

**MESURES TECHNIQUES ET ORGANISATIONNELLES****Mai 2018**

**Le présent document est délivré à titre informatif.**

**Compte tenu des évolutions techniques et législatives, les informations contenues dans le présent document sont susceptibles de modifications à tout moment.**

**Sarbacane Software****3 Avenue Antoine Pinay****P.A. des Quatre Vents****59510 Hem - FRANCE****Tél : +33 (0) 328 328 000**

SAS au capital de 167.817 €

RCS Lille Métropole 509.568.598

**Mesures techniques et organisationnelles****Mai 2018**

## **1. Contrôle d'accès physique aux locaux et aux installations**

**Mesures appropriées pour contrôler et empêcher l'accès physique des personnes non autorisées aux Locaux et installations.**

- **Système d'alarme**
- **Personnel de sécurité, concierges**
- **Installations de vidéo surveillance**
- **Système automatique de contrôle d'accès / Distinction de zones selon les risques**
- **Lecteur d'identification, badges, cartes à puce, cartes magnétiques, système de verrouillage à transpondeur**
- **Serrures de sécurité**
- **Vérification d'identité**
- **Enregistrement / Accompagnement des visiteurs**

**En fonction de l'emplacement et de l'installation, une combinaison de la liste ci-dessus est présente. Il est nécessaire de prendre en compte que toutes les fonctionnalités ne sont pas présentes et nécessaires sur tous les locaux ou installations.**

## **2. Contrôle d'accès aux données, aux systèmes**

**Mesures techniques (ID / password security) et organisationnelles (données de base de l'utilisateur) approprié pour l'identification et l'authentification des utilisateurs.**

- **Attribution des droits des utilisateurs répondant au principe de moindre privilège, avec révision ou suppression en cas de changements d'affectation ou de départ.**
- **Création de profils utilisateur :**
  - **Droits d'accès différenciés (profils, rôles, transactions et objets)**
  - **Administration des droits par les administrateurs système**
- **Procédures de mot de passe (y compris les caractères spéciaux, la longueur minimale, le changement de mot de passe etc.)**
- **Authentification avec nom d'utilisateur / mot de passe**
- **Utilisation de gestionnaire de mots de passe sécurisés**
- **Verrouillage automatique des sessions en cas de non utilisation**
- **Chiffrement des disques d'ordinateurs nomades**
- **Chiffrement des échanges**
- **Utilisation de la technologie VPN**
- **Utilisation de systèmes de détection d'intrusion**
- **Utilisation d'un logiciel anti-virus / firewalls / limitation des services et flux non nécessaires**
- **Mises à jour automatique des systèmes d'exploitation et applications**
- **Cloisonnement des réseaux / réseau d'administration**
- **Actes d'administration tracés (bash\_history), enregistrement des logs systèmes et applicatif en particulier en cas d'accès, d'entrée, de modification ou suppression de données**
- **Utilisation de déchiqueteurs de documents**

**Selon le rôle, le type de logiciel, le niveau de risque, des exigences clients spécifiques et la nécessité, une combinaison des mesures est en place.**

### 3. Contrôle de disponibilité

Mesures prévoyant la disponibilité et la protection des données contre la destruction ou la perte accidentelle.

- Procédures de sauvegarde ; Stockage de sauvegarde
- Stockage à distance
- Plan de continuité d'activité (PCA)
- Systèmes d'alarme incendie et fumée
- Systèmes anti-virus / pare-feu
- Détection automatique des incendies (Certification APSAD R7)
- Extinction automatique à gaz (Certification APSAD R13)
- Détection des intrusions (Certification APSAD R81)
- Présence d'extincteurs portatifs et mobiles (Certification APSAD R4)
- Alimentation électrique de secours en cas de défaillance
- Lien Internet de secours en cas de défaillance
- Plan de maintenance préventive et tests basés sur les préconisations des constructeurs

En fonction de l'emplacement et de l'installation, une combinaison de la liste ci-dessus est présente. Il est nécessaire de prendre en compte que toutes les fonctionnalités ne sont pas présentes et nécessaires sur tous les locaux ou installations.

### 4. Contrôle de ségrégation

Mesures pour prévoir un traitement distinct (stockage, modification, suppression, transmission) de données à des fins différentes.

- Séparation du système de test et de production
- Séparation du système de développement et de production
- Séparation logique des données clients

### 5. Mesures internes et Sensibilisation

Mesures prévoyant l'information et la sensibilisation du personnel de la société concernant la sécurité des données. Mesures internes générales.

- Évaluation périodique des mesures en place
- Clause de confidentialité au contrat de travail

- **Charte Utilisation des Moyens Informatiques et de Communication (UMIC), annexée au Règlement Intérieur**
- **Action de sensibilisation auprès des salariés sur les aspects de protection et sécurité des données**
- **Société adhérente auprès de l'Association Française des Correspondants à la protection des Données (AFCDP) à caractère Personnel**
- **Société adhérente auprès du Syndicat National de la Communication Directe (SNCD)**