

Questionnaire Cyber risques

Description des principales activités / compétences :

La mairie assure la **gestion administrative et financière** de la commune, traite des **données personnelles** (état civil, élections, urbanisme, facturation) via plusieurs **logiciels métiers**, gère les **relations avec les usagers**, la **communication institutionnelle**, et la **préparation des décisions municipales**. Elle dépend de systèmes informatiques pour garantir la **continuité du service public** et la **sécurisation des échanges** avec les services de l'État.

Activités contrôlées par le système d'information :

☒ Gestion du personnel	☒ Comptabilité	☒ État civil
☒ Urbanisme	☒ Marchés publics	☒ Gestion des listes électorales
☒ Gestion des établissements scolaires	☐ Gestion des prestations sociales	☐ Gestion des crèches
☐ Foyers personnes âgées	☐ Autres :	

Disposez-vous d'équipements matériels/industriels contrôlés par le système d'information (machines, vannes, signalisation urbaine, etc.) ☐ OUI ☒ NON

	< 10	11 - 100	> 100
<i>Nombre d'utilisateurs des SI</i>	☒	☐	☐
<i>Nombre de postes mobiles</i>	☒	☐	☐
<i>Nombre de serveurs administrés en interne</i>	☒	☐	☐
<i>Avez-vous un site web de service en ligne ?</i>	☐ OUI ☒ NON		
<i>Si oui, quelle est la part de CA généré par le site web ?</i>	% ou €		

Externalisation du système d'information :

Quelles sont les fonctions informatiques externalisées ?	OUI	NON	Nom du fournisseur de service
Gestion des postes de travail	☒	☐	BSI
Gestion des serveurs	☒	☐	CDG47
Gestion du réseau	☒	☐	BSI
Gestion du site web	☒	☐	Neopse
Gestion d'applications (comptabilité, paye, CRM, ...)	☒	☐	Coloria
Autres, à préciser :	☐	☐	

Appréciation générale du risque

	OUI	NON
Les comptes d'accès au SI sont nominatifs en très grande majorité ou en totalité	☒	☐
Les mots de passe initiaux sur les équipements matériels ou les logiciels sont changés systématiquement, en respectant les bonnes pratiques de complexité ?	☒	☐
Les utilisateurs standards disposent de droits d'administration sur les postes de travail	☒	☐
Les postes de travail sont équipés d'un anti-virus	☒	☐
Les exécutions automatiques (à l'insertion d'un périphérique amovible, ou l'ouverture d'un partage réseau par exemple) sont désactivées	☒	☐
Interdisez-vous la connexion d'équipements personnels sur votre réseau ?	☒	☐
Si vous disposez d'un système d'information industriel ou de matériels contrôlés par le système d'information, sont-ils isolés du système d'information de gestion ?	☐	☒
Avez-vous des accès internet en libre-service (type borne) ?	☒	☐
Si oui, est-il possible depuis cet accès libre-service, d'accéder au reste du SI ?	☐	☒
Avez-vous des réseaux Wifi ?	☒	☐
Si oui : - les équipements personnels ou ceux de visiteurs voire du public, utilisent-ils un réseau Wifi dédié et isolé du reste de votre réseau	☒	☐
- le réseau Wifi professionnel utilise-t-il un chiffrement robuste (WPA2/AES) ?	☒	☐
Vous disposez d'un pare-feu au niveau de l'accès Internet, pour interdire les accès directs à votre SI, en dehors de services en ligne cloisonnés ou d'accès distants bien définis, et pour filtrer les connexions directes sortantes	☐	☐
Votre système d'information est connecté à d'autres SI	☐	☒
Si oui : - Utilisez-vous un canal sécurisé assurant la confidentialité (type VPN) ?	☐	☐
- Filtrez-vous ces accès au strict nécessaire ?	☐	☐
Le stockage des terminaux nomades est chiffré	☐	☐
Les terminaux nomades peuvent se connecter au SI à distance	☐	☐
Si oui : - Ils utilisent un canal d'échange sécurisé (type VPN)	☐	☐
- Ils passent en toute circonstance par votre réseau pour consulter Internet	☐	☐
Vous avez défini une politique de mise à jour des systèmes et logiciels	☒	☐
Que vous ayez une politique ou non, les correctifs les plus critiques sont appliqués rapidement (sous 5j maximum)	☐	☐
Avez-vous des systèmes obsolètes n'étant plus maintenus par leur éditeur ?	☐	☒
Si oui : - Ont-ils été isolés au sein du réseau ?	☐	☐
- Avez-vous planifié leur migration/remplacement ?	☐	☐
Avez-vous mis en œuvre des sauvegardes des systèmes ?	☒	☐
Si oui : - Pour toutes les données (oui) ? Ou seulement les données critiques(non) ?	☐	☒
Selon quelle fréquence ?		
- Les sauvegardes sont-elles extraites hors-ligne, en lieu sûr ?	☒	☐
- Disposez-vous de plusieurs copies des sauvegardes en des lieux séparés ?	☒	☐
- Les sauvegardes sont-elles dans la même salle que les systèmes sauvegardés ?	☐	☒
- Effectuez-vous des tests réguliers de restauration pour vous assurer que les sauvegardes sont utilisables en cas de besoin ?	☒	

Sensibilisation et formation ?

	OUI	NON
Les équipes informatiques suivent des formations sur la sécurité des systèmes d'information (risques et menaces : ransomwares, phishing ou hameçonnage ; authentification et contrôle d'accès, cloisonnement réseau, etc.)	☒	☐
L'utilisateur est informé des règles à respecter et des bons comportements de sécurité dans l'usage de l'informatique et d'Internet (informations sensibles, usage des mots de passe, signalement, verrouillage de session, etc.) Si oui : - dès son arrivée - régulièrement	☒ ☒ ☒	☐ ☐ ☐
Les personnels disposant de terminaux nomades (ordinateur portable, smartphone, tablette) sont sensibilisés aux risques spécifiques du nomadisme (perte, vol, accès distant au SI)	☒	☐
Faites-vous appel à des prestations d'infogérance ? Si oui, existe-t-il un document contractuel décrivant l'ensemble des engagements pour garantir le respect des exigences de sécurité (réversibilité, audits, sauvegarde, maintien à niveau de sécurité, etc.) ?	☒ ☐	☐ ☐

Connaître le système d'information

	OUI	NON
Avez-vous identifié vos données sensibles ? (identification, données de santé, etc.) Si oui, avez-vous inventorié leur localisation (bases de données, partages de fichiers, postes de travail, etc.)	☒ ☒	☐ ☐
Conservez-vous une cartographie des équipements en lien avec ces localisations, ainsi que des équipements de sécurité qui les protègent ?	☐	☒
Disposez-vous d'un inventaire exhaustif des comptes utilisateurs privilégiés dans votre SI qui indique leur usage ? (Il s'agit des comptes d'utilisateurs de niveau administrateur, les comptes d'utilisateurs permettant d'accéder aux répertoires de travail des responsables ou de tous les utilisateurs, et les comptes d'utilisateurs d'un poste non administré par le service informatique ou sans les mesures de sécurité nécessaires.)	☒	☐
Disposez-vous d'un inventaire des comptes techniques de services et d'administration ?	☒	☐
Lorsqu'un utilisateur change de fonction ou de missions, ses droits sont-ils revus pour supprimer ceux qui ne lui sont plus nécessaires ?	☒	☐
Les droits affectés à une personne sont-ils révoqués lors de son départ ?	☒	☐

Authentifier et contrôler les accès

	OUI	NON
Les comptes génériques (donc non nominatifs) sont en nombre restreint et les personnes qui les utilisent sont connues	☒	☐
Les utilisateurs ayant une fonction d'administration du SI disposent d'un compte personnel standard sans privilèges, et d'un compte personnel dédié exclusivement aux opérations d'administration, avec un mot de passe différent	☒	☐
Toutes les actions liées aux comptes sont journalisées (connexion réussies/échouées, compte ajouté, désactivé, etc.)	☒	☐
Avez-vous défini des habilitations pour limiter les accès aux données sensibles ?	☒	☐
Effectuez-vous une revue régulière des droits d'accès sur les emplacements contenant des données sensibles pour détecter des anomalies ?	☐	☒
Le mot de passe de l'utilisateur respecte des règles de complexité (ex : longueur minimale de 8 caractères, typologies variées de caractères, etc.)	☒	☐
Un nombre répété de tentatives infructueuses de connexion verrouille le compte de l'utilisateur	☒	☐
Possédez-vous des dispositifs d'authentification forte pour les accès ou les opérations sensibles ?	☒	☐

Sécuriser les postes

	OUI	NON
La session de l'utilisateur se verrouille automatiquement en cas d'inactivité	☒	☐
L'inventaire des données selon leur niveau de sensibilité est réalisé ?	☒	☐
Les données les plus importantes sur les postes de travail font l'objet de sauvegardes régulières et déconnectées	☒	☐
Les périphériques amovibles sont automatiquement inspectés par l'anti-virus du poste de travail	☒	☐
La gestion des politiques de sécurité des postes de travail est centralisée (Il s'agit de l'application des politiques de mots de passe, les restrictions de certains postes sensibles, les configurations de certaines applications comme les navigateurs web, etc. Il s'agit communément de « GPO » ou équivalent.)	☒	☐
La gestion des politiques de sécurité des serveurs est centralisée	☒	☐
Les postes de travail disposent d'un pare-feu local	☒	☐
Si oui, le pare-feu local autorise l'accès aux protocoles d'administration du poste de travail uniquement aux équipes chargées de l'administration	☒	☐

Sécuriser le réseau

	OUI	NON
Le réseau est découpé en différentes zones logiques (adressage) Si oui : - Un pare-feu limite et filtre les échanges entre les différentes zones, et plus spécifiquement entre postes de travail et serveurs - Les postes de travail des équipes d'administration se trouvent sur un réseau logique isolé de celui des postes de travail standards	☒ ☒ ☒	☐ ☐ ☐
Les flux Internet sont inspectés (analyse antivirus, filtrage par catégories de site, etc.)	☒	☐
Vous disposez d'un équipement capable d'effectuer une analyse antivirale des messages électroniques reçus avant qu'ils ne soient déposés dans les boîtes aux lettres	☒	☐
Vous disposez d'un anti-spam capable de filtrer les messages malveillants reçus	☒	☐
Les salles serveurs et locaux techniques sont des zones d'accès restreint	☒	☐

Superviser, auditer, réagir

	OUI	NON
Disposez-vous de journaux pertinents pour détecter des tentatives d'accès illicites ?	☐	☐
Effectuez-vous des audits réguliers de votre SI pour analyser ses vulnérabilités ? Si oui, les recommandations sont-elles mises en œuvre ?	☒ ☒	☐ ☐
Disposez-vous d'une personne référente de la sécurité du SI ?	☒	☐

Continuité

	OUI	NON
Avez-vous défini et mis en œuvre un plan de reprise d'activité informatique ?	☐	☒
Avez-vous défini et mis en œuvre un plan de continuité d'activité informatique ?	☐	☒
Vos équipements principaux sont-ils redondés ? Si oui, la redondance est-elle effectuée sur plusieurs salles informatiques ?	☒ ☐	☐ ☒
Avez-vous sécurisé l'alimentation en électricité de vos systèmes (onduleur, redondance électrique, groupe électrogène, etc.) ?	☒	☐
La ou les salles informatiques sont équipées des dispositifs de protection spécifiques contre l'incendie ?	☐	☒

Criticité des Systèmes d'Information

Certification ISO 27001 ☐ oui ☐ non

Existe-t-il un accès distant au système d'information de l'entreprise (VPN ou extranet) ? ☒ oui ☐ non

• L'entité autorise-t-elle la connexion au SI d'équipements personnels ? ☐ oui ☒ non

A partir de quelle durée d'interruption de vos Systèmes d'Information vos activités subiront-elles un impact quantifiable ?

Application (ou Activité)	Durée maximale d'une interruption avant impact sur l'activité				
	Immédiat	Max 12 h	Max 24 h	Max 48 h	Au-delà (précisez)
Coloria (paie, comptabilité, état-civil)	☒	☐	☐	☐	
Oxalis (urbanisme)	☐	☐	☐	☒	
	☐	☐	☐	☐	
	☐	☐	☐	☐	