SI de l'intercom de la Vire au Noireau, de la commune de Vire Normandie, et de son CCAS doit respecter les normes et textes de lois encadrant l'utilisation de moyens de télécommunications ainsi que la traçabilité des échanges conformément à la loi du 23 janvier 2006 relative à la lutte contre le terrorisme (dite « Loi Sarkozy »).

Par ailleurs, l'usage des dispositifs de vidéosurveillance est soumis aux codes et règlements suivant :

- Loi du 6 janvier 1978 modifiée en 2004 dite « loi informatique et libertés » ;
- Article n°10 de la loi n°95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité dite « loi Pasqua » et décret n°96-926 du 17 octobre 1996 ;
- Décret du 3 août 2007 définissant les nouvelles normes techniques applicables à la vidéosurveillance.
- Les autres règlements à respecter sont :
- Respect du secret professionnel.
- Respect de la vie privée.
- Respect de l'ordonnance n°2005-1516 relative aux échanges électroniques entre les usagers et les autorités administratives.
- Respect du décret de confidentialité n°2007-960 du 15 mai 2007.
- Respect du Règlement Général sur la Protection des Données (RGPD)
- La norme française NF Z 40-350 pour l'archivage physique
- La norme française NF Z 42-013 pour l'archivage électronique

B. Normes et documents de référence

Les textes qui doivent être pris en compte pour l'élaboration et la mise en œuvre de la PSSI sont :

- Référentiel Général de Sécurité (RGS) portant en particulier sur la signature électronique, l'authentification, la confidentialité et l'horodatage ;
- Label de confiance SecNumCloud de l'ANSSI concernant la qualification de prestataires de services d'informatique de confiance en nuage.
- La norme ISO 27002 : 2013 concernant les bonnes pratiques en matière de sécurité des systèmes d'information.

V. EXIGENCES DE SÉCURITÉ ET RÈGLES APPLICABLES

1. Format de présentation des exigences

A. Organisation des exigences par thématique

L'élaboration de la PSSI est architecturée conformément à la norme ISO 27002 : 2013 qui définit une liste d'objectifs et de bonnes pratiques en matière de sécurité des systèmes d'information.

Les exigences de la PSSI sont structurées selon 7 thématiques basées sur les 14 chapitres et les 114 mesures de la norme ISO 27002 : 2013 :

- Thématique 1 : Répondre aux obligations légales
- Thématique 2 : Promouvoir et organiser la sécurité
- Thématique 3 : Assurer la sécurité physique des équipements informatiques du SI
- Thématique 4 : Protéger les infrastructures informatiques
- Thématique 5 : Maîtriser les accès aux informations
- Thématique 6 : Acquérir des équipements, logiciels et services
- Thématique 7 : Limiter la survenue et les conséquences d'incidents de sécurité

Pour chaque thématique, une ou plusieurs sous-thématiques sont définies. Chacune d'elle énonce un ensemble d'exigences et de règles.

La table de correspondance entre les thématiques de la PSSI et les chapitres de la normes ISO 27002 :2013 sont les suivants :

Thématique PSSI	Articles NF ISO/CEI 27002 – janvier 2014 (ISO27002:2013)
T1 - Répondre aux obligations légales	18 - Conformité
T2 - Promouvoir et organiser la sécurité	5 - Politiques de sécurité de l'information
	6 - Organisation de la sécurité de l'information
	7 - La sécurité des ressources humaines
T3 - Assurer la sécurité physique des équipements informatiques du SI	11 - Sécurité physique et environnementale
T4 - Protéger les infrastructures informatiques	8 - Gestion des actifs
	12 - Sécurité liée à l'exploitation
	13 - Sécurité des communications
T5 - Maîtriser les accès aux informations	9 - Contrôle d'accès
	10 - Cryptographie
T6 - Acquérir des équipements, logiciels et services qui préservent la sécurité du SI	14 - Acquisition, développement et maintenance des systèmes d'information
	15 - Relations avec les fournisseurs
T7 - Limiter la survenue et les conséquences d'incidents de sécurité	16 - Gestion des incidents liés à la sécurité de l'information
	17 - Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

B. Nomenclature

Chaque exigence et règle sont identifiées par un numéro de référence, constitué du numéro de thématique, du numéro de sous-thématique, du numéro de l'exigence concernée.

Exemple : la règle T6-4.B fait partie de la thématique T6, sous-thématique T6-4, exigence T6-4.B.

THÉMATIQUE 1 : RÉPONDRE AUX OBLIGATIONS LÉGALES

T1-1. Conformité aux obligations légales et réglementaires

T1-1.A. Respecter les obligations légales et réglementaires

Des procédures appropriées doivent être mises en œuvre pour garantir la conformité avec les obligations légales et règlementaires du système d'information.

Voir Annexe 5 - Documents et recommandations de référence

T1-1.B. Respecter les droits de propriété intellectuelle

Des procédures appropriées doivent être mises en œuvre pour garantir la conformité avec les droits de propriété intellectuelle et à l'usage des licences de logiciels propriétaires.

Les utilisateurs ne doivent pas pouvoir installer des logiciels non autorisés sur leur équipement informatique appartenant à la structure.

T1-1.C. Sensibiliser le personnel aux enjeux de la sécurité du SI et plus particulièrement aux enjeux concernant les données à caractère personnel

Toute personne doit être sensibilisée aux enjeux de la sécurité du SI et aux risques encourus.

Toute personne amenée à participer à un traitement de données à caractère personnel doit être sensibilisée aux principes de protection de ce type de données.

Cette sensibilisation doit être renouvelée périodiquement et a minima 1 fois par an.

T1-1.D. Respecter les principes de la protection des données à caractère personnel

Tout responsable de traitement ne peut mettre en œuvre un traitement automatisé contenant des données à caractère personnel qu'après s'être assuré du respect des formalités préalables applicables, le cas échéant, à la mise en œuvre du traitement.

Les utilisateurs devront se rapprocher du DPO en cas de nouveaux traitements pour renseigner les fiches de traitement de données associées et mettre en place les mesures techniques et organisationnelles appropriées pour assurer la protection des données de manière effective.

En cas de doute ou de difficulté, le responsable de traitement doit se rapprocher du DSI pour disposer de son avis consultatif.

Tout traitement de données à caractère personnel doit faire l'objet d'une fiche dans le registre des traitements, charge aux responsables de traitement de les maintenir à jour.

T1-1.E. Respecter les droits des personnes

Exigences : Toute personne dont des données à caractère personnel sont traitées par la structure doit pouvoir exercer les droits qui y sont associés : droit à l'information, droit d'opposition, droit d'accès et droit de rectification.

Les procédures internes impliquant la collecte et le traitement de données à caractère personnel doivent prévoir une étape d'information des personnes concernées.

T1-1.F. Répondre aux obligations d'enregistrement, de conservation et de restitution des données à caractère personnel

Exigences : Toute donnée à caractère personnel ne doit être conservée que pendant une durée cohérente avec la finalité du traitement pour lequel elle a été collectée.

La durée de conservation des données à caractère personnel doit être fixée au préalable à leurs collectes.

T1-1.G. Respecter le référentiel général de sécurité (RGS)

Les règles formulées dans le RGS contribuant à la sécurité des informations, parmi lesquelles la signature électronique, l'authentification, la confidentialité ou encore l'horodatage doivent être respectées, et plus particulièrement pour la sécurisation des services en ligne l'intercom de la Vire au Noireau, de la commune de Vire Normandie, et de son CCAS sont responsable.

T1-2. Revue de la sécurité de l'information

T1-2.A. Assurer une veille réglementaire des dispositions applicables à la structure en matière de SSI

Une veille règlementaire des évolutions légales et règlementaires en matière de sécurité des systèmes d'informations doit être réalisée par le RSSI et le DPO, ainsi que les jurisprudences dans le domaine.

Les évolutions seront être traduite dans la PSSI si elle s'applique à la structure dans un délai approprié.

La PSSI sera révisée dans le cadre des COSSI.

T1-2.B. Vérifier la conformité technique du SI avec la réglementation

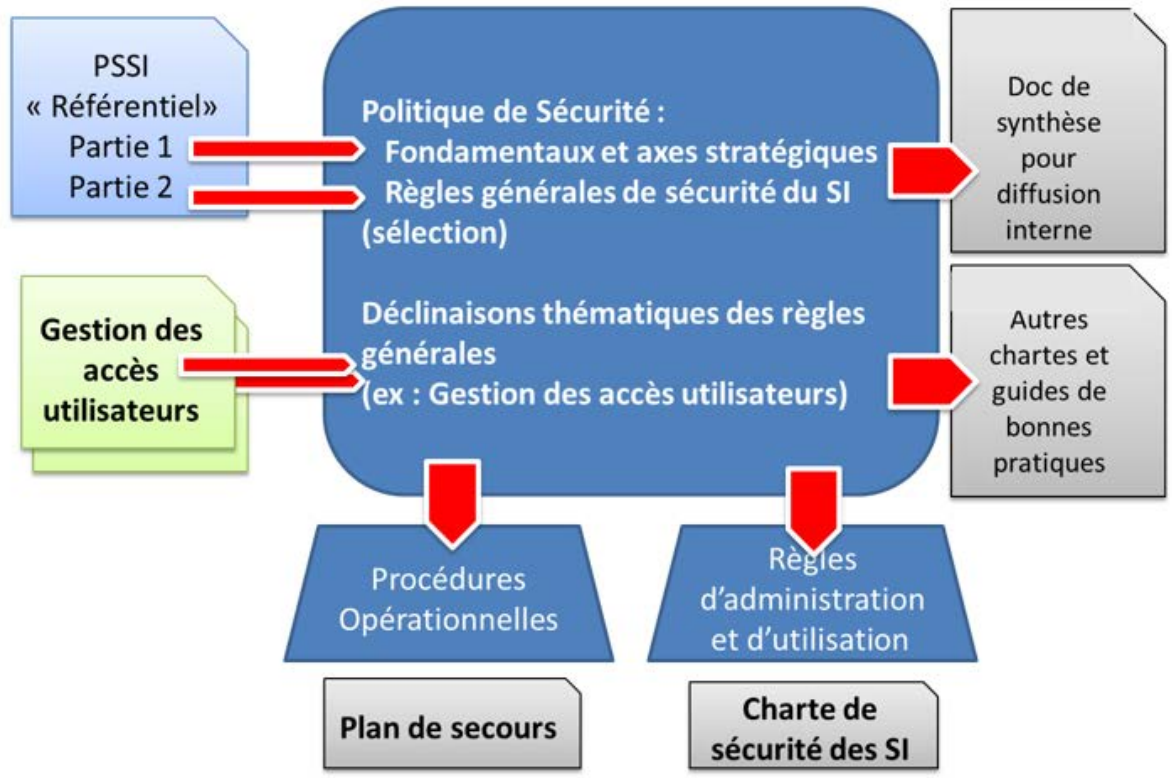
Le système d'information doit être examiné régulièrement quant à sa conformité avec les politiques et les normes de sécurité de l'information de l'organisation.

THÉMATIQUE 2 : PROMOUVOIR ET ORGANISER LA SÉCURITÉ

T2-1. Politique de sécurité du système d'information

T2-1.A. Définir et formaliser un ensemble de politique de sécurité du système d'information

Un ensemble de politiques de sécurité de l'information doit être défini, approuvé par la direction, diffusé et communiqué aux salariés et aux tiers concernés, comme l'indique le modèle présenté ci-dessous :



T2-1.B. Suivre et maintenir la politique de sécurité de l'information

Une procédure d'amélioration continue de la PSSI doit être définie, approuvé par la direction et appliquée.

La politique de sécurité de l'information doit avoir un responsable de sa mise en œuvre, de son suivi et de son évolution.

Il s'assure notamment :

L'examen périodique de l'efficacité de la politique de sécurité en termes :

- D'amélioration des dispositifs de sécurité du système d'information (sécurité des réseaux, gestion des habilitations…) ;
- De diminution des incidents et de leurs impacts sur le fonctionnement de la collectivité (diminution des arrêts, diminution des pertes de données…).

La prise en compte de l'évolution des activités et de l'organisation, ainsi que des nouveaux risques pesant sur le système d'information de l'intercom de la Vire au Noireau, de la commune de Vire Normandie, et de son CCAS.

La mise en conformité au RGPD et les mises à jour majeurs des chartes répondent aussi à cette exigence d'amélioration continue.

T2-2. Organisation interne de la sécurité du système d'information

T2-2.A. Identifier les acteurs de la politique de la sécurité de la structure et leurs activités

Au sein de l'intercom de la Vire au Noireau, de la commune de Vire Normandie, et de son CCAS, la responsabilité générale de la sécurité des systèmes d'information relève du Directeur Général des Services. Il est assisté dans cette fonction par le Responsable de la Sécurité des Systèmes d'Information (RSSI).

L'intercom de la Vire au Noireau, de la commune de Vire Normandie, et de son CCAS procèdent à la nomination d'un Responsable de la Sécurité des Systèmes d'Information (RSSI), dont les missions et responsabilités font l'objet d'une fiche de poste (voir les missions ci-dessous) et d'une délégation formelle du DGS, et dont les moyens d'action sont en rapport avec les missions confiées :

Le RSSI a un rôle de pilotage et de coordination pour la mise en œuvre, l'application et l'évolution de la politique de sécurité de l'information : il est le maître d'ouvrage des projets sécurité et participe à la sensibilisation des acteurs à la sécurité. Il n'intervient pas au niveau opérationnel mais en tant que maître d'œuvre des projets de sécurité. Il peut être assisté soit d'une petite équipe dont il a la responsabilité directe, soit de correspondants qui lui sont rattachés fonctionnellement.

Indépendamment de son rattachement hiérarchique, le RSSI est rattaché fonctionnellement au DGS, auquel il rend compte de son action.

Fonction	Missions
Le Maire	• Porte la responsabilité de la sécurité du SI • S'engage sur la disponibilité des ressources de la collectivité à mobiliser sur la SSI
ELU au Numérique	• S'engage à promouvoir la Politique de Sécurité du SI
DGS	• S'engage à appliquer l'orientation décidée par le Maire
DSI	• Soutient l'action du RSSI

	• Arbitre, valide • Rends compte de l'efficacité de la PSSI auprès de la DG
RSSI	• Avec le DSI, définir la politique de sécurité des systèmes d'information (PSSI) : Suivre la mise en place des procédures liées. • Définir les normes et les standards de sécurité, valider les outils de sécurité et effectuer le suivi des évolutions réglementaires et techniques. • Organiser l'information et la sensibilisation de tous les acteurs de la collectivité aux enjeux de la sécurité des SI : Elus, Direction Générale, équipes de la DSI, et utilisateurs. • Participer à l'élaboration de la charte d'utilisation des systèmes d'information, à sa promotion et à sa bonne application • Evaluer ou faire évaluer les risques, les menaces et leurs conséquences, prendre les mesures techniques et organisationnelles permettant la surveillance, l'appréciation de la sécurité et la réaction face aux cyberattaques (déclenchement de la cellule de crise). • Avec le DSI, proposer un plan de prévention des risques informatiques et un plan de reprise et de continuité informatique (PRI/PCI). • Réaliser ou faire réaliser des audits de sécurité du SI. • Collaborer avec le DPO (Délégué à la Protection des Données) pour la définition et la mise en œuvre des mesures techniques de mise en conformité avec le RGPD (Règlement Général pour la Protection des Données) • Effectuer une veille et un suivi des évolutions réglementaires et technologiques liées aux SI, des méthodes de protection et d'analyse du risque, et des menaces cyber afin de garantir le maintien de la sécurité du SI.
DPO	• Délégué à la protection des données à caractère personnel • Charger de conseiller et d'accompagner la structure dans sa conformité avec le RGPD
Equipes Techniques	• Déploient les mesures de sécurité dans leur domaine respectif
Direction des Services Techniques	• Gestion des infrastructures des bâtiments (électricité, climatisation, protection incendie, etc.) • En charge de la sécurité physique des bâtiments de la collectivité (contrôle d'accès, surveillance, etc.)
Comité SSI	• Le comité SSI rassemble les élus au numérique, les DGS, le DSI, le RSSI qui veille à la cohérence de la sécurité du SI global. • L'homologation doit permettre d'attester formellement que le SI est protégé conformément à la PSSI.

Les fonctions de sécurité au sein de la collectivité sont désignées en annexe n°1.

Les fonctions et responsabilité liées à la SSI sont en partie identifiées dans les fiches de postes.

T2-2.B. Séparer les tâches et domaine de responsabilité

Les tâches et les domaines de responsabilité incompatibles doivent être cloisonnés pour limiter les possibilités de modification ou de mauvais usage, non autorisé(e) ou involontaire, des actifs de l'organisation.

Pour les applications métiers, les référents métiers (RH, Finance, etc.) ont en charge l'attribution des droits et privilèges propres à leur métier suivant les recommandations de la PSSI.

T2-2.C. Sensibiliser, former et responsabiliser le personnel aux principes essentiels de sécurité informatique

La sensibilisation vise à faire prendre conscience à chaque utilisateur du système d'information qu'il détient une part importante de responsabilité dans la lutte contre les accidents, erreurs et malveillances.

La responsabilité des utilisateurs dans la lutte contre les accidents, erreurs et malveillances fait l'objet d'un énoncé clair et succinct quant :

- Au respect de la législation : le rappel des principales règles à respecter avec la mention du texte de référence;
- Aux consignes de vigilance à appliquer : les enjeux de la vigilance et les consignes essentielles d'alerte doivent être connues de tout le personnel.

Ainsi, toute personne en relation avec le SI de la structure doit être sensibiliser aux enjeux de la sécurité du SI et aux risques encourus. Cette sensibilisation doit être renouvelée périodiquement et s'inscrire dans un programme annuel.

Les chartes d'utilisation des ressources informatiques (cf. annexe 5) doivent être diffusées et validées à tout utilisateur du système d'information, qu'il s'agisse de personnel interne ou de tiers amenées à utiliser le SI ou à intervenir sur le SI.

La charte doit être annexée au règlement intérieur et être facilement accessible à l'ensemble des utilisateurs.

Pour toute mise à jour majeure de la charte informatique, une sensibilisation adaptée envers les utilisateurs doit être réalisée.

Les personnes en charge de l'administration et de l'exploitation des infrastructures et des applications du SI aussi bien à la DSI que dans les Directions métiers doivent être formées à la réalisation des tâches qui leur incombent, pour chacun des composants dont ils ont la charge.

De même, les utilisateurs du SI doivent être formés à l'utilisation des équipements et applications du SI qui leur sont destinés suivant leur niveau de droit et de privilège qui leur sont conférés.

T2-2.D. Rôle des Directions dans la sensibilisation et la responsabilisation des agents

Pour être efficace, la sensibilisation du personnel doit faire l'objet de rappels périodiques par les responsables des services (chefs de services, DGA, responsables d'encadrement). L'engagement de l'encadrement est un levier fort de la sensibilisation.

Ce rappel périodique peut être réalisé sous plusieurs formes : rappel des consignes, bilan annuel des incidents de sécurité avec rappel des consignes, ...

T2-2.E. Relation avec les autorités et acteurs de la sécurité numérique

Des relations appropriées avec les autorités compétentes doivent être entretenues (Gendarmerie, Préfecture, ANSSI, etc.).

Les relations avec la Gendarmerie sont assurées pour la vidéoprotection par la Direction des Services Techniques.

T2-2.F. Décliner les règles de la PSSI dans les procédures opérationnelles

La sécurité de l'information doit être considérée dans la gestion de projet conformément à la PSSI, quel que soit le type de projet concerné.

Les procédures de groupes de travail pour un projet donné doivent intégrer les aspects sécurité du SI conformément à la PSSI.

Lors de l'initialisation d'un projet donné, le responsable du projet doit compléter les informations projet intégrant les aspects SSI (données traitées, logiciels utilisées, besoin d'archivage, etc.).

Une sensibilisation particulière sur les enjeux de la sécurité du SI dans le cadre de projet doit être réalisée périodiquement par le RSSI, soutenue par la DSI et le service formation. Cette sensibilisation doit être adaptée suivant le niveau de risque encouru pour le projet donné.

T2-3. Sécurité des ressources humaines

T2-3.A. Décliner les règles de la PSSI dans les procédures liées aux ressources humaines

Avant l'embauche :

- Vérification du CV (contacter les anciens employeurs, vérifier les diplômes, certifications...) du candidat ;
- En fonction de la sensibilité du poste, un extrait de casier judiciaire peut être demandé.

Pendant l'embauche :

Droit d'accès : Les droits d'accès aux locaux, aux applications et aux ressources fichiers sont affectés en fonction du poste du nouvel agent (création de comptes utilisateurs, accès aux répertoires nécessaires, etc.) et physiques (badges, clé, etc.).

L'utilisateur concerné doit signer la charte informatique au préalable.

Préalablement à son accès aux outils informatiques, l'utilisateur doit être informé des droits et devoirs en matière de SSI que lui confère la mise à disposition par son entité de ces outils.

Cette information se fait au travers du règlement intérieur et plus particulièrement de la charte informatique (cf. annexe 5).

Sensibilisation : Une sensibilisation aux politiques et procédures internes de l'organisation et une sensibilisation régulière à la sécurité du SI adaptée aux fonctions doivent être réalisées par le RSSI, la DSI et le service formation.

Procédure disciplinaire : Une procédure disciplinaire formelle et connue de tous permet de prendre des mesures à l'encontre de l'agent, ou du stagiaire ayant enfreint les règles liées à la sécurité de l'information.

Dans le cas d'une mobilité externe :

- Retrait de tous les accès, les habilitations et restitution du matériel fourni (badge, ordinateur, etc.).

T2-3.B. Des procédures sont à établir entre la DRH et la DSI pour les arrivées, départs de personnes ainsi que pour les changements de poste

Les procédures d'embauche ou d'arrivée de personnel temporaire, de prise de fonction lors d'un mouvement interne, de départ que ce soit définitif ou pour mouvement interne doivent intégrer les aspects sécurité du SI.

Les informations d'arrivée, de départ et changement de poste doivent être transmises à la DSI par la DRH au minimum 15 jours avant la mise en application effective de ces accès. Progressivement, ce délai sera amené à un mois

Dans tous les cas, une demande doit être faite par le chef de service du nouvel agent, afin de lui affecter du matériel, des droits d'accès aux applications et aux ressources du service.

THÉMATIQUE 3 : ASSURER LA SÉCURITÉ PHYSIQUE DES ÉQUIPEMENTS INFORMATIQUES DU SI

T3-1. Sécurité physique et environnementale

T3-1.A. Contrôler l'accès physique aux locaux

Une protection physique adéquate des équipements informatiques est indispensable pour limiter les risques de dommages, accidentels ou malveillants, ou de vol.

La sécurité globale des bâtiments de la collectivité est gérée par la Direction des Services Techniques.

Un système de contrôle par badge permet de contrôler l'accès physique à l'entrée des locaux sensible de l'intercom de la Vire au Noireau, de la commune de Vire Normandie, et de son CCAS.

L'accès aux locaux techniques, ou équivalent, qui hébergent des équipements informatiques doit être limité aux seules personnes autorisées.

Plus particulièrement, les accès aux salles informatiques sont restreints uniquement aux personnes habilitées. Les salles informatiques sont équipées d'un dispositif de contrôle d'accès physique. Le personnel autre que celui explicitement autorisé et habilité, mais néanmoins appelé à intervenir dans les zones sensibles, intervient systématiquement et impérativement sous surveillance.

Quand les risques le justifient dans certains locaux, un dispositif d'alarme, voire de vidéo-surveillance, doit être mis en place.

T3-1.B. Assurer la protection physique des équipements informatiques

Les actifs matériels et logiciels doivent être recensés, affectés à un utilisateur ou à une entité. Les mouvements des actifs doivent également être suivis.

Les locaux informatiques (Cf. Annexe 4) seront dédiés et sécurisés en adéquation avec leurs criticités.

Tout équipement informatique installé dans une zone recevant du public doit être équipé d'un dispositif de sécurité adapté.

Tout accès réseau installé dans une zone d'accueil du public doit être filtré ou isolé du reste du réseau informatique de l'entité.

Les infrastructures de câblage électriques et réseaux supportant les services d'information doivent être protégées et transitées sur des chemins de câble et/ou gaines techniques conformes à l'état de l'art.

Les supports de données amovibles et documents papier sensibles doivent être protégés contre le vol et doivent être stocké dans un espace sécurisé adapté suivant la sensibilité des données qu'ils contiennent.

Par ailleurs, les supports informatiques contenant de l'information sensible doivent être protégés contre les accès non autorisés, les erreurs d'utilisation et l'altération lors du transport.

De manière générale, la sortie et l'utilisation à l'extérieur de l'entité de tout équipement informatique doivent avoir été au préalable autorisé.

Les salles informatiques sont équipées de dispositif de détection et d'extinction de feu.

T3-1.C. Assurer la disponibilité des équipements informatiques

Les infrastructures informatiques doivent être entretenues et maintenues pour garantir leur disponibilité et leur intégrité.

Pour les infrastructures informatiques nécessitant des niveaux de service spécifiques, des contrats de maintenance sont à prévoir auprès de tiers prestataires.

Alimentation électrique : Les infrastructures informatiques critiques (serveurs, équipements actifs, etc.) doivent être alimentées par du courant ondulé et/ou disposées de deux sources d'alimentation électrique différentes, si applicable.

Les onduleurs disposent d'une autonomie de 1h30 heures pour les salles informatiques. Les messages d'alerte sont transmis automatiquement au système de supervision de la DSI.

En cas de dépassement de coupure électrique persistante, les infrastructures informatiques critiques doivent être arrêtées proprement suivant la procédure établie.

Climatisation : Les salles informatiques (cf. Annexe 4) sont équipées de systèmes de climatisation (redondante pour les plus critiques). Les remontées de température et messages d'alerte sont transmis automatiquement au système de supervision de la DSI.

En cas de dépassement d'un seuil de température les infrastructures informatiques critiques doivent être arrêtées proprement suivant la procédure établie.

T3-1.D. Assurer la destruction de données au préalable à la mise au rebut ou recyclage

Une procédure formalisée doit être mise en place afin de garantir que tout matériel informatique en fin de vie voit l'ensemble des données qu'il contient effacées par une méthode adéquate afin d'éviter tout risque de divulgation accidentelle ou intentionnelle.

La méthode d'effacement utilisée doit être adaptée en fonction de la nature de l'équipement et de la sensibilité des données concernées, afin d'assurer un effacement efficace.

La destruction de données peut être réalisée par un partenaire de recyclage fiable utilisant des filières agréées afin d'avoir toutes les garanties de conformité à la législation environnementale.

La fourniture du BSDI (Bordereau de Suivi des Déchets Industriels) doit être réalisée par le partenaire.

THÉMATIQUE 4 : PROTÉGER LES INFRASTRUCTURES INFORMATIQUES

T4-1. Gestion des actifs

T4-1.A. Maitriser le parc informatique (serveurs, postes de travail, équipements, réseaux, etc.).

L'inventaire exhaustif des composants du SI est un prérequis à la sécurisation du SI : « on ne peut sécuriser que les équipements que l'on a identifiés ».

Ainsi, tout équipement informatique, connecté ou non au réseau du SI détenu par la structure, doit être identifié et recensé dans l'inventaire des composants du SI avec les informations utiles à sa gestion.

Par ailleurs, chaque équipement informatique doit être attribué à un propriétaire (nom AD affecté) à chaque fois que possible.

De même, tout système d'exploitation ou logiciel applicatif installé sur un équipement présent dans l'inventaire des équipements informatique du SI doit être identifié et recensé dans l'inventaire des composants logiciels du SI avec les informations utiles à sa gestion.

Les inventaires et les informations associées doivent être maintenus à jour au fil des ajouts, retraits et modifications des éléments qu'ils recensent.

Une revue régulière, au moins annuelle, de ces inventaires doit être organisée progressivement par la DSI afin d'identifier et de traiter les écarts entre inventaire enregistré et parc informatique constaté.

Cette revue doit également être l'occasion de vérifier que la structure est en règle vis-à-vis des licences dont elle dispose au regard des logiciels effectivement déployés sur les différents équipements.

Les règles de bonne utilisation de ces équipements sont précisées dans la charte informatique (cf. annexe 5).

T4-1.B. Cartographier le système d'information

Des schémas d'architecture logique et physique doivent permettre de visualiser et de localiser les composants techniques et applicatifs du système d'information.

Chaque responsable de projet doit réaliser le schéma d'architecture de son domaine ou mettre à jour les schémas de référence.

T4-1.C. Classifier les informations

Les informations traitées par le SI doivent être classifiées en termes d'exigences légales, de valeur, de disponibilité (accessibilité), d'intégrité (exactitude des données et paternité) et de confidentialité (sensibilité).

Des procédures pour le marquage de l'information doivent être élaborées et mises en œuvre conformément au plan de classification adopté par l'organisation.

La matrice d'évaluation est tenue à jour par le RSSI.

T4-2. Sécurité liée à l'exploitation

T4-2.A. Des procédures d'exploitation doivent être formalisées

Les systèmes et moyens de traitement de l'information doivent disposer de procédures d'exploitation.

Les procédures d'exploitation doivent être documentées et mises à disposition des utilisateurs concernés.

Une nomenclature des principales procédures d'exploitation doit être réalisée sous contrôle du RSSI. Ce dernier doit veiller à leur maintien à jour et à leur disponibilité.

A cet effet, les procédures d'exploitation doivent être stockées dans un espace GED organisé et dédié à cet usage.

Les procédures d'exploitation et en particulier celles qui ont des conséquences en matière de sécurité des systèmes d'information, doivent être progressivement documentées.

La documentation d'exploitation doit être tenue à jour.

Les procédures d'exploitation doivent indiquer les instructions détaillées pour l'exécution de chaque tâche d'exploitation. Il s'agira de progressivement rédiger et mettre en œuvre les procédures suivantes :

- Traitement et manipulation des données ;
- Ordonnancement des tâches ;
- Traitement des erreurs et autres procédures exceptionnelles d'exploitation, y compris les restrictions d'accès aux données ou les procédures et restrictions d'utilisation de certains utilitaires systèmes outrepassant les autorisations ;
- Procédures d'escalade et coordonnées des contacts en cas d'incident ;
- Instructions de manipulation de sorties spéciales, telles que l'utilisation de papeterie spécifique (papier de couleur, pré imprimé…) ou la définition de procédures de stockage et de destruction d'informations classifiées imprimées accidentellement suite à une erreur d'exécution ;
- Procédures de redémarrage et reprise sur incident des systèmes ;
- Sauvegardes d'exploitation et de secours ;
- Maintenance des systèmes ;

- Entretien et ménage des locaux informatiques ;

T4-2.B. Une procédure de gestion des changements doit être définie

Les changements envisagés sur l'organisation, les processus métier, les systèmes et moyens de traitement de l'information ayant une incidence sur la sécurité de l'information doivent être partagés et validés au préalable par le COPIL du projet et le RSSI.

A minima, les changements envisagés par les métiers doivent être partagés au préalable avec la DSI.

Les environnements de développement, de test et d'exploitation doivent être séparés pour réduire les risques d'impact d'un changement non autorisé sur l'environnement de production.

T4-2.C. Mettre en œuvre des mesures contre les logiciels malveillants

Une solution antivirale (actuellement WithSecure) doit être installée, activée et à jour pour protéger l'environnement du SI (postes de travail, serveurs physiques et virtuels, fichiers, etc.) contre les logiciels malveillants.

Une mise à jour des environnements logiciels est assurée régulièrement et plus particulièrement les logiciels critiques.

Les mises à jour de sécurité et les mises à jour critiques concernant les solutions Microsoft et l'antivirus WithSecure sont assurées automatiquement sur l'ensemble des postes de travail et des serveurs.

Les flux de messagerie électronique de l'intercom de la Vire au Noireau, de la commune de Vire Normandie, et de son CCAS sont protégés par les solutions de sécurité spécifiques d'anti-spam et d'anti-virus.

Les flux de navigation internet sont protégés par des solutions de sécurité et de filtrage (filtrages de flux, filtrages d'url, filtrage applicatifs, antivirus, IPS, etc.).

Les utilisateurs doivent être sensibiliser sur les dispositifs de prévention et de protection mis en œuvre sur leur environnement informatique.

T4-2.D. Les environnements du système d'information doivent être sauvegardés et archivés

Une politique de sauvegarde et d'archivage doit être définie et validée avec les parties prenantes. Elle doit stipuler les engagements en matière de sauvegarde et d'archivage des données (type de données, médias utilisés, fréquence et plages horaires des sauvegardes, durée de rétention, délai de restauration, etc.).

L'archivage de données doit se conformer à la réglementation en vigueur (cf.§.4.2.1 du document).

Les données audiovisuelles enregistrées par les systèmes de vidéosurveillance de la collectivité doivent être conservées de manière adéquate.

Des procédures de sauvegarde, d'archivage et de restauration doivent être formalisées (cf. annexe xx).

Les agents d'exploitation doivent s'assurer de la bonne exécution de chaque opération de sauvegarde et de chaque opération d'archivage, suivant les périodicités définies.

Des tests de restauration de fichiers doivent être réalisés à intervalle régulier.

T4-2.E. Une journalisation et une surveillance des activités informatiques doivent être assurées

Le SI doit comprendre des dispositifs ou procédures de journalisation centralisée et protégée de l'utilisation des services.

Des journaux d'événements enregistrant les activités de chaque profil utilisateur, les exceptions, les défaillances et les événements liés à la sécurité de l'information doivent être créés, tenus à jour, sécurisés et vérifiés régulièrement.

La durée de conservation des fichiers de traces à des fins de preuve doit se conformer a minima à la règlementation.

Par ailleurs, les horloges des systèmes informatiques doivent être synchronisées sur le serveur NTP de référence de la collectivité.

T4-2.F. Conserver une trace des connexions Internet et VPN

Toute connexion ou tentative de connexion à un service web donne lieu à la génération d'une trace détaillée, de niveau application comme de niveau réseau, de cet accès.

Ces données de connexion sont conservées à minima 1 an, conformément à la règlementation.

T4-2.G. Maîtriser les logiciels en exploitation

Les équipements et logiciels doivent être maintenus et mis à jour en cohérence avec la mise à disposition des mises à jour et des correctifs de sécurité par les éditeurs.

Le remplacement des équipements et logiciels dont la fin de période de maintenance approche doit être anticipée et planifiée.

Les utilisateurs ne disposent pas de droit administrateur de leur poste de travail afin qu'ils ne puissent installer librement des logiciels, sauf cas exceptionnel et sous couvert d'une validation par voie hiérarchique.

Par ailleurs, l'installation de logiciel sur les systèmes en exploitation par les profils administrateurs est validée au préalable par la DSI.

T4-2.H. Une veille continue doit être réalisée pour identifier les éventuelles failles de sécurité des systèmes en exploitation

La DSI se tient informée des éventuelles vulnérabilités techniques des systèmes d'information en exploitation afin de prendre les mesures appropriées pour traiter le risque associé.

Des solutions permettant de réduire les risques de vulnérabilité et d'intrusion sont mises en œuvre (actuellement, la solution WithSecure est utilisée pour détecter les potentielles vulnérabilités).

Des audits de vulnérabilité et d'intrusion doivent être réalisés périodiquement afin de réduire au minimum les perturbations subies par les processus métier (vol de données, utilisations frauduleuses, contamination par rebond, etc.).

Un audit de vulnérabilité et d'intrusion a été réalisé en 2022.

T4-3. Sécurité des communications

T4-3.A. Cloisonner les réseaux informatiques selon les besoins de sécurité

L'architecture du réseau est conçue, aux niveaux physique et logique, pour satisfaire les besoins et contraintes, tout en tenant compte de la configuration des locaux de la structure et des contraintes d'exploitation du SI.

Des mesures de cloisonnement logique, voire physique, des flux sont mises en œuvre chaque fois que les besoins de sécurité ou de performance l'exigent.

Des mesures de redondance logique et physique de l'infrastructure réseau sont mises en œuvre chaque fois que les besoins de sécurité ou de performance l'exigent.

T4-3.B. Sécuriser la connexion Internet

Seuls les flux prévus et autorisés doivent pouvoir transiter entre le SI de la structure et les réseaux externes, dont Internet en particulier. Ce contrôle doit être assuré par un dispositif de filtrage de flux réseau.

Un contrôle des flux au niveau applicatif doit être effectué sur les flux en provenance ou à destination d'Internet.

L'accès à Internet depuis le SI n'est possible qu'aux utilisateurs ou services autorisés et préalablement authentifiés.

Les flux en provenance ou à destination d'Internet font l'objet d'une détection et d'un blocage automatique des contenus malveillants.

Tout dispositif directement accessible depuis Internet doit être positionné dans une zone réseau tampon cloisonnée, dite « zone démilitarisée » ou « DMZ », isolée du reste du SI par un dispositif de sécurité adéquat.

Si la connexion Internet est nécessaire à l'exécution de processus critiques, des mesures garantissant le niveau de disponibilité requis doivent être mises en œuvre.

T4-3.C. Identifier ou authentifier chaque équipement connecté au SI

Tout équipement connecté au SI doit être identifié et, dans la mesure du possible ou si le contexte l'exige, être authentifié avant de pouvoir communiquer avec le reste du SI.

T4-3.D. Contrôler les transferts de l'information

Des procédures et des mesures de transfert formelles doivent être mises en place pour protéger les transferts d'information transitant par tous types d'équipements de communication.

Actuellement, la solution de messagerie électronique Microsoft Exchange doit être utilisée par l'ensemble des utilisateurs pour l'échange de courrier électronique, dans le respect de la charte informatique. Des solutions antivirus et antispam sont utilisées pour sécuriser les informations transférées.

Par ailleurs, des solutions sont mis à disposition des utilisateurs pour le partage d'information. Ces outils de communication sont protégés par un dispositif de pare feux.

Lors d'échange d'informations confidentielles auprès d'un tiers, des engagements de confidentialité ou de non-divulgation, doivent être identifiées, vérifiées régulièrement et documentées conformément aux besoins de l'organisation.

Des clauses administratives portant sur les engagements de confidentialité ou de non-divulgation doivent être présentes dans les documents du dossier de consultation des entreprises dans le cadre d'appel d'offre et de procédure adaptée

.

THÉMATIQUE 5 : MAÎTRISER LES ACCÈS AUX INFORMATIONS

T5-1. Contrôle d'accès

T5-1.A. Définir et contrôler les droits d'accès au système d'information

Une politique de contrôle d'accès est établie au sein de la collectivité, documentée et revue sur la base des exigences métier et de sécurité de l'information. (cf. annexe 5)

Les utilisateurs ont uniquement accès aux réseaux et aux services informatiques pour lesquels ils ont spécifiquement reçu une autorisation. Les droits d'accès aux réseaux et aux ressources informatiques sont strictement limités à l'usage requis.

Les personnes pouvant délivrer les droits d'accès au réseau sont les administrateurs systèmes et réseaux de la DSI.

L'attribution et la gestion des droits d'accès des utilisateurs pour les applications métiers spécifiques sont déléguées aux responsables de service métiers.

Toute demande de création ou de modification de droits d'accès au réseau doit être formalisée, validée par voie hiérarchique et archivée par la DSI.

Les accès au réseau de l'intercom de la Vire au Noireau, de la commune de Vire Normandie, et de son CCAS sont réalisés par le dispositif de sécurité de type : user name AD / mot de passe personnel.

La création du compte Active Directory d'un utilisateur est conditionnée par la validation de la charte informatique par ce dernier.

Une procédure de gestion des comptes Active Directory stipule que tout compte inactif depuis plus de 6 mois doit être automatiquement désactivé.

En cas de départ de l'utilisateur, le compte Active Directory de ce dernier est désactivé au plus tôt puis supprimé dans un délai de 6 mois, sauf cas exceptionnel et sous couvert d'une validation par voie hiérarchique.

T5-1.B. Le contrôle d'accès de tiers utilisateurs doit respecter la politique de contrôle d'accès de l'intercom de la Vire au Noireau, de la commune de Vire Normandie, et de son CCAS

La DSI n'assure pas la fourniture de services informatiques et l'hébergement de certaines ressources (serveurs virtuels, sites internet, etc.) pour le compte de tiers utilisateurs (élèves du conservatoire, adhérents de la bibliothèque, cinéma, etc.) sauf demande spécifique.

Le contrôle d'accès de ces tiers utilisateurs doit respecter la politique de contrôle d'accès de la collectivité.

La DSI assurera selon des demandes spécifiques la gestion des habilitations, des droits d'accès et le support à ces tiers utilisateurs.

T5-1.C. Lutter contre les accès non autorisés au système d'information

Lorsque la politique de contrôle d'accès l'exige, l'accès aux systèmes et aux applications doit être contrôlé par une procédure de connexion sécurisée.

Des règles de blocage de la messagerie, d'initialisation de VPN et des règles spécifiques par profil sont appliquées sur les postes de travail des utilisateurs.

L'utilisation des programmes utilitaires permettant de contourner les mesures de sécurité d'un système ou d'une application doit être limitée et étroitement contrôlée.

Les systèmes qui gèrent les mots de passe doivent interagir avec l'Active Directory de la collectivité et doivent garantir la qualité des mots de passe.

L'accès au code source des programmes est restreint au personnel de la DSI ayant la compétence requise.

Un utilisateur authentifié sur un équipement du SI doit soit se déconnecter, soit verrouiller sa session d'utilisation lorsqu'il quitte son poste de travail.

Un système de verrouillage de la session utilisateur est installé et activé sur les postes utilisateurs.

T5-1.D. Adopter les bonnes pratiques en matière d'authentification des utilisateurs

Les comptes utilisateurs sur le système d'information sont individuels et nominatifs.

Si un utilisateur est amené à remplacer un autre utilisateur dans sa fonction, il ne doit en aucun cas utiliser le compte nominatif personnel de l'utilisateur remplacé.

Les tentatives d'usurpation d'identité doivent être découragées sans pour autant impacter fortement les utilisateurs.

Les verrouillages de compte après trois essais de connexion infructueux doivent être tracés et conservés.

Les informations d'authentification (mots de passe d'accès aux SI, clés privées liées aux certificats électroniques, etc.) doivent être considérées comme des données sensibles. Elles doivent être stockées et sauvegardées de manière sécurisée.

Les utilisateurs ne doivent pas stocker leurs mots de passe en clair sur leur poste de travail ou sur un papier à proximité de leur station de travail. Les mots de passe ne doivent pas transiter en clair sur les réseaux.

Les règles de définition des mots de passe doivent présenter une complexité rendant difficile à retrouver à l'aide d'outils automatisés et à deviner par une tierce personne. Les règles de définition des mots de passe doivent être communiquées aux utilisateurs et être appliquées sur l'ensemble des systèmes d'information.

L'utilisation de certificats électroniques doit respecter les règles édictées par le RGS.

Des mesures de protection des comptes administrateurs techniques par défaut doivent être mises en place pour s'assurer de leur non-utilisation. Les dispositifs d'authentification (mots de passe des comptes ou certificats associés) par défaut doivent impérativement être modifiés au moment de l'installation de l'équipement ou de l'application.

T5-2. Cryptographie

T5-2.A. Utiliser des moyens de cryptographie garantissant la sécurité des échanges

Le chiffrement constitue un moyen privilégié de protection des données. Il est d'emploi obligatoire pour le stockage et l'échange de données particulièrement sensibles.

Des mesures cryptographiques doivent être appliquées sur les supports amovibles (clé USB, disque dur externe, etc.) et équipements informatiques portables hébergeant des données sensibles.

Si un échange d'information ne peut pas être réalisé sur un réseau maîtrisé, le flux d'échange doit être protégé en confidentialité, soit par l'utilisation de logiciel sécurisé, soit par le chiffrement du flux (ex. TLS).

Tout chiffrement doit impliquer la mise en œuvre de procédures permettant de restituer en toutes circonstances les données en clair en cas de perte du secret permettant de les déchiffrer. Cela peut se faire par séquestre de clés, procédure de recouvrement, voire maintien d'une copie en clair.

THÉMATIQUE 6 : ACQUÉRIR DES ÉQUIPEMENTS, LOGICIELS ET SERVICES QUI PRÉSERVENT LA SÉCURITÉ DU SI

T6-1. Acquisition, développement et maintenance du SI

T6-1.A. Intégrer les exigences liées à la sécurité du SI en amont

Les exigences de sécurité du SI doivent être mentionnées dans les documents de consultation et dans les documents contractuels (cahier des charges, contrats de service, etc.) avec les prestataires externes.

Tout nouveau système d'Information doit prévoir l'évaluation des besoins de disponibilité, d'intégrité et confidentialité. Pour tout nouveau projet, le responsable de service doit partager en amont avec la DSI les exigences de sécurité du SI.

Il faut s'assurer que les applications envisagées n'ont pas une trop forte adhérence vis-à-vis des environnements sur lesquels elles reposent pour éviter que l'apparition de failles sur cet environnement support n'ait pas d'impact sur la sécurité des applications qui en dépendent.

Tout compostant technique du système d'information doit faire l'objet d'une décision d'homologation de sa sécurité par le RSSI avant sa mise en exploitation dans les conditions d'emploi définies.

T6-1.B. Prendre en compte les exigences liées à la sécurité du SI dans les développements informatiques

Toute initiative de développement informatique doit respecter les exigences liées à la sécurité du SI, concernant la prise en compte de la sécurité dans les projets et les développements informatiques. Pour les développements web, des règles spécifiques de sécurité doivent être appliquées.

Des environnements de test sont disponibles pour toutes les applications selon les exigences de sécurité et recommandations des éditeurs et en adéquation avec les enjeux de la collectivité afin de pouvoir exécuter des tests de fonctionnalité de la sécurité et de valider tout changement informatique avant sa mise en production effective.

Lors de la mise à jour logiciel ou d'implémentation de nouvelles versions, une procédure de tests de conformité et de non-régression doit être exécutée.

Les données de test sont protégées, sauvegardées et contrôlées au même titre que les données de production.

Le service à l'origine du projet de développement informatique doit se référer au DSI et au RSSI afin d'évaluer la nécessité d'engager une démarche d'analyse des enjeux de sécurité.

T6-2. Relation avec les fournisseurs

T6-2.A. Mettre en œuvre et contrôler les prestations de télésurveillance, télémaintenance ou téléassistance

Tout prestataire externe réalisant des interventions à distance doit s'engager par contrat au respect des règles de sécurité de l'intercom de la Vire au Noireau, de la commune de Vire Normandie, et de son CCAS.

Une charte de sécurité des prestataires est formalisée à destination des prestataires externes devant intervenir sur le système d'information de la collectivité.

Aucun accès ne sera octroyé à un prestataire externe, si ce dernier n'a pas signé la charte informatique.

Le prestataire externe et la DSI doivent définir les modalités pratiques permettant la bonne réalisation de l'intervention à distance, au travers une convention de service par exemple (objectifs, périmètre des interventions à distances prévues, obligations réciproques du fournisseur et du responsable du SI, moyens mis en œuvre, procédures, règles de sécurité particulières, etc.).

Les modalités pratiques doivent être portées à la connaissance des personnes concernées.

Les interventions de téléassistance s'effectuent sous le contrôle de la collectivité. Au préalable, elles doivent être explicitement autorisées à la prise de main ou le suivi à distance de son poste de travail.

Dans la mesure du possible, l'accès aux équipements objets de l'intervention à distance doit être réalisé à travers un « bastion » appliquant une politique de sécurité des accès à privilèges.

La collectivité peut interrompre techniquement la téléassistance en cours à tout moment.

Chaque équipement objet d'une télésurveillance ou d'une télémaintenance dispose d'un dispositif d'identification et d'authentification spécifiques.

THÉMATIQUE 7 : LIMITER LA SURVENUE ET LES CONSÉQUENCES D'INCIDENTS DE SÉCURITÉ

T7-1. Gestion des incidents liés à la sécurité de l'information

T7-1.A. Les responsabilités et les procédures de gestion des incidents de sécurité doivent être établies

Les fonctions et responsabilité liées à la SSI sont en partie identifiées dans les fiches de postes.

Le RSSI, voire le DPO si cela concerne des données à caractère personnel, doit réaliser ou faire réaliser un contrôle régulier de la mise en œuvre effective des règles de sécurité prévues par la PSSI. Pour cela, il peut :

- Demander aux responsables en charge d'une partie du SI d'effectuer une auto-évaluation ;
- Procéder à ce contrôle lui-même ;
- Mandater un prestataire externe pour cette tâche.

Le personnel et les sous-traitants utilisant les systèmes et services d'information de la collectivité doivent noter et signaler toute faille de sécurité.

En cas d'incident lié à la sécurité, des procédures doivent être respectées pour assurer une réponse rapide, efficace et pertinente.

T7-1.B. Détecter et gérer les incidents de sécurité

Tous les incidents de sécurité du SI doivent être remontés à la DSI et renseignés dans un outil centralisé.

Le RSSI met en place progressivement le suivi des incidents et des failles de sécurité à des fins d'évaluation de l'efficacité des solutions de protection mises en œuvre et des impacts subis :

La connaissance des causes et des circonstances de survenue des incidents permet à la collectivité d'envisager des mesures en termes de prévention, de protection, de correction et/ou de réaction.

Le plan d'action comprend des améliorations des mesures et dispositifs de sécurité pour diminuer ou faire disparaître les incidents identifiés.

Tout évènement pouvant avoir un impact significatif sur la sécurité du SI (Disponibilité, Intégrité, Confidentialité) est traité par les administrateurs du système d'information en collaboration éventuelle avec le prestataire concerné (Editeur, prestataire d'infogérance…) et le RSSI.

En cas d'incident de sécurité suspecté ou avéré, les administrateurs du système d'information en collaboration avec le RSSI, voire le DPO si cela concerne des données à caractère personnel, doivent identifier les experts techniques auxquels ils peuvent recourir, qu'il s'agisse de personnel interne ou de prestataire externe.

Le RSSI doit établir le processus d'escalade de l'alerte afin de mobiliser les niveaux hiérarchiques adéquats de la structure et si nécessaire d'activer la cellule de crise.

De même, pour les incidents de sécurité concernant des données à caractère personnel, le DPO doit établir et appliquer les procédures de gestion et de communication conformément au RGPD.

T7-1.C. Sauvegarder et tirer enseignement des incidents de sécurité

Le RSSI en collaboration avec les administrateurs du système d'information, voire le DPO si cela concerne des données à caractère personnel, doivent tirer enseignement des incidents de sécurité survenus, et le cas échéant établir des propositions de mesures à mettre en œuvre pour éviter qu'ils se répètent ou pour en limiter les impacts.

Pour chaque incident de sécurité, des procédures d'identification, de collecte, d'acquisition et de protection de l'information pouvant servir de preuve doit être appliquées.

Les éléments de preuve doivent être protégées, sauvegardées et contrôlées au même titre que les données de production.

T7-2. Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

T7-2.A. Sauvegarder les données

Un plan de sauvegarde du SI définissant les besoins opérationnels métiers et d'infrastructure de sauvegarde et de restauration au minimum est établi (cf. annexe xx).

Les serveurs du SI doivent faire l'objet de procédures de sauvegarde spécifiques répondant aux exigences de continuité de fonctionnement de ces composants centraux.

Le plan de sauvegarde du SI est testé régulièrement par la DSI.

Un contrôle de la qualité des supports de sauvegarde et du résultat des opérations de restauration est réalisé systématiquement.

Le plan de sauvegarde doit être mis à jour pour toute mise en production d'un nouveau système, d'une nouvelle application ou d'espaces de données.

T7-2.B. Gérer la continuité de la sécurité de l'information

Un Plan de Continuité d'Activité (PCA) est établi et fixe les exigences en matière de continuité d'activité de la collectivité dans des situations défavorables, comme lors d'une crise ou d'un sinistre.

L'organisation nécessaire à la mise en application et la maintenance du Plan de Continuité d'Activité est formalisée.

La continuité de la sécurité de l'information fait partie intégrante des systèmes de gestion de la continuité de l'activité.

Un Plan de Continuité Informatique fixe les exigences en matière de sécurité de l'information et de continuité de management de la sécurité de l'information en cohérence avec le Plan de Continuité d'Activité (PCA) de la collectivité. Ce PCI est tenu à jour par la DSI.

Une analyse des risques doit être réalisée régulièrement afin d'aligner les dispositifs de continuité et de reprise des moyens informatiques sur les besoins de sécurité des métiers.

Le Plan de Continuité Informatique est régulièrement testé par la DSI, a minima annuellement.

ANNEXES

ANNEXE 1 : FONCTION SÉCURITÉ

Nom de la fonction	Responsable
Référent SI	Gilles de Closets
RSSI	Jocelyn Helie
Référent incident SSI	Jocelyn Helie
Référent DPO	Maxime Llorente

ANNEXE 2 : DURÉE DE CONSERVATION

Selon les circulaires émanant du Service interministériel des Archives de France régissent les archives des collectivités et établissements publics.

ANNEXE 3 : GLOSSAIRE

Sigle / Acronyme	Signification
AES	Advanced Encryption Standard
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CIL	Correspondant Informatique et Libertés
CNIL	Commission Nationale de l'Informatique et des Libertés
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DPO	Data Protection Officer
GT	Groupe de Travail
IP	Internet Protocol
IPSec	Internet Protocol Security
MAC	Media Access Control
MCO	Maintien en Conditions Opérationnelles
Plan d'action SSI	Plan d'Action Sécurité des Systèmes d'Information
PCA	Plan de Continuité d'Activité
PDCA	Plan Do Check Act
PSSI	Politique de Sécurité des Systèmes d'Information
RSSI	Responsable de la Sécurité des Systèmes d'Information ou Référent Sécurité des Systèmes d'Information
RGPD	Règlement Général sur la Protection des Données
RGS	Référentiel de Sécurité Général

Sigle / Acronyme	Signification
SI	Système d'information
SMSI	Système de Management de la Sécurité de l'Information
SSI	Sécurité des Systèmes d'Information
SSID	Service Set IDentifier
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security
WPA2	Wifi Protected Access 2
WPS	Wifi Protected Setup

ANNEXE 4 : CRITICITÉ DES SALLES INFORMATIQUES

Bâtiment	Localisation	Sécu bâtiment	Sécu. Local	Criticité
Hôtel de Ville	Salle Informatique	Badge	Badge	1
	Salle des services Technique	Clef	Clef	1
	Salle Henry Lesage	Badge	Badge	2
	Armoire de brassage			3

1 *Importante*
2 *Moyenne*
3 *Modérée*

ANNEXE 5 : DOCUMENTS ET RECOMMANDATIONS DE RÉFÉRENCE

Charte informatique utilisateur

Charte informatique prestataire

Charte Informatique administrateur

Référentiel Général de Sécurité (RGS)
https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_Corps_du_texte.pdf

L'hygiène informatique en entreprise (ANSSI)
https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

Recommandations de sécurité relatives aux mots de passe (ANSSI)
https://www.ssi.gouv.fr/administration/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/

La loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004 qui impose, entre autre, la conservation des données pour les Fournisseurs d'Accès Internet.

La loi HADOPI du 12 juin 2009 qui gère la diffusion des créations pour le respect des droits d'auteur.

La loi pour une république numérique du 7 octobre 2016 qui impose la publication des données publiques et d'intérêt général dans les 2 mois (Open Data) ainsi que l'obligation de répondre et traiter les saisines par voie électronique (SVE) dans les deux mois.

La dématérialisation des factures (CPP) et des flux comptables (PESV2)

La dématérialisation totale des marchés publics depuis le 1 octobre 2018

La publication obligatoire sur le géoportail de l'urbanisme des règlements d'urbanismes (PLU) depuis le 1er janvier 2020.

L'échange dématérialisé des actes d'état civil.

La loi Informatique et libertés de 1978, modifiée en 2004, et le RGPD applicable depuis le 25 mai 2018 sur la protection des données personnelles.

ANNEXE 6 : POLITIQUE DES MOTS DE PASSE

GESTION DES MOTS DE PASSE DES UTILISATEURS

Lorsque l'authentification des utilisateurs est réalisée sur la base d'un mot de passe, la collectivité applique la démarche suivante :

1. Les procédures internes informent chaque utilisateur qu'il est responsable de la gestion et de l'utilisation des mots de passe qui lui sont attribués : il ne doit pas les divulguer ;
2. Lorsque les utilisateurs sont chargés de maintenir eux -mêmes leurs propres mots de passe, un mot de passe temporaire et sûr doit leur être attribué ; ils devront le changer immédiatement
3. Lorsqu'un utilisateur a oublié son mot de passe, un mot de passe temporaire doit lui être généré après identification certaine de l'utilisateur ;
4. La transmission de mot de passe temporaire doit être sûre, et ne doit en particulier pas être réalisée via un tiers ou via une messagerie électronique non protégée ;
5. L'utilisateur doit accuser réception de ses mots de passe.

STOCKAGE DES MOTS DE PASSE

La collectivité veille à ce qu'en aucun cas un mot de passe ne soit stocké sur un système informatique sous une forme non protégée.

REVUES DES AUTORISATIONS DES UTILISATEURS

Pour maintenir l'efficacité du contrôle d'accès à ses systèmes d'information, La collectivité passe régulièrement en revue les autorisations accordées aux utilisateurs. Cette revue est menée sur les bases suivantes :

Revue des droits d'accès des utilisateurs tous les 6 mois et après chaque évolution significative d'un système d'information ;

Revue des droits des utilisateurs privilégiés (« administrateurs ») tous les 3 mois ;

Revue périodique des utilisateurs ayant accès aux fonctions privilégiées.

RESPONSABILITÉS DES UTILISATEURS

Il s'agit d'obtenir la coopération des utilisateurs pour maintenir l'efficacité du contrôle d'accès.

La coopération des utilisateurs est indispensable au maintien dans le temps d'un certain niveau de sécurité. Afin de l'obtenir, les utilisateurs doivent être conscients de leurs responsabilités personnelles en matière de contrôle d'accès, et notamment sur l'utilisation de leurs authentifiant et équipements de sécurité

UTILISATION DES AUTHENTIFIANTS

L'authentifiant d'un utilisateur est l'élément permettant de lui attribuer des droits d'accès, mais aussi de le rendre responsable des actions réalisées sous son identité. Chaque utilisateur doit donc être informé des mesures à prendre concernant l'utilisation de ses authentifiant (mots de passe, carte à puce, certificat…) :

Un authentifiant est confidentiel, l'utilisateur ne doit donc pas le communiquer à un tiers, ni s'authentifier pour laisser un tiers utiliser ses droits ;

Un authentifiant est personnel, l'utilisateur ne doit donc pas le prêter à un tiers ou le partager avec lui, ni s'authentifier pour laisser un tiers utiliser ses droits.

PROTECTION DE LA CONFIDENTIALITÉ DES MOTS DE PASSE

Les mots de passe sont des authentifiants reposant exclusivement sur le secret. La collectivité doit donc informer les utilisateurs des règles nécessaires au maintien de ce secret :

- Ne pas écrire ses mots de passe sur un papier ou si c'est absolument indispensable, conserver celui-ci dans un endroit sûr ;
- Changer le mot de passe s'il y a la moindre possibilité que celui -ci soit connu d'un tiers ;
- Ne pas construire ses mots de passe sur la base d'informations que l'on peut facilement deviner si l'on connaît l'utilisateur (nom, prénom, numéro de téléphone, date de naissance…) ;
- Changer les mots de passe temporaires dès la première connexion ;
- Changer les mots de passe régulièrement, et ne pas réutiliser un ancien mot de passe ; Ne pas stocker ses mots de passe dans un système d'accès automatique.

La collectivité définit des règles concernant la qualité des mots de passe et met en œuvre les moyens techniques permettant de contrôler l'application de ces règles :

- Longueur minimale du mot de passe (10 caractères recommandée pour les utilisateurs, 14 pour les administrateurs) ;
- Faciles à mémoriser (proposer des procédés mnémotechniques tels que les anagrammes) ;
- Pas de répétition consécutive d'un même caractère ou groupe de caractère (ex : abcccef, abcabc00…) ;
- Utiliser à la fois des chiffres et des lettres ;
- Utiliser à la fois des lettres minuscules et majuscules.
- Ne pas utiliser les mots de passe suivants :
    - 123456
    - 123456789
    - Azerty
    - 12345
    - 000000
    - Un mot de passe composé d'un prénom
    - Qwerty
    - 1234561

- Loulou
- Marseille ou Un mot de passe composé d'un nom de ville

PROTECTION DES ÉQUIPEMENTS LAISSÉS SANS SURVEILLANCE

Tout équipement librement accessible (c'est-à-dire sans contrôle d'accès physique) doit être protégé contre les accès non autorisés lorsqu'il est laissé sans surveillance pendant un certain temps.

La collectivité informe donc ses agents et ses prestataires des consignes de sécurité à respecter :

- Fermer sa session ou verrouiller le poste (par exemple, à l'aide d'un économiseur d'écran à mot de passe) lorsqu'on doit s'en écarter ;
- Fermer sa session sur les ordinateurs centraux lorsqu'on a fini, et ne pas simplement éteindre son terminal ou son PC ;
- Empêcher l'accès aux PC et aux terminaux lorsqu'ils ne sont pas utilisés, à l'aide d'un verrouillage ou d'un mot de passe.

PSSI

Direction des systèmes d'information

Mairie de Vire Normandie

14, rue Chênedollé

14500 Vire Normandie

Tél. **02 31 66 60 30**

informatique@virenormandie.fr

Vire Normandie

11, rue Deslongrais - CS 70076 Vire
14500 Vire Normandie

Charte informatique

jeudi 30 mars 2023

Vire Normandie

Charte informatique

La charte a été élaborée par la Direction des Systèmes d'Information et validée par la Direction Générale des Services et le Maire de Vire Normandie.

L'objectif de ce guide est de présenter un ensemble de recommandations et conseils à respecter pour un usage responsable du Système d'Information de Vire Normandie.

Il présente successivement les recommandations à respecter, les moyens de suivi mis en œuvre par le DSI, et pour finir des questions réponses permettant de mieux appréhender certaines contraintes juridiques.

Ce guide s'appuie sur la charte de bon usage des ressources informatiques de Vire Normandie s'appliquant à tout utilisateur de son Système d'Information.

La négligence ou la mauvaise utilisation des ressources fait courir des risques à l'ensemble de la collectivité. Aussi, le non-respect de la charte peut être considéré comme une faute professionnelle susceptible d'entraîner pour l'utilisateur une suspension conservatoire des outils mis à disposition, des sanctions disciplinaires, sans préjudice d'éventuelles actions pénales ou civiles à son encontre.

Table des matières

I. ACCÈS AU SYSTÈME D'INFORMATION ET AU POSTE DE TRAVAIL

1. Principes

Le Système d'Information de Vire Normandie est constitué de l'ensemble des matériels informatiques, des matériels téléphoniques, des équipements réseaux, des logiciels et des données stockées sur les ressources internes, ainsi que sur les ressources hébergées dans le cloud.

L'accès aux ressources du système d'information de Vire Normandie est **réservé à l'activité professionnelle** des utilisateurs, même temporaire, dans les limites des habilitations qui leurs sont accordées pour remplir leurs missions.

L'accès aux ressources du système d'information est soumis à l'usage d'un authentifiant strictement personnel. L'authentifiant est composé d'un identifiant et d'un mot de passe. Ces derniers ne doivent en aucun cas être écrit sur un quelconque support.

A ce jour le mot de passe est défini sur 10 caractères au minimum et est soumis à des exigences de complexité (4 types de caractères parmi les suivants majuscules, minuscules, chiffres, caractères spéciaux). Il est conseillé de le remplacer tous les ans et ne doit comporter ni le nom, ni le prénom, ni la date de naissance de vous ou d'un proche et ne peut être identique aux quatre mots de passe précédents.

Ne pas modifier la configuration, ni procéder à des ajouts de périphériques. La connexion de clés USB et autres périphériques qui ne nécessitent pas l'installation de logiciel est aujourd'hui déconseillée et doit être limitée aux périphériques et dont le contenu est sûr. Cette tolérance pourra être supprimée si la sécurité de nos systèmes l'exige.

VIRE NORMANDIE se réserve le droit de supprimer l'accès d'un utilisateur au système d'information en cas de non-respect de la législation ou de nécessité impérieuse d'urgence (tentative de piratage par exemple).

2. Dispositions et obligations

<u>L'utilisateur doit</u> :

- Changer régulièrement son mot de passe, selon le rythme préconisé par la DSI
- Veiller à arrêter son poste de travail en fin de journée et fermer à clé son bureau si cette possibilité lui est offerte
- Verrouiller son poste de travail (CTRL-ALT-SUPP puis Verrouiller cet ordinateur ou CTRL-ALT-FIN pour les client léger) en cas d'absence temporaire.
- Assurer la confidentialité de son authentifiant en évitant notamment de noter son mot de passe sur un document, surtout si ce document est accessible facilement ou affiché à côté du poste de travail.

- Refuser d'utiliser l'authentifiant d'un autre utilisateur pour accéder à des fichiers ou données contenus sur un poste de travail.
- Refuser de communiquer son authentifiant à un autre utilisateur y compris à son supérieur hiérarchique. Pour éviter tout problème de fonctionnement du service en cas d'absence d'un utilisateur, il convient de stocker les fichiers et données professionnels sur les espaces de stockage partagés.
- Signaler au service support de la DSI toute violation ou tentative de violation suspectée de son compte réseau et de manière générale tout dysfonctionnement
- Respecter les consignes d'usage, de maintenance et de sécurité définies par le DSI. En particulier, l'utilisateur doit éviter de perturber le fonctionnement du Système d'Information, notamment en essayant de contourner les dispositifs de sécurité et de mise à jour techniques des postes de travail.
- Veiller à mettre en lieu sûr et non visible son ordinateur portable, que ce soit dans les locaux de l'entreprise, des clients ou lors de ses déplacements.

Le responsable hiérarchique de l'utilisateur ne doit pas :

- Exiger de l'utilisateur qu'il lui communique son authentifiant pour pouvoir accéder à son poste de travail en son absence.

II. MESSAGERIE

1. Principes

Chaque utilisateur permanent bénéficie d'une messagerie professionnelle. Il est répertorié dans l'annuaire du Système d'Information et associé, selon son affectation, à des listes de diffusion regroupant d'autres utilisateurs. En cas de départ de l'utilisateur, sa boîte aux lettres est verrouillée et une réponse automatique est mise en place pour indiquer l'adresse mail du service. Le contenu de la boite mail est conservé 6 mois, puis supprimé. Le responsable hiérarchique en est informé. Sur cette période, il peut demander le transfert de ce contenu à l'exception d'un éventuel dossier identifié comme personnel.

Pour des utilisateurs non permanents dans les locaux (consultants, renforts temporaires, stagiaires) ou des prestataires externes, la création d'une l'adresse générique est proposée si elle est nécessaire, cependant si la durée sans réponse est trop longue une adresse nominative sera créée. Le droit d'utilisation de l'adresse sera limité à la durée de la présence de l'utilisateur ou du prestataire dans les effectifs ou les locaux de Vire Normandie.

La taille de la boîte aux lettres est limitée à 2 Go afin de favoriser la disponibilité des serveurs de messagerie et pour tendre à une sobriété d'usage.

La messagerie est un outil de communication professionnelle. L'usage à des fins personnelles est admis à condition de rester modéré et conforme à la présente charte.

Toute suppression d'un message (contenu dans la boite poubelle) qu'il soit volontaire ou involontaire est définitive. La sauvegarde de la messagerie est une action personnelle dont chacun est responsable.

VIRE NORMANDIE pourra prendre connaissance des courriers à caractère professionnel de toute boîte aux lettres. Cet accès devra cependant être justifié par un cas de force majeure et en l'absence durable de l'utilisateur, ou une procédure judiciaire diligentée par les autorités compétentes. Cet accès sera effectué par le DSI en présence d'un représentant de la Direction et se limitera à la stricte exploitation des informations nécessaires. Par respect du secret des correspondances (Loi du 10 juillet 1991), il ne pourra être accédé au contenu d'un e-mail identifié comme étant une correspondance personnelle, sauf s'il s'agit de fournir des éléments d'information dans le cadre d'une procédure judiciaire.

2. Dispositions et obligations

<u>L'utilisateur doit</u> :

- Respecter les règles de déontologie applicables, notamment le principe de neutralité, et s'exprimer dans tout message électronique avec discrétion, probité, modération et correction

- Directement supprimer et avertir le support s'il trouve une pièce jointe de messages électroniques dont le contenu ou l'origine paraissent douteux, et il ne doit surtout pas cliquer sur des liens qui leur paraîtraient suspects.
- Eviter d'engager la responsabilité de Vire Normandie à des fins personnelles au sein de la collectivité, en utilisant la messagerie comme moyen de conclure un contrat ou de réaliser un acte juridique
- Placer les messages qui relèvent de la correspondance personnelle dans un dossier comportant clairement la mention « Privé », « Perso » ou « Personnel »
- Dans le cas d'un départ ou d'une absence prolongée, mettre en place une réponse automatique afin de prévenir ses correspondants de sa future absence et de les rediriger vers un autre point de contact. En cas de circonstances exceptionnelles le DSI se réserve le droit de mettre en place une réponse automatique.
- Veiller à bien cibler les destinataires et à éviter les envois inutiles, notamment avec des pièces jointes volumineuses
- Etre vigilant sur la taille des pièces jointes. La taille de chaque message est limitée à 10 Mo (Message + pièce jointe). Au-delà de cette taille, il faut utiliser les plateformes d'échange interne proposée par la collectivité.

L'utilisateur ne doit pas :

- Envoyer ou transférer des messages à caractère raciste, négationniste, sexiste, homophobe, pédophile, discriminatoire ou susceptible de porter atteinte à la dignité d'autrui ou à l'ordre public
- Transmettre des données ou des informations sans respecter la réglementation en vigueur (droit d'auteur, respect de la vie privée, droit à l'image)
- Générer des envois en masse de messages électroniques à des destinataires externes en utilisant sa messagerie professionnelle, ces envois pouvant être assimilés à une action de « spamming »
- Diffuser ou participer à des messages de type canulars (hoax), chaînes, escroquerie par hameçonnage (phishing), jeux, paris, ...
- Réémettre de façon automatique ou manuelle les messages, ainsi que leurs pièces jointes, à caractère professionnel sur des messageries personnelles.
- Répondre à une demande de transmission d'informations confidentielles : Mot de passe, code confidentiel, ...

III. INTERNET

1. Principes

Tout poste de travail connecté au Système d'Information de Vire Normandie permet d'accéder à Internet à des fins professionnelles. L'usage à des fins personnelles est admis à condition de rester modéré et conforme à la présente charte.

L'accès à Internet peut être filtré par un système de sécurité permettant d'éviter une connexion à des sites à caractère raciste, négationniste, pédophile, pornographique, discriminatoire ou susceptible de porter atteinte à la dignité d'autrui ou à l'ordre public, ainsi que fournissant accès à des services illégaux (vente d'arme, substances illégales, etc.).

En dehors des connexions directes au réseau professionnel, **les accès aux réseaux en mobilité (wifi ou autres) ne sont autorisés que via des logiciels fournis par l'administration**, par exemple par l'emploi d'un VPN (virtual private network) ou un proxy.

La connexion directe à Internet est interdite depuis le réseau administratif de Vire Normandie.

L'utilisateur est informé que les traces de la navigation sont archivées durant un an. En effet, à la demande d'une autorité judiciaire ou administrative, l'administrateur devra fournir les informations de la navigation web.

VIRE NORMANDIE se réserve le droit

- De contrôler le contenu de toute page Web hébergée sur ses serveurs en vue de s'assurer du respect des conditions d'utilisation des services énoncées par la présente Charte
- De supprimer l'accès à Internet d'un utilisateur en cas de non-respect de la législation ou des dispositions de la présente charte.

2. Dispositions et obligations

<u>L'utilisateur doit</u> :

- Signaler au Service support tout dysfonctionnement dans le filtrage des sites Internet lorsqu'ils sont mis en place, ou lorsqu'il accède involontairement à un site à caractère raciste, négationniste, pédophile, discriminatoire ou susceptible de porter atteinte à la dignité d'autrui ou à l'ordre public.
- Eviter d'utiliser l'accès à Internet pour procéder à l'acquisition ou à la vente d'objets ou de services d'ordre personnel.

- Eviter de surcharger le trafic réseau en écoutant ou en visionnant régulièrement et de façon continue via Internet des contenus multimédias type streaming et webradio dans un but non professionnel, pour ne pas pénaliser le bon fonctionnement des applications professionnelles.
- Demander une autorisation hiérarchique préalable avant toute utilisation des services Internet susceptible d'engager VIRE NORMANDIE dans une relation contractuelle (commande, engagement de payer, offre de biens ou de service, etc.)

L'utilisateur ne doit pas :

- Chercher à contourner les dispositifs de filtrage des sites Internet lorsqu'ils sont mis en place afin d'accéder à des sites à caractère raciste, négationniste, pédophile, pornographique, discriminatoire ou susceptible de porter atteinte à la dignité d'autrui ou à l'ordre public
- Télécharger sur Internet des fichiers musicaux, vidéos, photos, des logiciels ou des plug-ins, qu'ils respectent ou non le droit de propriété ou les droits d'auteur à l'exception des services culturels dans le cadre où le droit de propriété et les droits d'auteur son respecté.
- Télécharger des fichiers sans être certains de la source.
- Se connecter à des services Poste à Poste visant à échanger ou télécharger des contenus non professionnels (WeTransfer, DropBox, OneDrive, GoogleDrive, etc.)
- Transférer ou recevoir des fichiers non professionnels par l'intermédiaire de sites de messagerie instantanée (par exemple Hangout, Skype, Teams, ...)
- Fournir des informations confidentielles ou personnelles ou utiliser les sites qui proposent une action sur le poste.
- Utiliser des propos susceptibles de révéler les opinions politiques, religieuses, ou encore de porter atteinte à la vie privée ou à la dignité, ainsi que des messages portant atteinte à l'image ou la réputation de Vire Normandie.
- Exercer une activité commerciale personnelle ou un travail clandestin

IV. LOGICIELS

1. Principes

Les logiciels sont des œuvres intellectuelles couvertes par une législation stricte.

L'installation (ou la désinstallation) de logiciels sur les postes de travail doit toujours être effectué par la DSI et par extension toute personne désignée par elle sous forme écrite

Ceci n'est pas autorisé pour les utilisateurs standard du Système d'Information.

Le DSI pourra désinstaller tout logiciel en cas de perturbations de fonctionnement sur le poste de travail ou du Système d'Information.

Les authentifiants d'accès aux applications sont créés par le DSI à la demande de la DRH suite à un besoin exprimé par un directeur ou un responsable de service. Une demande émanant directement d'un utilisateur ne sera pas prise en compte. Les authentifiants sont supprimés quand l'utilisateur change de poste ou d'activité, et que l'accès à cette application n'est plus justifié.

2. Dispositions et obligations

L'utilisateur doit :

- Contacter le DSI via le support pour toute installation ou désinstallation d'un logiciel
- Contacter le support pour toute demande d'accès à une application fournie par le DSI.
- Respecter le droit de propriété applicable et ne pas effectuer de copie d'un logiciel dont VIRE NORMANDIE dispose d'une licence
- Veiller à la confidentialité de l'authentifiant (identifiant et mot de passe) lui permettant de se connecter à une application

L'utilisateur ne doit pas :

- Chercher à contourner les protections mises en œuvre par le DSI pour limiter l'installation de logiciels sur les postes de travail

Le responsable hiérarchique de l'utilisateur ne doit pas :

- Exiger de l'utilisateur qu'il lui communique son authentifiant d'accès à une application.

V. TÉLÉTRAVAIL

1. Principes

Le télétravail désigne une forme d'organisation du travail dans laquelle un travail, qui aurait pu être exécuté dans les locaux de l'administration, est effectué par un agent hors de ces locaux, de façon régulière et volontaire en utilisant les technologies de l'information et de la communication.

Utiliser sa connexion Internet personnelle pour accéder à distance (hors site) au système d'information introduit des risques supplémentaires pesant sur les activités de Vire Normandie.

Les règles relatives à la sécurité des systèmes d'information et de protection des données pour les agents en fonctions sur le site s'appliquent de la même manière aux agents en télétravail. Ainsi, ceux-ci doivent se conformer aux règles relatives à la sécurité des systèmes d'information et veiller à l'intégrité et à la bonne conservation des données auxquelles ils ont accès dans le cadre professionnel.

VIRE NORMANDIE met à la disposition de l'agent le matériel lui permettant d'exercer son activité professionnelle à son domicile et en assure la maintenance. Les équipements fournis restent la propriété de l'administration.

Le télétravailleur ne peut utiliser un autre matériel que celui fourni par l'administration (sauf exception définie par VIRE NORMANDIE). Il s'engage à réserver l'usage des équipements mis à disposition par l'administration à un usage strictement professionnel et à prendre soin de l'équipement qui lui est confié.

Le moyens mis à dispositions pour se connecter à distance au système d'information de Vire Normandie font donc l'objet de mesures de sécurité particulières. **Il est de la responsabilité de chacun d'agir en fonction de l'environnement utilisé pour se connecter au système d'information de faire preuve de prudence.**

2. Dispositions et obligations

L'utilisateur doit :

- Utiliser les équipements mis à disposition à un usage strictement professionnel
- Obligatoirement pour accéder à distance au réseau de Vire Normandie par un accès VPN ou par un « bureau à distance » (raccourci couramment appelé Connexion serveur).

L'utilisateur ne doit pas :

- Utiliser du matériel personnel, sauf accord de la DSI, pour exercer ses fonctions lorsque VIRE NORMANDIE lui a fourni du matériel spécifique à cet effet
- Chercher à contourner les protections mises en œuvre par le DSI pour accéder au Système d'Information (VPN, Pare-feu local, Filtrage Web, etc.)

VI. BYOD

1. Principes

Le BYOD (Bring Your Own Device) s'entend de la capacité d'un établissement à accepter que ses collaborateurs utilisent du matériel informatique personnel (smartphones, PC, tablettes, etc.) pour travailler.

Conformément au chapitre Télétravail, VIRE NORMANDIE met à la disposition des moyens permettant aux utilisateurs de télétravailler. Cependant si aucune ressource n'est mise à disposition, VIRE NORMANDIE tolère l'utilisation du BYOD ;

Hors télétravail, toute autre utilisation du BYOD par les collaborateurs de Vire Normandie relève de leur libre choix. **Cette utilisation ne peut donner droit à aucune compensation (heures supplémentaires, remboursement de matériel, etc.).**

L'utilisation des services BYOD par l'agent vaut acceptation des règles de la présente charte.

L'utilisation de ces services engage la responsabilité personnelle du collaborateur, qui doit prendre toutes les précautions pour assurer la confidentialité des données auxquelles il accède.

2. Dispositions et obligations

L'utilisateur doit :

- En cas de perte ou de vol de son équipement, prévenir le DSI sans délai pour supprimer l'accès technique à partir de l'équipement.
- **Mettre en place un contrôle d'accès sur son équipement : code PIN, mot de passe, etc.** Ce contrôle d'accès vient s'ajouter au contrôle d'accès technique qui pourrait éventuellement être mis en place par le DSI pour l'accès au service : MDM, certificat, mot de passe, etc.

VII. FICHIERS ET DONNÉES

1. Principes

Toute donnée hébergée sur le Système d'Information doit être une donnée à caractère professionnel, qu'il s'agisse de fichiers ou de bases de données. Comme pour la messagerie, le stockage de fichiers à caractère personnel (par exemple photos personnelles) est toléré sur le disque dur du poste de travail si les volumes occupés restent modestes (de l'ordre de quelques Mo) et s'il ne perturbe pas le bon fonctionnement du poste de travail. Le dossier et les fichiers présent à l'intérieur doivent disposer de la mention « Privé » ou de la mention « Personnel »

Toute donnée hébergée sur le Système d'Information doit respecter le code de la propriété intellectuelle.

Ne pas essayer d'accéder à des données pour lesquelles on ne dispose pas des autorisations.

Les données considérées comme confidentielles par VIRE NORMANDIE sont les suivantes (liste non exhaustive) :

- Informations sur les usagers,
- Informations sur les projets,
- Orientations stratégiques de Vire Normandie,
- Stratégies politique,
- Partenariats couverts par des clauses de confidentialité.
- Données financières sur VIRE NORMANDIE non publiées,
- Informations sur les agents et les élus (répertoires, organigrammes, listes du personnel, etc.),
- Architecture, systèmes, ressources informatiques (données et programmes),
- Le code source développé par les développeurs de Vire Normandie et ses partenaires

2. Protection des données nominatives

La Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dite « Loi Informatique et Libertés », définit les conditions dans lesquelles des traitements de données personnelles peuvent être opérés.

Le Règlement (UE) n° 2016/679 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, fige les nouvelles règles en matière de protection des Données personnelles.

Ces textes instituent, au profit des personnes concernées par les traitements, des droits, que la présente Charte invite à respecter, tant à l'égard des Utilisateurs que des tiers.

Il est également interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celle-ci.

Le DSI n'ayant pas la capacité de contrôler le contenu même des fichiers informatiques gérés par les utilisateurs**, il appartient à chaque utilisateur qui élabore un fichier contenant des données nominatives d'être rigoureux et d'informer le « Délégué à la Protection des données »** quant à l'élaboration de nouveaux traitements, n'ayant pas été déclarés dans le registre des traitements de Vire Normandie.

L'utilisateur doit signaler au DPO, au RSSI, ou à la DSI dans les plus brefs délais **toute tentative malveillante ou violation constatée : sur son poste de travail ; sur ses fichiers ; ou sur ses données**. Ceci permet aux services compétents d'adopter les mesures adaptées (en cas de violation de données à caractère personnel par exemple, le délai de signalement à la CNIL est de 72 heures après la constatation de l'événement.

3. Stockage des données

Les fichiers et données à caractère professionnel doivent être stockés en majorité sur le réseau de Vire Normandie dans les serveurs de fichiers **fournis par le DSI**.

Seuls les fichiers stockés sur ces serveurs de fichiers fournis par le DSI sont sauvegardés. En cas de perte de fichier, l'utilisateur peut en demander la restauration au Support, qui lui fournira la version la plus récente en sa possession.

Les données des sessions locales (sur Desktop ou Laptop) seul le dossier « mes documents » est redirigé sur les serveurs. Il convient que les utilisateurs sauvegardent eux-mêmes les autres données.

L'usage des supports externes est toléré (Clés USB, disques durs externes). **VIRE NORMANDIE se réserve cependant le droit à tout moment et sur le champ, de limiter ou de supprimer cette autorisation** d'usage de supports externes, par exemple s'il est avéré que l'utilisateur ne respecte pas les instructions de son supérieur ou les règles ou conventions reprises dans la présente charte.

4. Accès aux données

Les données stockées sur les dossiers partagés sont considérées comme des informations professionnelles et accessibles par les utilisateurs y ayant accès.

VIRE NORMANDIE pourra prendre connaissance des données stockées sur le poste de travail d'un utilisateur ou sur sa session. Cet accès devra cependant être justifié par un cas de force majeure et en l'absence durable de l'utilisateur ou une procédure judiciaire diligentée par les autorités compétentes. Cet accès sera effectué par la DSI en présence d'un représentant de Vire Normandie et se limitera à la stricte exploitation des informations nécessaires. La DSI pourra récupérer l'ensemble des fichiers hébergés sur l'ordinateur d'un utilisateur si celui-ci quitte VIRE NORMANDIE définitivement.

Les données qui sont clairement identifiables comme relevant du **domaine personnel** ne pourront être accédées qu'avec présence et accord de la personne concernée.

En cas de départ de l'utilisateur du Système d'Information de Vire Normandie, toutes les données seront supprimées au bout d'un an sans accord ou confirmation préalable de celui-ci.

5. Dispositions et obligations

L'utilisateur doit :

- Respecter le droit de protection des données nominatives (cf. paragraphe 4.)
- Informer le DPO de toute création d'un fichier contenant des données nominatives afin du déclarer ou de valider la dispense de déclaration
- Détruire systématiquement tout fichier contenant des données nominatives lorsque le traitement ou la tâche qui a nécessité son élaboration est terminée (statistiques par exemple)
- Créer un dossier « Privé » pour y stocker les fichiers relevant du domaine personnel
- S'engager à ne pas placer dans un dossier « Privé » des données et fichiers à caractère professionnel
- Eviter de stocker sur son poste de travail des données ou fichiers personnels représentant plus de quelques Mo de volume
- Eliminer ou archiver régulièrement les fichiers et données devenus inutiles

L'utilisateur ne doit pas :

- Élaborer des fichiers contenant des données nominatives, en particulier si ces fichiers n'ont pas un rapport direct avec l'activité de l'utilisateur ou s'ils font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale des personnes, ou des informations relatives à la santé ou à la vie sexuelle de celles-ci
- Stocker des données ou fichiers personnels sur les répertoires fournis par le DSI ni dans le dossier « mes documents »
- Stocker des données ou des fichiers qui ne respecteraient pas le code de la propriété intellectuelle et les droits d'auteur
- Stocker des fichiers sensibles, confidentiels ou comportant des données nominatives sur une clé USB, qui peut être perdue ou un autre support de stockage de type mémoire de stockage d'imprimante.

IX. TÉLÉPHONIE

1. Principes

VIRE NORMANDIE met à la disposition des utilisateurs des services des téléphones fixes basés en majorité sur une technologie dite « Téléphonie sur IP ». VIRE NORMANDIE met à la disposition de certains utilisateurs des téléphones mobiles lorsque l'exercice des missions le justifie.

Les numéros de téléphone internes sont enregistrés dans un **annuaire téléphonique** interne, accessible à partir des postes téléphoniques fixes disposant d'un clavier alphabétique.

L'usage d'un téléphone fixe ou mobile est destiné à des fins professionnelles. L'usage à des fins personnelles est admis à condition de rester modéré et conforme à la présente charte.

Certains numéros surtaxés sont interdits en appel.

L'accès exceptionnel à l'international doit être justifié au travers d'une demande écrite.

2. Dispositions et obligations

L'utilisateur doit :

- Eviter d'utiliser son téléphone fixe ou mobile pour un usage personnel
- Respecter les limitations d'appels vers certains numéros surtaxés et ne pas tenter de les contourner
- Signaler dans les meilleurs délais toute perte ou vol d'un téléphone mobile à la DSI.
- Protéger l'accès à son téléphone mobile et aux données qu'il contient par un code d'accès

Le responsable hiérarchique de l'utilisateur ne doit pas :

- Exiger d'un utilisateur qu'il lui communique son numéro de téléphone mobile personnel

X. IMPRIMANTES

1. Principes

VIRE NORMANDIE met à la disposition des utilisateurs des services des imprimantes réseau partagées.

L'usage d'une imprimante est destiné à des fins professionnelles. L'usage à des fins personnelles est admis à condition de rester très modéré (quelques pages par an) et conforme à la présente charte.

Comme les fichiers et les données gérées sur un poste de travail, **les éditions papier peuvent contenir des données nominatives ou confidentielles**, qu'il convient de gérer avec attention.

2. Dispositions et obligations

L'utilisateur doit :

- Récupérer les éditions papier afin d'éviter de laisser sur une imprimante des documents confidentiels ou contenant des données nominatives
- Éviter d'utiliser les imprimantes de Vire Normandie pour des besoins personnels, notamment l'impression en couleur de documents à caractère privé

XI. MOYENS DE CONTRÔLE MIS EN ŒUVRE ET RÈGLES DE DÉONTOLOGIE

1. Principes

Le DSI peut mettre en place un certain nombre d'outils techniques d'enregistrement et d'analyse lui permettant de :

- Détecter des comportements ou des utilisations anormaux (tentatives d'intrusion, utilisation frauduleuse d'un authentifiant) ou contraires aux dispositions de la présente charte et aux dispositions légales (utilisation abusive à titre personnel des ressources, non-respect des droits de propriété par exemple)
- Répondre à ses obligations légales en lui donnant la possibilité le cas échéant de fournir toute information nécessaire dans le cadre d'une procédure judiciaire à la demande des autorités compétentes
- Assurer le fonctionnement du réseau et veiller à sa sécurité

2. Accès au système d'information et poste de travail

Le DSI s'autorise l'utilisation d'outils permettant de :

- Enregistrer les horaires de connexion au système d'information, afin de détecter un problème ou pour recueillir des informations utiles dans le cadre d'une procédure judiciaire
- Vérifier la configuration réseau du poste de travail
- Prendre la main à distance sur la session d'un utilisateur du poste de travail quand ce dernier sollicite l'intervention du Support pour résoudre un problème technique ou un conseil d'utilisation d'un logiciel
- Enregistrer la date, l'heure et la personne concernée pour les demandes d'intervention adressées au Support
- Limiter les possibilités d'installation de périphériques sur les postes de travail sauf pour la DSI
- Authentifier de façon forte les utilisateurs

3. Messagerie

Le DSI s'autorise l'utilisation d'outils permettant de :

- Mesurer la taille occupée par la boîte aux lettres d'un utilisateur et le pourcentage d'utilisation du quota alloué.
- Contrôler l'adresse émettrice de tout message reçu d'Internet afin de vérifier la non-usurpation des adresses utilisées en interne à VIRE NORMANDIE
- Vérifier la présence de virus dans tout message reçu et le cas échéant le traiter
- Limiter la taille des pièces jointes aux messages reçus et envoyés
- Détecter les e-mails indésirables (« spamming ») et les rejeter

4. Internet

Le DSI s'autorise l'utilisation d'outils permettant de :

- Filtrer l'accès à Internet afin d'éviter l'accès à des sites à caractère raciste, négationniste, pédophile, discriminatoire ou susceptible de porter atteinte à la dignité d'autrui ou à l'ordre public
- Accéder à la liste des sites Internet consultés par un utilisateur en cas de problème grave (utilisation d'Internet pour commettre des crimes et délits), auquel cas l'accès à ces informations est conditionné par l'ouverture d'une procédure judiciaire.
- Visualiser le volume de trafic réseau engendré par la consultation Internet des utilisateurs.
- Vérifier le téléchargement de fichiers sur Internet.

5. Logiciels

Le DSI s'autorise l'utilisation d'outils permettant :

- D'interdire les possibilités d'installation de logiciels sur les postes de travail
- De Procéder à un inventaire des logiciels installés sur les postes de travail
- De Contrôler les accès aux applications

6. Règles déontologiques d'utilisation des moyens de contrôle par la DSI

Les utilisateurs de la DSI ayant accès aux moyens de contrôle décrits précédemment sont soumis à une obligation de confidentialité par la charte des administrateurs et s'engagent à respecter les règles déontologiques suivantes :

- Accéder aux informations liées à un utilisateur (historique de navigation, horaires de connexion, volumes et nature des données stockées, historique d'appels téléphoniques) uniquement pour :
    - Régler un problème technique ne pouvant pas être réglé par un autre moyen
    - Vérifier le respect de la réglementation ou des dispositions de la présente charte
    - Fournir toute information nécessaire dans le cadre d'une procédure judiciaire à la demande des autorités compétentes
- Adopter un devoir particulier de réserve, de discrétion et de confidentialité vis-à-vis des informations liées à un utilisateur
- Ne jamais procéder à des copies des informations liées à un utilisateur
- Ne jamais accéder à la prise de connaissance de messages ou de fichiers clairement identifiés comme relevant du domaine personnel
- Ne jamais procéder à une prise de main à distance de la session d'un utilisateur sur le poste de travail sans avoir obtenu l'accord préalable de l'utilisateur concerné

Les agents de la DSI concernés pourront se prévaloir des dispositions de la charte et de ces règles déontologiques vis-à-vis de leur hiérarchie.

Dans le cas d'un non-respect des règles de cette charte de façon répétée le DG et uniquement lui se trouve dans la possibilité de faire une demande à la DSI afin de surveiller l'activité de cet utilisateur sur le système d'information. Dans ce cas l'utilisateur sera prévenu par lettre recommandée avec accusé réception des dates pendant lesquelles il sera surveillé et cela au minimum 2 semaines à l'avance.

XII. ANNEXE : QUESTIONS / RÉPONSES

Pourquoi changer régulièrement son mot de passe ?	Le changement régulier de mot de passe contribue à limiter la validité d'un mot de passe qui serait utilisé de façon frauduleuse. C'est une mesure certes contraignante mais qui vise à protéger l'utilisateur de toute usurpation d'identité.
Tous les mots de passe se valent-ils ?	Non, certains mots de passe, comme les prénoms ou les dates de naissance sont particulièrement faciles à déchiffrer puis à utiliser à l'insu de l'utilisateur. Il est conseillé de gérer un mot de passe de plus 10 caractères, en mélangeant si possible des lettres, des chiffres et des caractères spéciaux *(&, /, -, par exemple)*.
Pourquoi s'embêter avec une mise en veille automatique des postes de travail ?	Il s'agit d'éviter qu'une personne utilise de façon frauduleuse le poste de travail d'un utilisateur en se faisant passer pour lui, lorsque celui-ci s'est absenté momentanément de son bureau ou s'il a oublié d'arrêter son ordinateur avant de partir. De plus en cas d'oubli cela permet de limiter la consommation d'énergie et de réduire l'impact environnemental des outils numériques utilisés.
Pourquoi enregistrer les dates et heures de connexion des utilisateurs au Système d'Information ?	Cela permet de détecter des tentatives de connexion ou des connexions potentiellement frauduleuses effectuées en dehors d'horaires habituels de travail. En outre, cela permettrait de rechercher la source des dysfonctionnements et de répondre aux demandes effectuées par les autorités dans le cadre d'une procédure judiciaire.
Comment distinguer mes e-mails personnels des autres courriers ?	Le mieux est de créer dans votre boîte aux lettres un dossier « Courrier privé » et d'y placer vos e-mails à caractère personnel.
Comment s'assurer que personne ne puisse lire mes e-mails personnels ?	Techniquement parlant, l'accès aux e-mails personnels est possible pour certains utilisateurs du DSI mais ces derniers s'engagent à respecter la règle déontologique qui leur interdit de prendre connaissance des e-mails ou fichiers clairement identifiés comme relevant du domaine personnel
Pourquoi faut-il éviter de participer à des chaînes d'emails, pyramides et autres procédés	Il s'agit d'e-mails envoyés à plusieurs destinataires et qu'on demande de diffuser largement, par exemple pour faire circuler une rumeur, une opinion, une information non vérifiée ou encore une tentative d'escroquerie financière. Ces e-mails qui n'ont aucun caractère professionnel augmentent le trafic de la messagerie sans représenter le moindre intérêt pour VIRE NORMANDIE. En outre, il vaut mieux éviter de s'associer à ces démarches qui peuvent être

analogues ? Qu'est-ce que c'est exactement ?	parfois assimilées à des messages diffamatoires ou malhonnêtes. Enfin, il s'agit pour les spammeurs d'un moyen efficace de collecter des adresses de messagerie qu'ils utilisent ensuite, en usurpant l'identité de l'utilisateur, pour diffuser des messages indésirables
Pourquoi faut-il éviter de réémettre de façon automatique les messages reçus à son adresse de messagerie professionnelle vers une autre adresse de messagerie ?	Il est préférable d'éviter ce transfert automatique car on ne connaît pas toujours le niveau de sécurité de l'hébergeur de la messagerie destinataire. Il n'est donc pas certain que la confidentialité des messages professionnels transférés soit assurée au même niveau que sur les serveurs de messagerie de Vire Normandie.
Je ne comprends pas pourquoi je ne devrais pas écouter la radio sur mon poste de travail, cela ne perturbe pas la qualité de mon travail.	L'écoute via Internet d'une radio génère un flux de données très consommateur de bande passante. Si plusieurs utilisateurs écoutent en même temps un flux radio sur Internet, ils consomment une partie importante du débit disponible, ce qui ralentit tous les autres accès à Internet, les Accès aux données stockées et les temps de réponse des applications.
Pourquoi l'installation d'un logiciel sur les postes de travail est-elle verrouillée ?	Cette mesure est nécessaire car elle permet de s'assurer qu'un logiciel dont VIRE NORMANDIE ne détiendrait pas la licence ne sera pas installé, ce qui engagerait sa responsabilité. Par ailleurs, il s'agit d'éviter de perturber la configuration technique du poste de travail, qui est définie selon un standard précis et identique pour une large majorité des postes. L'installation d'un logiciel pourrait entraîner des dysfonctionnements sur le poste. Dans ce domaine, il n'est pas possible d'avoir la souplesse d'un poste de travail utilisé dans le cadre familial.
Pourquoi n'est-il pas permis de se connecter à des sites d'échange ou de téléchargement de fichiers (musique, logiciels, films...) ?	Pour plusieurs raisons : ces fichiers n'ont pas un caractère professionnel, ils peuvent contenir des virus et enfin ils ne respectent que très rarement les droits de propriété intellectuelle.
Pour des nécessités de service je suis obligé(e) de donner mon authentifiant de connexion à mes	Tout à fait. Il ne faut jamais donner son authentifiant à un collègue. Il faut dans ce cas stocker les fichiers nécessaires au bon fonctionnement du service sur l'espace fournis à cet effet.

collègues de travail, afin qu'ils puissent accéder à mes données en mon absence. Est-ce contraire aux dispositions de la charte ?	
Pourquoi le DSI filtrerait-t-elle les sites Internet accessibles ?	VIRE NORMANDIE ne peut pas autoriser l'accès à des sites à caractère raciste, négationniste, pédophile, discriminatoire ou susceptible de porter atteinte à la dignité d'autrui ou à l'ordre public, d'une part pour d'évidentes raisons morales, d'autre part pour éviter d'engager sa responsabilité. De plus certains sites représentent un danger pour l'intégrité des systèmes d'information de la collectivité
Pourquoi le DSI se permettrait-elle de conserver un historique de la navigation Internet des utilisateurs ?	VIRE NORMANDIE doit être en mesure d'identifier une personne qui aurait utilisé les moyens de l'institution pour effectuer des actions pouvant faire l'objet d'une procédure judiciaire.
Pourquoi le DSI se permettrait-elle d'enregistrer la date, l'heure, la durée des appels entrants ou sortants d'un téléphone fixe ainsi que les numéros appelés et d'en calculer le coût ?	Pour plusieurs raisons : être capable de fournir ces informations en cas de procédure judiciaire, détecter une utilisation injustifiée par l'activité professionnelle et contrôler les factures reçues des opérateurs de téléphonie.
A quoi sert le suivi des impressions ?	Le suivi des impressions permet de disposer d'éléments factuels sur les volumes imprimés pour adapter le profil et l'emplacement des imprimantes. Il permet également de détecter une utilisation injustifiée par l'activité professionnelle et anticiper la consommation des toners d'imprimantes.