

Annexe sur les sécurités

[Note : plusieurs cases peuvent être cochées en réponse à une question]

A. L'architecture informatique, les sécurités et sauvegardes.

1. Description du système informatique. Il est constitué :

- ☐ d'un parc de micro-ordinateurs sans serveur central
- ☐ d'un mini/petit serveur d'entreprise
- ☐ d'un ensemble de serveurs au sein de l'organisme ou externalisés
- ☐ d'un gros ordinateur au sein de l'organisme ou externalisé
- ☐ par l'hébergement chez un fournisseur internet. Nom de l'hébergeur : _____
- ☐ autre architecture informatique : _____

Nom(s) du (des) fournisseur(s) et du (des) modèle(s) : _____

Nom(s) du (des) système(s) d'exploitation : _____

2. Nature du réseau informatique permettant les échanges d'informations en interne.

- ☐ aucun réseau (par ex. des micro-ordinateurs isolés)
- ☐ un réseau local d'entreprise. Nom (par ex. Netware) : _____
- ☐ un serveur interne accessible de l'extérieur via internet
- ☐ un hébergement externe accessible via internet.
- ☐ un extranet mis en œuvre par un Réseau Privé Virtuel (RPV ou VPN en anglais). Nom du dispositif technique ou du prestataire : _____
- ☐ des lignes privatives louées à un opérateur de télécommunication
- ☐ utilisation de technologies sans contact. Nom (WiFi par ex.) : _____
- ☐ utilisation de postes de travail nomades (micro-ordinateurs par ex.)
- ☐ autre type de réseau : _____

Nombre total de postes de travail : _____

Eventuellement, nom(s) du (des) logiciel(s) réseau(x) ou du moniteur de télétraitement : _____

3. En cas d'échanges d'informations avec des partenaires ou organismes extérieurs, préciser le(s) procédé(s). technique(s) utilisé(s) :

- ☐ support magnétique ou analogue (disque, bande, cd-rom, clé USB,..) : _____
Chiffrement : OUI NON
- ☐ messagerie internet. Chiffrement : OUI NON
- ☐ transfert de fichier par internet. Chiffrement : OUI NON
- ☐ transfert via un réseau privatif. Nom éventuel du réseau : _____
Chiffrement : OUI NON
- ☐ autre procédé : _____
Chiffrement : OUI NON

4. Sécurité (protection) physique des locaux et équipements, sauvegarde du système informatique.

- ☐ Décrire brièvement les dispositifs/procédures permettant d'assurer la sécurité physique des locaux et équipements informatiques (badge d'accès, gardiennage etc.) :

- ☐ Mesures assurant la sauvegarde du système informatique

- Type de support utilisé : _____
- Fréquence des sauvegardes : _____
- Chiffrement des sauvegardes : _____ OUI NON
- Lieu de stockage : _____

- ☐ Protection supplémentaire du lieu de stockage des supports de sauvegarde. Préciser :

5. Protection contre les intrusions extérieures utilisant le canal des réseaux informatiques.
Procédé(s) technique(s) utilisé(s) :

- ☐ un routeur. Nom : _____
- ☐ un pare-feu (firewall). Nom : _____
- ☐ un système complet de détection d'intrusion (IDS). Nom : _____
- ☐ autre procédé : _____

6. Mesures destinées à assurer la confidentialité des données lors du développement de l'application informatique.

- ☐ Le développement de l'application s'effectue dans un environnement informatique distinct de celui de la production (par ex. sur des ordinateurs différents, dans des salles machine différentes)
- ☐ Le personnel affecté aux tâches de développement est distinct de celui assurant la gestion /l'exploitation des équipements informatiques de production
- ☐ La mise au point des logiciels s'effectue sur des données fictives et non sur des données réelles
- ☐ Autres mesures destinées à protéger la confidentialité des données de production :

7. Mesures destinées à assurer la confidentialité des données lors des opérations de maintenance des équipements informatiques

- ☐ Les interventions de maintenance des matériels sont enregistrées dans une main-courante
- ☐ Les interventions de maintenance des matériels par un sous-traitant se font en présence d'un informaticien de l'entreprise
- ☐ La télé-maintenance des matériels n'est pas autorisée
- ☐ Les supports de stockage envoyés à l'extérieur à fin de réparation font l'objet d'une procédure de protection particulière. Si oui, préciser laquelle :

- ☐ Les supports de stockage destinés à la destruction font l'objet d'une procédure de protection particulière. Si oui, faire une description :

8. Mesures destinées à assurer la confidentialité des données lors des opérations de maintenance des logiciels informatiques

- ☐ Les interventions de maintenance des logiciels dans l'environnement de production sont enregistrées dans une main-courante
- ☐ Les interventions de maintenance des logiciels de l'environnement de production se font sous le contrôle du chef d'exploitation en respectant une procédure spécifique
- ☐ La télé-maintenance des logiciels de l'environnement de production n'est pas autorisée
- ☐ Une procédure particulière est mise en œuvre dans le cas où une opération de maintenance logicielle nécessiterait un accès aux fichiers de données nominatives. Si oui, la décrire :

B. Le logiciel d'application.

9. Il met en œuvre :

- ☐ une base de données.(ou un logiciel de gestion d'un entrepôt de données).
Nom : _____
- ☐ un (des) progiciel(s). Nom(s) : _____
- ☐ un infocentre. Nom : _____
- ☐ un logiciel d'analyse de données permettant des statistiques/profilages/segmentations
Nom : _____
- ☐ Autre : _____

10. Finalités mettant des procédés techniques particuliers

- ☐ carte à puce
- ☐ biométrie (voir également la rubrique 13)
- ☐ RFID (reconnaissance à distance par radio-fréquence)
- ☐ vidéo-surveillance
- ☐ autre : _____

11. Authentification/identification des personnes habilitées à accéder à l'application. Le contrôle d'accès se fait-il par :

- ☐ un mot de passe.
Préciser :
 - s'il a une structure obligatoire (par ex. alphanumérique, présence d'un caractère spécial,...)
: _____
 - sa longueur minimale : _____
 - sa durée de vie avant changement obligatoire : _____
 - s'il y a interdiction de réutiliser les n précédents mots de passe : _____
 - s'il y a interdiction d'utiliser certains mots de passe (par ex. date de naissance, prénom,...) :

- s'il y a blocage automatique du terminal d'accès au bout d'un certain nombre d'essais infructueux (si oui, préciser ce nombre) : _____
- ☐ des profils d'habilitation définissant pour chaque utilisateur les fonctions autorisées ou les catégories d'informations accessibles
- ☐ une carte à puce
- ☐ un dispositif biométrique (voir également la rubrique 13)
- ☐ autre : _____
- ☐ Lors d'une connexion, des informations concernant la précédente connexion s'affichent sur le terminal (par ex. date, heure et identifiant de l'utilisateur)
- ☐ Les accès à l'application font l'objet d'une journalisation (données de connexion). Si oui, préciser les informations journalisées :
 - ☐ date/heure de connexion
 - ☐ identifiant du poste de travail
 - ☐ identifiant de l'utilisateur
 - ☐ date/heure de déconnexion
 - ☐ autres informations journalisées : _____
- ☐ Les accès aux fichiers de données nominatives de l'application font l'objet d'une journalisation spécifique. Si oui, préciser les informations journalisées :
 - ☐ date/heure d'accès
 - ☐ identifiant du poste de travail
 - ☐ identifiant de l'utilisateur
 - ☐ la référence des données du fichier auxquelles il a été accédé
 - ☐ autres informations journalisées : _____
 - ☐ type d'accès journalisés, pour : CONSULTATION CREATION MISE A JOUR

12. Confidentialité/authentification. L'application met en œuvre des procédés :

- ☐ d'anonymisation des données. Nom : _____
- ☐ de chiffrement des données.
Nom (par ex. 3DES) : _____ Longueur de la clé : _____
- ☐ de chiffrement du transport des données.
Nom (par ex. SSL) : _____ Longueur de la clé : _____
- ☐ d'authentification émetteur/destinataire (signature électronique, certificat,...).
Procédé et nom commercial : _____
- ☐ Expliquer brièvement les raisons du recours à ces procédés : _____

13. En cas d'usage d'un procédé biométrique. Préciser :

- sa nature (par ex. contour de la main, empreinte digitale, iris,...) : _____
- le nom commercial du dispositif ou du fournisseur : _____
- si l'empreinte biométrique est mémorisée sur un support individuel : OUI NON
- si les empreintes biométriques sont mémorisées dans un fichier : OUI NON

NB : les traitements de données biométriques sont soumis à autorisation préalable de la CNIL.

C. Sensibilisation des utilisateurs à la politique de sécurité.

- ❑ La politique de sécurité/confidentialité est formalisée dans des documents
- ❑ Action de sensibilisation des utilisateurs à la politique de sécurité.

Si oui, sous quelle forme (formation, affiche,...) : _____