TwinnTax - Mesures organisationnelles et techniques

	MESURES
1. Sensibilisation des utilisateurs	Séance d'information et de sensibilisation des employés
	Charte informatique
	Clause de confidentialité dans les contrats des employés
2. Authentification des utilisateurs	Identifiant unique par utilisateur et interdiction des comptes partagés
	Authentification des utilisateurs basée sur des mots de passe
	Limitation du nombre de tentatives d'accès à un compte
	Stockage des mots de passe de façon sécurisée (hachage cryptographique)
3. Gestion des habilitations	Définition de profils d'habilitation dans les systèmes (accès à certains dossiers)
	Validation de toute demande d'habilitation
	Suppression des permissions d'accès (y compris à la fin d'un contrat)
	Réalisation d'une revue régulière (annuelle) des habilitations
4. Traçage des opérations et gestions des incidents	Système de journalisation (enregistrement des fichiers jours ou logs) des activités des utilisateurs, des interventions techniques et des anomalies
	Conservation de la journalisation pendant six mois à un an
5. Sécurisation des postes de travail	Mécanisme de verrouillage automatique de session en cas de non-utilisation du poste pendant un temps donné
	Pare-feu sur le poste de travail
	Antivirus et logiciels régulièrement mis à jour
	Logiciels configurés pour que les mises à jour de sécurité se fassent automatiquement
	Stockage des données des utilisateurs sur un espace de stockage régulièrement sauvegardé plutôt que sur les postes de travail
	Effacement de façon sécurisée des données présentes sur un poste préalablement à sa réaffectation à une autre personne
	Interdiction d'exécution d'applications téléchargées ne provenant pas de sources sures
6. Sécurisation de l'informatique mobile	Sensibilisation aux risques (vol, connexion aux réseaux publics non maitrisés)
	Mot de passe sur les téléphones mobiles
	Sauvegardes ou synchronisations régulières

7. Protection du réseau informatique interne	Limitation des accès Internet en bloquant les services non nécessaires (VoIP, pair à pair)
	Gestion et sécurisation des réseaux WiFi (chiffrement WPA3 ou WAP2)
	VPN pour l'accès à distance pour les appareils nomades
8. Sécurisation des serveurs	Limitation de l'accès aux outils et interfaces d'administration aux seules personnes habilitées
	Installation des mises à jour critiques sans délai
	Utilisation des logiciels de détection et de suppression de programmes malveillants régulièrement mis à jour
	Sauvegardes
	Mise en œuvre d'un protocole TLS (en remplacement de SSL)
9. Sécurisation des sites internet	Mise en œuvre d'un protocole TLS (en remplacement de SSL) et les rendre obligatoires pour toutes les pages d'authentification
	Limitation des ports de communication strictement nécessaires au bon fonctionnement des applications installées
	Limitation de l'accès aux outils et interfaces d'administration aux seules personnes habilitées
10. Sauvegardes et continuité d'activité	Sauvegardes fréquentes des données
	Stockage au moins d'une sauvegarde sur un site extérieur
	Isolation au moins d'une sauvegarde hors ligne
	Protection des données sauvegardées au même niveau de sécurité que celles stockées sur les serveurs d'exploitation
11. Archivage	Définition d'un processus de gestion des archives
12. Développements informatiques	Mise en place d'une défense en profondeur des systèmes (combinaison de plusieurs mesures de sécurité)
	Tests complets avant la mise à disposition ou la mise à jour d'un produit
	Audit ou une revue de code avant tout passage en production d'une mise à jour pour éviter l'apparition de sources de violation de données personnelles
13. Gestion de la sous-traitance	Faire appel uniquement à des sous-traitants présentant des garanties suffisantes et prévoir un contrat
	Moyens permettant de vérifier l'effectivité des garanties offertes par le sous-traitant en matière de protection des données (ex. : audits de sécurité, visite des installations)
14. Sécurisation des échanges vers d'autres organismes	Lors d'un envoi via un réseau : - chiffrer les pièces sensibles à transmettre, - utiliser un protocole garantissant la confidentialité et l'authentification du serveur destinataire pour les transferts de fichiers, par exemple SFTP ou HTTPS, - assurer la confidentialité des secrets (ex. :

	clé de chiffrement, mot de passe) en les transmettant via un canal distinct des données protégées
15. Protection des locaux	Installation des alarmes anti-intrusion et vérifier leur bon fonctionnement périodiquement
	Mise en place des détecteurs de fumée ainsi que des moyens de lutte contre les incendies et les inspecter annuellement
	Protection des clés permettant l'accès aux locaux ainsi que les codes d'alarme