Plan d'Assurance Sécurité Annexe « Sûreté »

1. Introduction

Cette annexe est liée et indissociable au Plan d'Assurance Sécurité.

2. Description du système

La Société propose des solutions de Détection d'intrusion, de Contrôle d'accès et Vidéo protection.

Ces systèmes traitant de la sécurité des biens et personnes nécessitent également la mise en œuvre de mesures de sécurité.

Les solutions de Détection d'intrusion permettent de connaitre les accès non légitimes aux zones protégées par le système.

Les solutions de Contrôle d'accès permettent de gérer les accès aux zones protégées par le système.

Les solutions de Vidéo protection permettent de visualiser et potentiellement enregistrer les accès aux zones protégées par le système.

Les solutions proposées étant liés aux systèmes et réseaux de son infrastructure, l'annexe « PAS – Annexe Infogérance » est également applicable.

3. Mesures de sécurité

3.1. Transfert

La Société se porte garant de l'intégrité et de la confidentialité des données qui lui sont confiées pendant la phase de transfert du système d'information. Sauf demande expresse auprès de la Société, le Client réalisera les sauvegardes de ses informations et gèrera ces sauvegardes de manière à permettre une reprise en cas d'incident lors de la bascule du système.

3.2. Exploitation

Ce paragraphe présente les mesures mises en place pour assurer la protection du système gérée par la Société.

Dans tous les cas, nous préconisons un contrat de service adapté aux besoins du client, afin de maintenir en conditions opérationnelles les installations déployées.

- ***Détection d'intrusion***

Nos solutions s'appuient sur des matériels répondant à la certification NF&A2P.

Une analyse de risque est réalisée pour chaque étude technique conformément à nos certificats APSAD R81 et NF Service.

Les mots de passe par défaut des matériels mis en place sont systématiquement modifiés.

➢ ***Contrôle d'accès***

Les mots de passe par défaut des matériels mis en place sont systématiquement modifiés.

Nous préconisons :

- L'utilisation d'accès nominatif à l'application de gestion.
- La sauvegarde de la base de données de l'application de gestion.
- Un test de restauration de cette sauvegarde de façon périodique.
- Une limitation aux seules personnes habilitées pour l'accès physique au serveur.
- Une solution de service afin de maintenir en conditions opérationnelles les installations déployées.

La solution de contrôle d'accès ne peut être une solution de gestion du temps.

➢ ***Vidéo protection***

Une analyse de risque est réalisée pour chaque étude technique conformément à nos certificats APSAD R82 et NF Service. L'intégrité du système de vidéo protection est formalisée en fonction de cette analyse de risque.

Nous respectons la durée de conservation légale des enregistrements vidéo (maximum 30 jours sauf cas particuliers).

Les mots de passe par défaut des matériels mis en place sont systématiquement modifiés.

En conformité avec l'arrêté du 3 aout 2007 portant définition des normes techniques des systèmes de vidéosurveillance, un journal électronique comportant l'identité de l'opérateur, les n° des flux exportés et les date et heure de l'exportation est généré automatiquement à chaque exportation.

Nous préconisons :

- L'utilisation d'accès nominatif à l'application de gestion.
- Une sauvegarde des enregistrements vidéo redondée.
- Un test d'extraction de ces enregistrements de façon périodique.
- Une limitation aux seules personnes habilitées pour l'accès physique au serveur/stockeur.
- L'utilisation d'un VLAN indépendant pour les flux vidéo avec une garantie de bande passante et de confidentialité des données.
- Une solution de service afin de maintenir en conditions opérationnelles les installations déployées.

➢ ***Infrastructure Système et Réseau***

D'une manière générale, la solution de Sûreté mise en place par la Société pour le compte du Client s'appuie sur son Réseau LAN et WAN ainsi que des serveurs mis en œuvre pour héberger la solution. Il est du ressort du Client d'assurer le Maintien en Condition Opérationnelle de son infrastructure Système et Réseau afin que la solution de Sûreté mise en œuvre puisse fonctionner dans de bonnes conditions, et selon les prérequis du constructeur de la solution.

Le Client doit également assurer la sécurité Informatique de son infrastructure selon les normes et les bonnes pratiques du domaine cf. l'annexe « PAS – Annexe Infogérance ».