Politique de Securex en matière de sécurité et de confidentialité des informations

11001
1010
01J

Securex s'engage à protéger la confidentialité, l'intégrité et la disponibilité des informations de ses clients.

La plate-forme Securex a été conçue pour garantir différents degrés de protection afin de prévenir ou limiter les menaces de sécurité et satisfaire aux réglementations légales et aux attentes de ses clients.

Personnel

Directeur de la sécurité : il est propriétaire du document sous-jacent. Toute modification de nos politiques doit être approuvée et signée par ses soins.

Responsable de la confidentialité des données : le directeur est assisté du responsable de la confidentialité des données. Le responsable de la confidentialité des données est la personne de contact pour toutes les questions relatives à la confidentialité des données. Ce dernier suit également l'évolution des réglementations en matière de protection des données et organise des programmes de sensibilisation dans ce cadre.

Audit interne (AI) : le département AI de Securex se charge de surveiller le respect des clauses de confidentialité et contrôle l'accès aux informations confidentielles.

Recrutement : tous les membres du personnel de Securex sont sélectionnés par le département RH au cours du processus de recrutement. Chaque employé et partenaire contractuel est tenu de signer une clause de confidentialité.

Sensibilisation et formation : tous les membres du personnel de Securex suivent une formation consacrée aux politiques en matière de sécurité et de confidentialité et sont sensibilisés à ce sujet. Tout nouveau recrutement ou toute nouvelle réglementation s'accompagne d'une mise à jour ou d'une nouvelle formation.

Sécurité physique et environnementale

Securex exploite ses systèmes dans des centres de données hautement sécurisés répondant aux normes ISAE 3402 et conçus pour minimiser l'impact des arrêts de fonctionnement. Ces centres sont physiquement sécurisés pour prévenir toute intrusion, manipulation et autres dommages, au moyen de caméras de surveillance et de badges d'accès électroniques délivrés au personnel. Les centres de données sont équipés d'une alimentation électrique et d'une connectivité réseau redondantes, d'un contrôle climatique et d'un système anti-incendie.

Sécurité logique et réseau

Securex utilise des techniques d'architecture de sécurité, de renforcement des serveurs, de surveillance du réseau, de détection des intrusions, d'isolement des données et de contrôle de sessions pour protéger les systèmes et les données des clients. Tout transfert de données vers les serveurs de Securex est crypté AES 256 bit et utilisent des connexions SSL/TLS.

Développement et maintenance

Securex dispose d'un cycle de vie de développement logiciel robuste incluant des pratiques de développement logiciel sécurisées, des techniques de conception et de codage sécuritaires, ainsi qu'un contrôle du code source et des tests d'assurance de la qualité. Tous les logiciels sont maintenus à jour et bénéficient de toutes les mises à niveau nécessaires en matière de sécurité et de maintenance.

securex
human capital matters

Pour de plus amples informations, contactez security@securex.eu

Récupération post-catastrophe et continuité des activités

Securex a mis en place des procédures et des systèmes pour sauvegarder les données sur site et les transférer quotidiennement vers un site extérieur. Securex dispose également de systèmes de surveillance automatiques capables de détecter et solutionner les arrêts de fonctionnement, ainsi que les problèmes de capacité et de dysfonctionnement du système.

Par ailleurs, toutes les données sont en permanence dupliquées et transférées vers notre Centre de récupération post-catastrophe. La validation de notre solution de récupération post-catastrophe est testée chaque année en situation réelle.

Les services Securex sont conçus pour garantir la fiabilité, la disponibilité, la performance, avec un service continu à 99 %.

Surveillance du réseau et réponse aux incidents

Securex utilise des outils et des systèmes de contrôle centralisé des fichiers de log pour détecter tout dysfonctionnement, activité anormale ou intrusion dans son réseau, ses ressources et ses hébergeurs informatiques. Securex dispose de procédures de réponse aux incidents, afin de rechercher, isoler, désactiver ou cesser toute activité suspecte détectée.

Authentification et accès

Securex requiert des identifiants pour accéder à son réseau et à ses services, et utilise une segmentation appropriée du réseau. Securex a mis en place des contrôles administratifs et techniques pour authentifier les individus, garantir des mots de passe non déchiffrables avec cryptage unidirectionnel et une révision périodique des rôles d'accès.

Rétention et retour des données

Securex conserve et protège les données de ses clients pendant toute la durée de l'accord de services ou plus longtemps si requis par la loi. Sur demande, Securex aidera à retourner les données au client au format standard et à supprimer les traces d'informations restantes. Les politiques de Securex garantissent l'écrasement des données restantes et la démagnétisation, le déchiquetage ou la destruction des supports physiques.

Éditeur responsable Group Securex, Piet Rosseel, avenue de Tervueren 43, 1040 Bruxelles - 740E003 - 201601206

securex
human capital matters