Plan d'Assurance Sécurité Annexe « Services Managés »

1. Introduction

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

2. Description du système

La Société décline ci-dessous les différentes mesures de sécurité applicables dans le cadre de l'externalisation de tout ou partie du Système d'Information du Client, sous forme d'hébergement de ressources serveurs ou de services managés.

Cette annexe porte sur l'ensemble des Services Managés proposés au CLIENT, dont notamment, sans que cela soit exhaustif :

- ✓ ***Do'BaaS*** : Sauvegarde externalisée de fichiers et documents
- ✓ ***Do'Cloud*** : Hébergement de machines virtuelles
- ✓ ***DNS/SSL*** : Gestion des noms de domaines, DNS publiques et certificats SSL
- ✓ ***Do'DRaaS Backup*** : Sauvegarde externalisée de systèmes physiques ou virtuels complets (Bar Metal)
- ✓ ***Do'DRaaS Réplication*** : Réplication externalisée de machines virtuelles dans le Cloud
- ✓ ***Do'Messagerie*** : Service de messagerie hébergée
- ✓ ***Do'Secu - Do'EPaaS*** : Gestion de la sécurité des emails
- ✓ ***Do'Secu - Do'AVaaS*** : Gestion des protections antivirales
- ✓ ***Do'Secu - Do'FWaaS*** : Gestion des pare-feu
- ✓ ***Do'Secu - Do'WFaaS*** : Gestion des réseaux Wifi
- ✓ ***Do'Supervision*** : Supervision du Système d'Information

3. Mesures de sécurité

3.1. Transfert

Certaines offres de services dont Do'Cloud, Do'BaaS, Do'DRaaS Backup et Do'DRaaS Réplication peuvent nécessiter un transfert de données depuis les infrastructures du Client vers les infrastructures de la Société.

La Société se porte garant de l'intégrité et de la confidentialité des données qui lui sont confiées pendant la phase de transfert.

A ce titre, toute modification ou suppression de la source de données initiale ne pourra être imputée à la Société. Le Client réalisera et gérera ses sauvegardes de manière à permettre une reprise en cas d'incident lors de la bascule du système.

Le transfert du Système d'Information se conclut par le passage en production sur l'environnement de la Société suite à l'acceptation de livraison par le Client.

Durant cette phase de transfert, la Société mettra en place la solution la plus adaptée pour rapatrier les données du Client en prenant en compte les problématiques de volumétries, disponibilités et coupure de service maximale souhaitées par le Client.

Les transferts de données ont lieu soit via des connexions chiffrées ou par support externe avec chiffrement des données sur le support.

Dans le cas, où la source de ces données serait amenée à être supprimée, modifiée ou corrompue par des actions non réalisées par la Société, le transfert pourra être relancé depuis le début et le coût supplémentaire sera supporté par le Client.

En cas de non-validation du passage en production à la date validée avec le Client et s'il est nécessaire de relancer une synchronisation à une date ultérieure, le coût de ce nouveau transfert sera facturé au Client.

3.2. Exploitation

La Société présente dans ce paragraphe les mesures mises en place pour assurer la protection des services externalisés.

- ***Hébergement des environnements***

Solutions Do'Cloud, Do'AVaaS, Do'FWaaS, Do'BaaS, Do'DRaaS Backup et Do'DRaaS Réplication

L'intégralité des systèmes et serveurs hébergeant ces solutions sont situés en Datacenter Tier3+.

La console de gestion Do'BaaS est située dans un Cloud privé partenaire.

Pour les solutions Do'BaaS et Do'DRaaS, les données sont stockées chiffrées dans notre Datacenter.

L'exploitation de l'environnement est réalisée depuis les locaux de la Société qui bénéficie d'une connexion sécurisée vers le Datacenter. La plateforme fait l'objet d'un contrôle et d'une surveillance aux heures ouvrées.

Seul le personnel autorisé est habilité à accéder aux équipements physiquement en Datacenter.

La Société applique les correctifs recommandés par les fournisseurs de solutions matérielles ou logicielles (logiciels système ou applicatifs, logiciels embarqués) sur tous les matériels supportant le service fourni au Client. Ces correctifs comportent ceux nécessaires à l'amélioration de la sécurité.

Sur la solution, la responsabilité du maintien en conditions opérationnelles de la Société s'arrête à l'infrastructure d'hébergement.

Solutions DNS/SSL, Do'EPaaS, Do'WaaS, Do'Supervision, Do'Messagerie

Les consoles de gestion de ces solutions sont hébergées dans les Datacenter de nos partenaires.

L'exploitation de l'environnement est réalisée depuis les locaux de la Société qui bénéficie d'une connexion sécurisée vers le Datacenter. La plateforme fait l'objet d'un contrôle et d'une surveillance aux heures ouvrées.

Seul le personnel autorisé est habilité à accéder aux équipements physiquement en Datacenter.

La responsabilité du maintien en condition opérationnelle et des mises à jours de sécurités appartient au partenaire. La Société s'engage à appliquer les demandes du partenaire afin de garantir le bon fonctionnement et la sécurité du service.

- ***Protection antivirale***

La Société préconise la mise en place d'une solution antivirale afin de pérenniser et sécuriser les données et systèmes du Client.

La Société propose et préconise l'utilisation d'une solution antivirale hébergée. Les mises à jour des signatures de la solution sont automatiques et réalisées régulièrement.

La solution est supervisée par la Société afin d'en garantir le bon fonctionnement.

- ***Mises à jour, correctifs de sécurité du Système d'Information Client***

Le Client est responsable de l'infogérance de son Système d'Information hébergé.

Le Client peut déléguer cette responsabilité à la Société via un contrat spécifique.

La Société préconise la mise à jour et l'application des correctifs de sécurité sur le Système d'Information du Client afin de protéger la confidentialité, l'intégrité des données.

- ***Sauvegardes et restaurations***

Le Client est responsable de la sauvegarde de ses données qu'il confie à la Société.

Le Client peut déléguer cette responsabilité à la Société en option. La Société mettra alors en place des mesures qui s'imposent en termes de sauvegarde et de restauration pour se conformer au niveau de service demandé par le Client.

La fiabilité des sauvegardes peut être mise à l'épreuve par des tests de restauration à la demande du Client, dont les rapports seront communiqués dans le mois suivant les tests. Ces tests font l'objet d'options contractuelles spécifiques.

La Société recommande la sauvegarde et des tests de restaurations réguliers du Système d'Information du Client afin de pouvoir assurer la disponibilité des données.

- ***Authentification***

Les interfaces d'accès aux fonctionnalités bas niveau (configuration du BIOS, interface des systèmes de sécurité et filtrage, routeur, switchs, etc..) ne sont accessibles que depuis une console d'administration permettant d'authentifier les administrateurs habilités.

Les identifiants des comptes d'accès sont dans la mesure du possible nominatifs. L'utilisation d'un même compte par plusieurs personnes n'est pas autorisée sauf pour contrainte justifiée, identifiée.

L'utilisation de mots de passe constructeur ou par défaut est proscrite. L'utilisation de protocoles dont l'authentification est diffusée en clair est interdite.

La Société met en place une politique de mot de passe conforme aux exigences du présent PAS pour les accès administrateurs et utilisateurs.

- ***Confidentialité et intégrité des flux***

Tous les flux d'administration sont chiffrés par des procédés fiables (SSH, SSL, IPSec, etc.), garantissant la confidentialité et l'intégrité des données. De plus, l'administration des équipements au sein de la Société s'effectue sur des liens d'interconnexion sécurisés.

De même, tous les flux contenant des informations sensibles et circulant sur un réseau public sont chiffrés par des procédés apportant ces mêmes garanties.

➢ *Contrôle et filtrage des flux*

Afin de garantir le cloisonnement des différents réseaux du Client et de la Société, la Société a mis en place les mesures suivantes :

- ✓ Les réseaux de la Société ne sont pas accessibles depuis les réseaux du Client ;
- ✓ Les réseaux du Client ne sont pas accessibles depuis les réseaux de la Société ;
- ✓ La Société accède aux réseaux du Client hébergé mutualisé avec les mêmes outils que les systèmes On Premise afin de garantir le cloisonnement du Client ;
- ✓ Chaque Client est isolé par un firewall dédié sur un réseau dédié ;
- ✓ Chaque environnement Client bénéficie d'un réseau virtuel (VLAN) dédié et étanche.

Dans le cadre de la fourniture et l'administration des services managés, conformément aux exigences de sécurité, la Société dispose de zones ayant leur propre niveau de sécurité, chacune étant protégée par un dispositif de filtrage :

- ✓ Une zone publique (WAN) matérialisée par l'accès Internet ;
- ✓ Une zone démilitarisée (DMZ) regroupant les machines exposées à l'extérieur ;
- ✓ Une zone privée (LAN) regroupant les machines n'étant pas exposé directement à Internet ;
- ✓ Un réseau dédié à l'administration des machines et des équipements à partir de postes de travail situés dans le domaine d'administration de la Société.

Le trafic réseau en provenance et à destination du système fait l'objet d'un contrôle permanent afin de n'autoriser que les flux légitimes. Une matrice de flux (inventaire des flux légitimes) est identifiée par la Société.

La politique de filtrage est définie à partir de la matrice des flux. Les dispositifs de filtrage sont bloquants par défaut, tout ce qui n'est pas explicitement autorisé étant interdit.

Le service global est protégé contre les attaques classiques sur IP et les protocoles associés notamment :

- ✓ Attaque en déni de service (TCP SYN Flood, Ping Flooding, SMURF, Ping of Death, large packet attacks, etc.) ;
- ✓ IP options (source routing, etc.).

Les interfaces d'administration des différents services sont accessibles uniquement via des protocoles sécurisés et chiffrés.

Seuls les services utiles au bon fonctionnement de l'application sont activés. Les autres services sont désactivés et si possible désinstallés.

La Société met à disposition du Client hébergé un pare-feu dédié. La Société préconise l'utilisation des trois zones suivantes :

- ✓ Une zone réseau public (WAN) qui définit les équipements actifs provenant de l'extérieur ;
- ✓ Une zone démilitarisée (DMZ) pour accueillir les services directement exposés à Internet ;
- ✓ Une zone privée (LAN) pour les équipements actifs appartenant à son réseau privé.

Le Client peut déléguer la gestion de son pare-feu à la Société via un contrat spécifique. La gestion du pare-feu n'est possible que depuis le réseau privé du Client ou le réseau dédié à l'administration des services de la Société.

- ***Protection contre les incendies, la foudre et les dégâts des eaux***

En ce qui concerne la protection contre les incendies, la foudre et les dégâts des eaux, des moyens ont été mis en œuvre conformément à la norme Tiers3+ du Datacenter partenaire de la Société où sont hébergés les services.

Les services hébergés chez les partenaires éditeurs de la Société remplissent les conditions de protection indiquées par les dit partenaires et sont disponibles sur simple demande.

- ***Formations et sensibilisations dans le domaine de la sécurité du Système d'Information des personnels en charge des prestations***

La fréquence et le contenu des formations et des sensibilisations du personnel aux enjeux de sécurité sont réalisés par un plan de formation défini chaque année.

- ***Surveillance et contrôle des accès aux locaux***

Pour le Datacenter, la Société bénéficie des moyens de sécurité d'accès aux locaux suivant via son partenaire :

- ✓ Moyens de surveillance, dispositifs anti-intrusion ;
- ✓ Contrôle et enregistrement des accès (gardiennage, moyen d'identification, etc.) ;
- ✓ Protection physique des équipements (verrouillage des baies, etc.).

Pour les services hébergés par les partenaires de la Société, cette dernière bénéficie des moyens mis en œuvre par ses partenaires pour sécuriser leurs installations respectives.