

Questionnaire Cyber risques

Description des principales activités / compétences : Gestion technique et administrative du service assainissement de 4 communes

Activités contrôlées par le système d'information :

<input checked="" type="checkbox"/> Gestion du personnel	<input checked="" type="checkbox"/> Comptabilité	<input type="checkbox"/> État civil
<input type="checkbox"/> Urbanisme	<input checked="" type="checkbox"/> Marchés publics	<input type="checkbox"/> Gestion des listes électorales
<input type="checkbox"/> Gestion des établissements scolaires	<input type="checkbox"/> Gestion des prestations sociales	<input type="checkbox"/> Gestion des crèches
<input type="checkbox"/> Foyers personnes âgées	<input type="checkbox"/> Autres :	

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

☒ OUI

☐ NON

	< 10	11 - 100	> 100
Nombre d'utilisateurs des SI	<input checked="" type="checkbox"/> x	<input type="checkbox"/>	<input type="checkbox"/>
Nombre de postes mobiles	<input checked="" type="checkbox"/> 4	<input type="checkbox"/>	<input type="checkbox"/>
Nombre de serveurs administrés en interne	<input checked="" type="checkbox"/> 1	<input type="checkbox"/>	<input type="checkbox"/>
Avez-vous un site web de service en ligne ?	<input type="checkbox"/> OUI <input checked="" type="checkbox"/> NON		
Si oui, quelle est la part de CA généré par le site web ?	% ou €		

Externalisation du système d'information :

Quelles sont les fonctions informatiques externalisées ?	OUI	NON	Nom du fournisseur de service
Gestion des postes de travail	<input checked="" type="checkbox"/> x	<input type="checkbox"/>	GSMA2I
Gestion des serveurs	<input checked="" type="checkbox"/> X	<input type="checkbox"/>	GSMA2I
Gestion du réseau	<input checked="" type="checkbox"/> X	<input type="checkbox"/>	GSMA2I
Gestion du site web	<input type="checkbox"/>	<input checked="" type="checkbox"/> X	
Gestion d'applications (comptabilité, paye, CRM, ...)	<input checked="" type="checkbox"/> X	<input type="checkbox"/>	JVSmairistem

Autres, à préciser :	<input type="checkbox"/>	<input type="checkbox"/>
----------------------	--------------------------	--------------------------

Appréciation générale du risque

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

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.)	<input type="checkbox"/>	x
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	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	x <input type="checkbox"/> <input type="checkbox"/>
Les personnels disposant de terminaux nomades (ordinateur portable, smartphone, tablette) sont sensibilisés aux risques spécifiques du nomadisme (perte, vol, accès distant au SI)	<input type="checkbox"/>	x
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.) ?	<input type="checkbox"/> <input type="checkbox"/>	x x

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.)	<input type="checkbox"/> <input type="checkbox"/>	x <input type="checkbox"/>
Conservez-vous une cartographie des équipements en lien avec ces localisations, ainsi que des équipements de sécurité qui les protègent ?	<input type="checkbox"/>	x
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.)	x	<input type="checkbox"/>
Disposez-vous d'un inventaire des comptes techniques de services et d'administration ?	x	<input type="checkbox"/>
Lorsqu'un utilisateur change de fonction ou de missions, ses droits sont-ils revus pour supprimer ceux qui ne lui sont plus nécessaires ?	x	<input type="checkbox"/>
Les droits affectés à une personne sont-ils révoqués lors de son départ ?	x	<input type="checkbox"/>

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	<input type="checkbox"/>	x
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	<input type="checkbox"/>	x
Toutes les actions liées aux comptes sont journalisées (connexion réussies/échouées, compte ajouté, désactivé, etc.)	<input type="checkbox"/>	<input type="checkbox"/>
Avez-vous défini des habilitations pour limiter les accès aux données sensibles ?	x	<input type="checkbox"/>
Effectuez-vous une revue régulière des droits d'accès sur les emplacements contenant des données sensibles pour détecter des anomalies ?	<input type="checkbox"/>	x
Le mot de passe de l'utilisateur respecte des règles de complexité (ex : longueur minimale de 8 caractères, typologies variées de caractères, etc.)	x	<input type="checkbox"/>
Un nombre répété de tentatives infructueuses de connexion verrouille le compte de l'utilisateur	<input type="checkbox"/>	x
Possédez-vous des dispositifs d'authentification forte pour les accès ou les opérations sensibles ?	x	<input type="checkbox"/>

Sécuriser les postes

	OUI	NON
La session de l'utilisateur se verrouille automatiquement en cas d'inactivité	<input type="checkbox"/>	x
L'inventaire des données selon leur niveau de sensibilité est réalisé ?	x	<input type="checkbox"/>
Les données les plus importantes sur les postes de travail font l'objet de sauvegardes régulières et déconnectées	x	<input type="checkbox"/>
Les périphériques amovibles sont automatiquement inspectés par l'anti-virus du poste de travail	x	<input type="checkbox"/>
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.)	x	<input type="checkbox"/>
La gestion des politiques de sécurité des serveurs est centralisée	x	<input type="checkbox"/>
Les postes de travail disposent d'un pare-feu local	x	<input type="checkbox"/>
Si oui, le pare-feu local autorise l'accès aux protocoles d'administration du poste de travail uniquement aux équipes chargées de l'administration	x	<input type="checkbox"/>

Sécuriser le réseau

	OUI	NON
Le réseau est découpé en différentes zones logiques (adressage)	X	<input type="checkbox"/>
Si oui : - Un pare-feu limite et filtre les échanges entre les différentes zones, et plus spécifiquement entre postes de travail et serveurs	X	<input type="checkbox"/>
- Les postes de travail des équipes d'administration se trouvent sur un réseau logique isolé de celui des postes de travail standards	X	<input type="checkbox"/>
Les flux Internet sont inspectés (analyse antivirus, filtrage par catégories de site, etc.)	<input type="checkbox"/>	X
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	<input type="checkbox"/>	X
Vous disposez d'un anti-spam capable de filtrer les messages malveillants reçus	<input type="checkbox"/>	X
Les salles serveurs et locaux techniques sont des zones d'accès restreint	<input type="checkbox"/>	X

Superviser, auditer, réagir

	OUI	NON
Disposez-vous de journaux pertinents pour détecter des tentatives d'accès illicites ?	<input type="checkbox"/>	X
Effectuez-vous des audits réguliers de votre SI pour analyser ses vulnérabilités ?	<input type="checkbox"/>	X
Si oui, les recommandations sont-elles mises en œuvre ?	<input type="checkbox"/>	<input type="checkbox"/>
Disposez-vous d'une personne référente de la sécurité du SI ?	X	<input type="checkbox"/>

Continuité

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

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) ? X oui ☐ non

• L'entité autorise-t-elle la connexion au SI d'équipements personnels ? ☐ oui X 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)
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	