Politique sécurité

LA SÉCURITÉ : UN ENGAGEMENT DE DIMO SOFTWARE

Les données informatiques représentent un **actif particulièrement précieux et sensible** pour toutes les entreprises.

Aussi, le groupe DIMO Software s'engage afin d'assurer la protection et la sécurisation des données informatiques de production confiées par ses clients (bases de données, fichiers de données...).

La démarche du groupe DIMO Software en matière de management de la sécurité de l'information permet ainsi de prévenir les **pertes, vols, altérations de données informatiques de production** et **d'empêcher toute intrusion dans les systèmes informatiques** concernés.

Dans le respect du principe d'amélioration continue (roue de Deming), DIMO Software consolide donc son système de management de la sécurité de l'information afin d'identifier les menaces et mettre en place les contrôles appropriés **pour préserver la confidentialité, l'intégrité et la disponibilité des données informatiques de ses clients.**

1. La sécurité chez dimo software

DIMO Software possède une architecture permettant une **sécurisation des données** et une **haute disponibilité** des machines virtuelles.

Le matériel actif autour de notre data center est doublé pour la **continuité de service** (switchs, alimentations, pare-feu en haute disponibilité, climatisation de la salle serveurs).

La gestion des contrôles d'accès

La gestion des contrôles d'accès aux ressources du SI

Grâce à notre Active Directory (serveur d'authentification et de gestion des comptes utilisateurs), une gestion fine de la sécurité est appliquée aux différents services du système d'information. De plus, un accès extérieur sécurisé permet aux collaborateurs de se **connecter à distance** aux données du système d'information.

Le **réseau de données** DIMO Software est contrôlé et cloisonné (supervision, antivirus, antispam) pour éviter toute faille de sécurité et interaction. De plus, pour le confort et la sécurité de nos visiteurs, DIMO Software propose un **Wi-Fi visiteurs**, séparé de l'ensemble des réseaux du système d'information.

Politique sécurité

Le contrôle d'accès physique

L'accès au bâtiment et aux différents espaces sensibles est contrôlé par un système biométrique et un contrôle vidéo des zones sensibles.

Un **service d'accueil** est présent tout au long de la journée pour accueillir le public et diriger les personnes dans les bons services.

Une **alarme anti-intrusion** avec une surveillance 24h/24, 7j/7 permet l'intervention rapide d'une équipe d'agents de sécurité en cas d'effraction.

La supervision

Pour s'assurer du bon fonctionnement quotidien du système d'information, **toute l'activité est enregistrée** (accès, modifications, erreurs).

En parallèle, les ressources dédiées au bon fonctionnement du système d'information sont **supervisées en temps réel** (bande passante des réseaux, puissance CPU, taux de disponibilité, capacité du data center).

Le PRA (Plan de Reprise d'Activité)

Le data center est répliqué quotidiennement sur le site distant d'un hébergeur ; ceci permet une **reprise d'activité sur les applications stratégiques** en cas de panne ou de perte totale du bâtiment.

Des tests annuels sont effectués pour vérifier le bon fonctionnement des réplications. Des **procédures de déclenchement du PRA** (documentation, décideurs, périmètre) sont élaborées et mises à disposition des techniciens DIMO Software et de l'hébergeur.

La sauvegarde

Le système d'information est sauvegardé quotidiennement, suivant la **procédure de gestion des sauvegardes** des machines virtuelles et des serveurs physiques. La restauration peut se faire au niveau des fichiers, des disques durs ou des machines virtuelles intégrales.

Le délai de rétention des données est fixé de base à une semaine pour les serveurs non sensibles et peut aller jusqu'à plusieurs mois.

La sécurisation électrique

DIMO Software assure chaque année la bonne **conformité électrique** grâce à un audit annuel effectué par une société externe habilitée.

Les circuits électriques des switchs (extrémité et coeur de réseau) **sont ondulés,** permettant la continuité d'activité et plus particulièrement l'alimentation du système de téléphonie.

La sécurisation électrique

DIMO Software assure chaque année la bonne **conformité électrique** grâce à un audit annuel effectué par une société externe habilitée.

Le système incendie

Le data center est sous **surveillance incendie** 24h/24 et 7j/7, reliée à la centrale de surveillance de SECURITAS. Une procédure d'évacuation des locaux (exercice incendie) est réalisée chaque année par le CHSCT. En parallèle est réalisée une vérification annuelle des installations incendie (ventilation, extincteurs).

La maintenance & support (matériels)

Tout le matériel actif de DIMO Software est sous **contrat de maintenance**. Selon l'importance du matériel, les temps de résolution d'une panne peuvent aller de 4 heures à 1 jour.

DIMO Software assure le **suivi des pannes et des demandes d'amélioration** au travers d'un outil de demande d'intervention interne et externe.

2. La sécurité des données informatiques

L'accès aux données des clients hébergés

Les accès sont limités et sont tracés.

Les données des clients sont cloisonnées.

Notre partenaire hébergeur est certifié ISO 27001.

Les données des clients non hébergés

Les données sont transférées via des outils sécurisés et sont supprimées après traitement.

3. Le management de la sécurité

Le management des RH

Tout au long de sa collaboration dans l'entreprise, le salarié DIMO Software est suivi par les équipes de management et des Ressources Humaines. Ce suivi se traduit par la rédaction détaillée de son contrat de travail, incluant des clauses de confidentialité, des réunions d'information sur le règlement intérieur, des entretiens annuels sur les compétences et les objectifs à réaliser.

Le comité de direction (COMEX)

Chaque mois, le Comité exécutif de DIMO Software se réunit pour valider les différents travaux à réaliser pour la maintenance et l'évolution du système d'information.