Instructions de travail

Politique de sécurité pour les fournisseurs de services_A.15.1

Table des matières

1. Objectif

1.1 Situation de départ

Le groupe Welser Profile exploite un système de gestion de la sécurité de l'information (ISMS). Ce système oblige le groupe Welser Profile à définir et à documenter des directives, des procédures et des instructions de travail qui sont décrites dans l'annexe A.15 "Relations avec les fournisseurs" de la norme DIN EN ISO 27001.

1.2 Objectif du document

Cette politique définit les règles de sécurité de l'information que les prestataires de services doivent suivre lorsqu'ils manipulent des informations et des équipements informatiques (par exemple, des PC, des postes de travail, des ordinateurs portables, des portails UWP).

Les prestataires de services sont définis comme tout tiers qui fournit des services à l'UWP sur la base de relations contractuelles et qui utilise l'accès et les services informatiques de l'UWP pour fournir ses prestations ou qui a accès à des informations UWP au moins confidentielles. Cette politique s'adresse à la direction des prestataires de services, à leurs employés ainsi qu'à leurs auxiliaires d'exécution (ci-après dénommés prestataires).

2. Termes et abréviations

Voir le glossaire Gallois

3. Champ d'application

Cette directive s'applique aux sites de production A, D et US (sauf SRF), ainsi qu'à tous les VNL du groupe Welser Profile.

4. Compétences

Les compétences sont régies par le chapitre 5.

5. Description

En ce qui concerne l'apport d'appareils informatiques sur le site de l'entreprise UWP ou dans des zones de sécurité du donneur d'ordre qui ne sont pas fournies par le donneur d'ordre, les règles de la société concernée s'appliquent.

L'utilisation de données ou de logiciels appartenant au client sur des systèmes informatiques ou des appareils de stockage qui ne sont pas mis à disposition ou validés par le client ou le prestataire de services n'est pas autorisée.

L'utilisation de données UWP sur des services de fichiers ou des services de cloud Internet non validés par le client n'est pas autorisée.

La transmission de données à des tiers n'est autorisée qu'avec l'accord écrit du propriétaire des données du donneur d'ordre.

Les règles du client concernant la collecte, le traitement et l'utilisation des données personnelles doivent être respectées.

Les collaborateurs du prestataire de services doivent être tenus par leur direction au respect de la confidentialité au sens de l'accord de confidentialité existant entre le client et le prestataire de services. Le client doit avoir accès à tout moment à ces accords. Si les données du client sont stockées sur des systèmes mobiles ou des appareils informatiques, ceux-ci doivent être cryptés à l'aide de matériel ou de logiciels correspondant à l'état actuel de la technique.

Après la fin du contrat, les données du client doivent être remises au client et doivent être effacées des appareils et supports de stockage du prestataire de services. Les exigences légales (par ex. obligations de conservation) doivent être respectées.

5.1 Sécurité du personnel

Un identifiant d'utilisateur qui n'est plus nécessaire ou un droit d'accès aux données du donneur d'ordre qui n'est plus nécessaire doit être immédiatement signalé par l'utilisateur concerné aux services donneurs d'ordre respectifs (p. ex. Service Desk, personne de contact interne au projet).

Les appareils (par exemple les ordinateurs portables) et les supports de données ou de stockage mis à disposition doivent être restitués au client à l'expiration du contrat ou lorsqu'ils ne sont plus nécessaires. La perte d'appareils informatiques remis à l'utilisateur ainsi que de supports à des fins d'authentification doit être immédiatement signalée par le contractant au service compétent du client.

5.2 Sécurité physique et environnementale

Les équipements informatiques qui stockent ou traitent des données du client doivent être utilisés de manière à ce qu'aucune personne non autorisée ne puisse voir ou accéder à ces données. Une attention particulière doit être portée à l'utilisation de systèmes mobiles.

Les documents confidentiels et secrets ne doivent jamais être laissés sans surveillance afin d'éviter qu'ils ne soient consultés par des personnes non autorisées.

5.3 Gestion des valeurs propres à l'organisation

Les informations ne doivent être rendues accessibles qu'à un groupe de personnes autorisées, aux fins des activités convenues et dans le respect des règles correspondantes. Le principe "ne connaître que si nécessaire" doit être respecté à cet égard.

En règle générale, les informations de catégorie "confidentielle" ou supérieure ne peuvent pas être divulguées sans accord de confidentialité. En outre, ces données doivent être stockées sous forme cryptée afin de garantir une sécurité adéquate.

5.4 Règles générales de sécurité

L'espionnage industriel et les cyber-attaques augmentent massivement dans de nombreux pays. Afin d'éviter le vol de données, l'espionnage et d'autres attaques de cybersécurité, veuillez suivre les points suivants :

- N'utilisez pas de connexions Wi-Fi publiques ou d'hôtel si des alternatives sûres sont disponibles.
- Utilisez la "navigation anonyme" pour éviter de stocker localement les sites que vous visitez, mais sachez que le fournisseur d'accès (carrier) a toujours accès à ces données.
- Utilisez HTTPS au lieu de http
- Ne publiez jamais de contenu sur les médias sociaux dans le cadre de votre travail.
- Si vous recevez des textes, des e-mails ou des liens inhabituels, supprimez-les immédiatement.
- Les disques durs et les clés USB doivent être cryptés
- Ne laissez JAMAIS quelqu'un d'autre emprunter ou utiliser votre matériel ;
- Installez toujours les mises à jour en temps voulu
- Faites attention aux "surfeurs d'épaule" - toute personne qui surveille physiquement l'utilisation de votre appareil. Installez un pare-vue de qualité sur votre ordinateur portable
- Utilisez un gestionnaire de mots de passe ou n'enregistrez pas de mot de passe dans les navigateurs ou en texte clair dans les fichiers.
- Désactivez tous les protocoles réseau inutiles (tels que WiFi, Bluetooth ou infrarouge) s'ils ne sont pas utilisés.
- Lors de réunions dans des salles de conférence, partez toujours du principe que chaque microphone, téléphone ou appareil de vidéoconférence enregistre ou écoute.

5.5 Exigences techniques de sécurité pour les contractants ayant accès au réseau interne UWP

Les exigences suivantes doivent être respectées par tous les prestataires de services appartenant à l'une des catégories suivantes :

- Prestataires de services auxquels des clients (terminaux) sont mis à disposition par l'UWP.
- Prestataires de services connectés au réseau UWP via des accès à distance ou d'autres solutions VPN avec accès direct.
- Prestataires de services directement connectés.
- les prestataires de services qui accèdent au réseau UWP sur place, dans l'usine, avec leur propre équipement informatique.

5.5.1 Organisation interne

En ce qui concerne l'utilisation du matériel et des logiciels UWP mis à disposition, les règles suivantes s'appliquent entre autres.

- Toute modification du matériel, du système (p. ex. changement d'une adresse IP fixe) et des paramètres de sécurité (p. ex. paramètres du navigateur) doit toujours être approuvée par le service informatique de l'UWP.
- L'utilisation ou la modification ultérieure de programmes du donneur d'ordre n'est autorisée que si elle est approuvée par les services informatiques d'UWP.
- Aucune donnée d'autres clients n'appartenant pas à l'UWP ne doit être traitée sur les appareils informatiques mis à disposition par l'UWP.
- L'utilisation d'équipements informatiques ou de données du client par des collaborateurs du prestataire de services requiert l'autorisation expresse du client. Le donneur d'ordre est autorisé à interdire à tout moment l'accès ou l'utilisation (par ex. en cas d'abus).

5.5.2 Sécurité physique et environnementale

Les appareils mis à disposition et appartenant à l'UWP doivent être traités de manière appropriée et protégés contre toute perte ou modification non autorisée. Les prescriptions du fabricant concernant la protection des appareils doivent être respectées. L'utilisateur est responsable de protéger au mieux l'appareil contre la perte ou le vol.

5.5.3 Protection contre les logiciels malveillants

En cas de suspicion d'infection par un logiciel malveillant, les appareils informatiques UWP et les supports de données concernés ne doivent plus être utilisés. Le service compétent (UWP Service Desk à l'adresse 2000@welser.com ou par téléphone au +437443800-2000) doit être immédiatement informé.

5.5.4 Contrôle d'accès

<u>Exigences commerciales pour le contrôle d'accès</u>

Les consignes suivantes doivent être respectées par tous les utilisateurs :

Exigences générales

- Il est interdit d'utiliser l'identifiant ou le compte d'une autre personne.
- La transmission de moyens d'identification (par ex. jetons matériels pour l'authentification à deux facteurs) n'est pas autorisée.
- Les mots de passe ou les codes PIN d'un identifiant destiné à un usage personnel (appelé "identifiant personnel") doivent être tenus secrets et ne doivent pas être divulgués.
- Il est interdit de stocker ou d'écrire des mots de passe (par exemple sur papier, via des appareils mobiles ou dans des fichiers), sauf si cela est considéré comme une méthode sûre.

- Dès qu'il y a suspicion de compromission ou de divulgation d'un mot de passe ou d'un code PIN, celui-ci doit être immédiatement modifié.
- Les mots de passe temporaires (par exemple pour les nouveaux comptes) doivent être modifiés lors de la première connexion.
- Tous les mots de passe doivent être modifiés régulièrement. Si des personnes non autorisées ont pris connaissance du mot de passe ou si elles le soupçonnent, il faut immédiatement en changer.
- Les mots de passe doivent être classés au moins comme confidentiels.
- Si l'utilisateur quitte le système en cours de fonctionnement (par ex. pause, réunion), il doit activer un verrouillage du système (par ex. écran de veille protégé par un mot de passe).

Génération de mots de passe

Lors de la génération d'un mot de passe, les exigences suivantes doivent être remplies :

- Il est interdit aux collaborateurs (du preneur d'ordre) d'utiliser un mot de passe identique à des fins professionnelles et privées pour accéder aux systèmes du donneur d'ordre.
- La longueur minimale des mots de passe imposée par les systèmes doit être respectée. Elle est déterminée par les prescriptions de la réglementation correspondante. Le mot de passe doit toutefois présenter la complexité suivante : Au moins 10 caractères avec 3 des 4 types de caractères (majuscules, minuscules, chiffres, caractères spéciaux).
- Les mots de passe triviaux ou les mots de passe à connotation personnelle ne sont pas autorisés.
- Pour les systèmes ou les applications, il convient d'utiliser des mots de passe complexes.

Identifiants de groupe

La réutilisation de certains identifiants de groupe par plusieurs personnes n'est autorisée que dans des cas exceptionnels et sous réserve du respect des conditions suivantes :

- L'attribution de l'identifiant est effectuée par une personne compétente. Cette personne établit un protocole écrit indiquant qui utilise quel identifiant et à quel moment, et archive le protocole correspondant.
- La réception de l'identifiant doit être confirmée par écrit par l'utilisateur concerné. Cette confirmation est conservée par la personne responsable de l'identification de l'utilisateur.
- Après avoir reçu son identifiant, l'utilisateur concerné doit changer son mot de passe en un mot de passe connu de lui seul.
- Après avoir rendu l'identifiant correspondant, la personne responsable doit changer le mot de passe en un mot de passe connu d'elle seule.

Les identifiants qui peuvent être utilisés simultanément par plusieurs personnes (appelés "identifiants de groupe") ne sont autorisés que si ces identifiants permettent uniquement l'exécution d'applications disposant d'une gestion séparée des

utilisateurs, y compris une authentification personnelle, et sont limités aux accès en lecture.

5.5.5 Contrôle d'accès aux réseaux

Un appareil informatique UWP mis à disposition par le client ne peut être connecté à des réseaux étrangers à l'entreprise (par ex. hot spot, WLAN privé ; à l'exception des réseaux de téléphonie mobile) que si cela est fait pour établir une connexion avec le réseau UWP (via accès à distance/VPN). Les connexions à distance doivent être établies via une authentification à deux facteurs. Si la connexion n'est plus nécessaire, elle doit être coupée.

5.5.6 Retrait des droits d'accès

Si la relation contractuelle prend fin ou si le collaborateur du mandataire n'a plus besoin de l'accès au réseau UWP ou aux applications UWP pour fournir sa prestation, une suppression / désactivation doit être initiée immédiatement auprès du service compétent du mandant.

5.5.7 Sauvegarde des données

Les personnes externes doivent s'assurer que les informations sont sécurisées de manière adéquate.

5.5.8 Notification des incidents de sécurité

Les personnes externes sont tenues de signaler immédiatement les incidents de sécurité pertinents.

L'inscription se fait par écrit à l'adresse e-mail 2000@welser.com ou par téléphone au (+437443) 800-2000.

Les personnes externes sont tenues d'aider à l'analyse et à la résolution des incidents de sécurité.

5.6 Enregistrements

Désignation	Documentation/emplacement	Responsable	Rangement

6. Gestion des modifications

La gestion des modifications de ces AA est soumise à l'IT et doit être effectuée selon les besoins.

7. Responsables de la mise en œuvre

voir la liste des responsables de la mise en œuvre du PMS

8. Documents à joindre

Liste des responsables de la mise en œuvre du PMS