



Politique de sécurité physique

Responsable de la politique : CEO

Date d'entrée en vigueur : 23 février 2024

Visée

Empêcher tout accès physique non autorisé ou tout dommage aux informations et aux installations de traitement de l'information de l'entreprise.

Champ d'application

Tous les bureaux et sites de Evalandgo Software. La présente politique s'applique à tous les employés de Evalandgo Software, ainsi qu'à tous les intervenants extérieurs disposant d'un accès physique aux installations détenues ou louées par Evalandgo Software.

Politique

Périmètre de sécurité physique

Les bureaux physiques et les installations de traitement doivent respecter tous les codes de construction locaux, notamment en ce qui concerne les matériaux de construction des murs, fenêtres, portes et mécanismes de contrôle des accès. Certaines zones intérieures peuvent être identifiées comme des zones sécurisées, dont l'accès physique est restreint à un sous-ensemble d'employés de Evalandgo Software, comme les bureaux privés, les armoires de câblage, les salles d'impression et de serveurs, et les baies de serveurs.

Dispositifs de contrôle d'accès physique

Les zones sécurisées doivent être protégées au moyen de dispositifs de contrôle d'accès appropriés de manière à garantir que seul le personnel autorisé puisse y accéder. Dans la mesure du possible, les systèmes de contrôle des accès de Evalandgo Software doivent être liés à un système centralisé qui fournit un contrôle d'accès précis au niveau de chaque individu. Les événements d'accès doivent être consignés de la manière adéquate et examinés lorsque nécessaire, en fonction du risque associé. Des caméras et des systèmes de détection d'intrusion doivent être employés dans les installations qui stockent ou traitent des données de production ou des données internes sensibles de l'entreprise.

Sécurisation des bureaux, des salles et des installations

La sécurité physique des bureaux, des salles et des installations doit être pensée et mise en œuvre de manière à protéger ces sites contre le vol, la mauvaise utilisation, les menaces environnementales, l'accès non autorisé ou toute autre menace susceptible de compromettre la confidentialité, l'intégrité et la disponibilité des données et systèmes classés.

Protection contre les menaces extérieures et environnementales

Une protection physique contre les catastrophes naturelles, les attaques malveillantes ou les accidents doit être définie et mise en œuvre. Les zones sécurisées doivent être surveillées au moyen de contrôles appropriés, tels que des systèmes de détection d'intrusion, des alarmes et/ou des systèmes de vidéosurveillance lorsque cela est possible. L'accès des visiteurs et des tiers aux zones sécurisées doit être restreint afin de réduire le risque de perte et de vol d'informations.

Les installations de traitement de production doivent être équipées de dispositifs de contrôle environnementaux et de continuité des activités appropriés, notamment de systèmes d'extinction des incendies, de contrôle et de surveillance du climat et d'alimentation de secours. Les équipements du système d'information et l'infrastructure de soutien doivent être régulièrement entretenus conformément aux recommandations du fabricant.

Travail dans des zones sécurisées et gestion des visiteurs

Les visiteurs, le personnel de livraison, les techniciens et autres agents externes ne doivent pas être autorisés à accéder aux zones sécurisées sans escorte et/ou surveillance appropriée. Tout personnel de Evalandgo Software amené à rencontrer des visiteurs sans escorte doit s'enquérir de leur identité et leur statut, et s'assurer que ceux-ci retournent dans les zones approuvées, ou signaler leur présence à l'autorité responsable, le cas échéant. L'accès d'intervenants extérieurs aux zones sécurisées doit faire l'objet d'une approbation préalable par le personnel approprié de Evalandgo Software. Tout personnel de Evalandgo Software permettant à des intervenants extérieurs d'accéder à des zones sécurisées doit s'assurer que ce personnel tiers respecte toutes les exigences de sécurité, et sera tenu responsable de toutes les actions entreprises par les intervenants extérieurs auxquels il a accordé l'accès. Les visiteurs peuvent être autorisés à travailler sans escorte à condition que la partie de Evalandgo Software les ayant invités puisse garantir qu'ils ne pourront accéder de manière non autorisée aux systèmes d'information, réseaux et données de Evalandgo Software.

Zones de livraison et de chargement

Les points d'accès, tels que les zones de livraison et de chargement, où tout autre espace à partir duquel des personnes non autorisées sont susceptibles de pénétrer dans des zones sécurisées, doivent être contrôlés et, si possible, isolés des installations de traitement des informations afin d'empêcher tout accès non autorisé.

Sécurité des fournisseurs, des sous-traitants et des tiers

Les fournisseurs, sous-traitants et tiers doivent se conformer aux exigences en matière de dispositifs de contrôle de sécurité physique et environnementaux de Evalandgo Software. Evalandgo Software évaluera la pertinence des dispositifs de contrôle de sécurité physique tiers dans le cadre du processus de gestion des fournisseurs, conformément à la politique de gestion des tiers.

Exceptions

Les demandes d'exception à la présente politique doivent être soumises à l'approbation du responsable des ressources humaines.

Violations et application

Toute violation connue de cette politique doit être signalée au responsable des ressources humaines. Toute violation de cette politique peut entraîner le retrait ou la suspension immédiats des privilèges système et réseau, et/ou une sanction disciplinaire conformément aux procédures de l'entreprise, pouvant aller jusqu'au licenciement.

Version	Date	Description	Auteur	Approuvé par
1.0	23-Févr-2024	Première version	Valentin Boschatel	Valérie Marusiak