

ANNEXE A – MESURES TECHNIQUES ET ORGANISATIONNELLES *(Version du 13 novembre 2018)*

Le sous-traitant décrit ci-dessous les mesures techniques et organisationnelles, applicables au(x) service(s) de Mindbaz et garantissant un niveau de sécurité adapté au risque :

1 – Mesures organisationnelles

1.1 – Organisation interne

Conformément à l'article 37 du RGPD, le sous-traitant a désigné **un délégué à la protection des données** en la personne de Téva Boesch, désigné en raison de ses qualités professionnelles et de ses connaissances spécialisées du droit et des pratiques en matière de protection des données.

Le Responsable de Traitement peut contacter le DPO à l'adresse suivante : dpo@m6.fr

Le sous-traitant veille à ce que, dans l'exercice de ses missions, le DPO :

- Soit impliqué correctement et en temps opportun dans toutes les questions relatives à la protection des données personnelles
- Ne reçoive aucune instruction
- Soit soumis au secret professionnel ou à une obligation de confidentialité, conformément au droit de l'Union ou au droit des Etats membres.
- Ne puisse pas être relevé de ses fonctions ou pénalisé par le Responsable de Traitement ou les éventuels sous-traitants

Un RSSI au sein de la Direction de l'Audit et du contrôle des risques du Groupe M6 est en charge de définir les politiques, règles ou plans d'action en sécurité informatique, d'accompagner leur déploiement et de contrôler leur application et efficacité,

Une première équipe technique est dédiée à la gestion des réseaux, systèmes et sécurité informatique de l'hébergement et une seconde à la sécurisation du Groupe M6 pour les réseaux et postes de travail utilisateurs.

1.2 – Documentation Interne

Le Groupe M6 a mis en place un corpus documentaire afin de définir les principes fondateurs en matière de sécurité informatique et de protection des données personnelles, notamment au regard du RGPD. A ce titre, M6 WEB s'engage à joindre à son règlement intérieur :

- La Politique de Sécurité des Systèmes d'Information (PSSI)
- La Politique de Protection Données Personnelles
- La Charte Informatique
- La Charte des Informaticiens

Le Groupe M6 s'engage à ce que l'ensemble de ces documents soit porté à la connaissance de ces collaborateurs avant l'entrée en vigueur du RGPD et qu'ils permettent d'assurer un niveau de confidentialité et de sécurité conformes à la réglementation en vigueur.

1.3 – Collaborateurs et confidentialité

Le sous-traitant s'engage à ce que tous les collaborateurs du Groupe M6, quels que soient leurs métiers, responsabilités et niveaux hiérarchiques :

- Connaissent l'ensemble de la Documentation Interne;
- Appliquent la Documentation Interne sur tous les périmètres où celle-ci est opérante, et plus généralement dans la protection du Groupe M6 contre les risques liés à la sécurité des SI et à l'accès aux données personnelles ;
- Collaborent au quotidien avec les responsables de la sécurité des SI pour maîtriser les risques
- Appliquent une vigilance de tous les instants par rapport aux menaces liées à la sécurité des SI;
- Manipulent les données numériques et les échangent avec l'extérieur dans le strict respect de la réglementation en vigueur.

Ces engagements portent sur l'ensemble des périmètres, des organisations, des métiers et des processus du groupe.

En outre, le Groupe M6 sensibilise l'ensemble de ces collaborateurs à la réglementation sur la protection des données personnelles, notamment au travers de journées de formation et de sensibilisation et de mise en place d'outil de contrôle interne.

2 – Sécurité informatique

M6 WEB s'engage à protéger les données personnelles, privées, confidentielles et sensibles et les systèmes utilisés pour traiter, collecter ou transporter de telles données. Cette section décrit les mesures employées par M6 WEB pour respecter son engagement.

Accès logique de Mindbaz

- Une transmission sécurisée des identifiants par email et message unique à durée de vie limitée est réalisée suite à la demande de création des utilisateurs
- La complexité du mot de passe est conforme aux recommandations de la CNIL : 8 caractères minimum avec un chiffre, une lettre majuscule, une lettre minuscule, un caractère spécial
- Le renouvellement des mots de passe est réalisé tous les 6 mois pour les clients
- Le blocage du compte est effectif au bout de 5 tentatives infructueuses. Le compte est débloqué sur demande auprès du service client
- La création d'un nouveau mot de passe par mécanisme de perte de mot de passe est disponible

Accès technique

- Les accès directs à la base de données Mindbaz ne sont pas autorisés aux clients, des API sécurisés permettent de réaliser des échanges entre le service Mindbaz et les serveurs clients
- Les comptes de base de données sont revus une fois par an et documentés en terme d'usage et de propriétaire
- Les accès serveurs sont réservés uniquement à l'équipe d'exploitation d'ODISO

Chiffrement

- Les communications Web (« https ») sont chiffrées pour les Utilisateurs et les appels API
- Les échanges des fichiers d'export de données sont réalisés avec le protocole SFTP en utilisant des comptes distincts de l'application Web

- Les mots de passe des utilisateurs sont chiffrés à l'aide d'un hachage cryptographique utilisant un grain de sel.

Journalisation et surveillance

- L'application permet la conservation des traces applicatives :
 - des actions d'administration des comptes Mindbaz
 - des exports de données réalisées à travers Mindbaz
 - des authentifications des comptes utilisateurs
- Les systèmes informatiques disposent également de traces techniques de bas niveau

Gestion des vulnérabilités

- Des tests d'intrusion de type « boîte noire » (à l'aveugle) et « boîte grise » (avec des identifiants valides) sont réalisés régulièrement par un prestataire PASSI (labélisée par l'ANSSI) et donne lieu à des correctifs
- Un outil d'analyse de sécurité Web permet d'analyser en continu la qualité du chiffrement et l'utilisation correcte des entêtes Http.

Accès physique

- Le centre de données dispose d'équipements de vidéosurveillance, de contrôle d'accès par badge et biométrie, de service de gardiennage 24 heures sur 24, de baies enfermées dans des cages sous clés. Des revues régulières des accès sont réalisées au moins 1 fois/an et au départ des administrateurs
- Les locaux du Groupe M6 sont également dotés de vidéosurveillance, de contrôle d'accès par badge des bâtiments et d'une définition de zones d'accès de publique à très restreint (accès aux salles techniques) en lien avec l'activité des collaborateurs sur validation managériale

Gestion de l'identité numérique du personnel M6 WEB

- Tous les membres du personnel du Groupe M6 (permanents, intermittents, stagiaires, prestataires externes...) reçoivent un compte utilisateur nominatif leur permettant l'accès aux données et aux applications du Groupe M6 validés par son Manager
- Ces comptes utilisateurs du personnel M6 WEB sont désactivés dès le départ du collaborateur au regard de la fin de son contrat ou de sa mission et supprimés définitivement au bout de 3 mois
- Le Groupe M6 exige que tous ses utilisateurs protègent leur compte utilisateur avec des mots de passe conformes à la stratégie du Groupe M6 en termes de longueur, de complexité, d'expiration et de réutilisation du mot de passe.
- Les membres du personnel du Groupe M6 ont interdiction de partager les informations d'identification ou de compromettre des mots de passe en les stockant dans ou sur tout support non protégé sous forme de texte clair et lisible. Cette obligation est rappelée dans la charte informatique.

Comptes à privilèges

- Les comptes à privilèges ou clés SSH (compte administrateur réseau, système ou base de données...) sont associés à une identité nominative afin de maximiser la responsabilisation et la vérifiabilité. Ils sont utilisés à chaque fois que possible pour réaliser des tâches d'administration uniquement et ne sont pas utilisés pour des raisons de commodité.
- Les comptes à privilèges ne sont pas partagés sauf si une application ou un système ne prend pas en charge plusieurs comptes d'utilisateurs privilégiés dédiés.

- Tous les comptes d'utilisateurs qui viennent, préconfigurés avec un nouveau matériel et/ou un logiciel par défaut, sont désactivés. Seuls les comptes d'utilisateurs nominatifs sont utilisés
- Tous comme les comptes utilisateurs, les comptes à privilèges sont désactivés immédiatement dès le départ de leur propriétaire

Réseaux

- Des mécanismes de réponse automatique aux attaques informatiques permettent de bloquer les échanges réseaux malicieux par l'analyse des trames réseaux (attaque DDOS ...) ou de filtrer les demandes selon des critères d'appartenance à des listes de réputation mondiales ou d'autres critères
- Des restrictions des ressources disponibles sur internet sont réalisées par filtrage au niveau réseau
- La ségrégation des réseaux est réalisée à plusieurs niveaux : Entre la zone bureautique et les zones de production, entre les zones de production au sein de ODISO et également entre les entités du Groupe M6. Chaque client possède son sous-réseau dédié
- Les connexions des administrateurs à distance sont réalisées à travers des VPN uniquement

Serveurs

- Une sauvegarde des systèmes et bases de données est réalisée tous les soirs avec une politique d'archivage. Les sauvegardes sont externalisées sur un site externe sécurisé
- Un dispositif de monitoring temps réel mesurant la disponibilité et de la consommation des ressources des serveurs permet de surveiller le système et de créer des alertes
- La mise à jour de sécurité des serveurs est réalisée régulièrement dès publication des packages
- La restriction des accès permet uniquement aux administrateurs via des clés SSH nominatives de se connecter aux serveurs

Postes de travail

- Le poste de travail est fourni avec un antivirus recevant une mise à jour hebdomadaire de la base virale et réalisant un scan du disque dur 2 fois par semaine, l'ensemble est supervisé par le Groupe M6
- Un Antivirus messagerie et de flux permettent de filtrer les fichiers malveillants provenant d'internet
- L'Anti-malware et l'analyse de la réputation des fichiers permettent de bloquer les malwares et les programmes indésirables avant exécution
- Les mises à jour de sécurité de Windows et des grands logiciels grands publics (Adobe, VLC, 7zip...) sont réalisées dans le mois de la diffusion par télédistribution
- Les postes sont configurés avec des restrictions des droits d'administration par une console d'administration centrale du Groupe M6
- La mise en veille en cas d'inactivité est automatique et impose une réouverture par la saisie du mot de passe