Sécurité des Ressources Humaines

Politique et procédure de contrôle des employés

Propriétaire	Version	Édité par	Date	Historique des changements
Solumada	1.0	Rudo Courtney Togara (Responsable de la sécurité de l'information)	09 juin 2023	Création du document et l'ajout des informations pertinentes.
Solumada	1.1	Kushal Mulleea (Coordinateur de la sécurité de l'information)	12 Octobre 2023	Révision du contenu et ajustements nécessaires
Solumada	1.2	Kushal Mulleea (Coordinateur de la sécurité de l'information)	12 Janvier 2024	Ajout du section 10 avec la procédure d'information de la direction supérieure.

Classification

Confidentiel	Restreint	Non classé
X		

Pertinence par rapport à la norme

Standard	Numéro de la clause
ISO 27001	6.2

Introduction

Pour assurer la sécurité des ressources humaines (ISO 27001, clause 6.2), une politique et une procédure de départ des employés sont mises en œuvre pour garantir de bonnes pratiques en matière de sécurité de l'information et de protection des données au sein de Solumada. Compte tenu des transitions qui se produisent lorsque les employés quittent l'entreprise, des mesures de sécurité appropriées doivent être appliquées pour protéger les données sensibles de l'entreprise et maintenir l'intégrité de ses systèmes. Ce document décrit les raisons pour lesquelles la procédure est nécessaire et énumère les actions à entreprendre pour assurer un départ adéquat des employés tout en préservant la sécurité de l'information.

La politique et les mesures mises en place dans ce document pour un contrôle efficace des employés sont essentiels pour les raisons suivantes:

1. **Protection des informations sensibles**

Ce processus permet de protéger les données sensibles de l'entreprise contre tout accès non autorisé ou toute utilisation abusive.

2. **Prévenir les violations de données**

Les employés qui ont démissionné peuvent avoir accès à des données précieuses de l'entreprise, notamment des informations sur les clients, des éléments de propriété intellectuelle, des documents financiers et des secrets commerciaux. En gérant efficacement leur départ, le risque de violation de données, de menaces internes ou de divulgations non autorisées est minimisé.

3. **Maintien de l'intégrité du système**

La suppression des droits d'accès des employés qui quittent l'entreprise garantit l'intégrité des systèmes et des réseaux de votre entreprise. Elle réduit les risques de modification non autorisée des systèmes, d'altération des données ou d'interruption des activités de l'entreprise.

4. **Atténuer les menaces internes**

Si la plupart des employés quittent l'entreprise en bons termes, il est possible que certains d'entre eux nourrissent de mauvaises intentions ou soient mécontents. Un processus de départ

approprié permet d'identifier et d'atténuer les menaces internes potentielles en examinant minutieusement les privilèges d'accès et en prenant les mesures qui s'imposent.

5. **Transition des responsabilités**

Lorsqu'un employé démissionne, il est important de transférer en douceur ses responsabilités et ses connaissances à son remplaçant ou à d'autres membres de l'équipe. Cela permet d'assurer la continuité des opérations et de minimiser les perturbations dans les projets ou les flux de travail critiques.

Conformément à la norme ISO 27001, les informations sensibles doivent être traitées et protégées de manière appropriée. En mettant en œuvre un processus de vérification complet, Solumada peut démontrer qu'elle respecte les normes du secteur et ses obligations contractuelles. Cela contribue également à préserver la réputation de l'entreprise et la confiance de ses parties prenantes, y compris les clients, les partenaires et les actionnaires.

Vous trouverez ci-dessous le processus complet de sortie pour les employés qui quittent Solumada, quel que soit leur poste/rôle.

La procédure de sortie/contrôle des employés

1. **Préavis**

Les employés doivent annoncer leur démission suffisamment à l'avance pour permettre une meilleure planification et une meilleure répartition des tâches pendant la période de transition.

Actions à entreprendre :

L'employé doit soumettre sa notification au personnel responsable des ressources humaines à l'avance. Après cette notification, la procédure de sortie doit commencer afin de garantir un processus et une transition en douceur.

2. **Entretien de sortie :**

Un entretien de départ doit être mené avec l'employé qui quitte l'entreprise dans le but de comprendre son rôle, ses privilèges d'accès et toute information sensible à laquelle il a eu accès. Cela permettra d'identifier les potentiels risques en matière de sécurité ou les sujets de préoccupation.

Actions à entreprendre :

Une copie de la **fiche d'enregistrement de l'entretien de sortie,** dont le lien figure ci-dessous, doit être établie pour chaque entretien:

https://docs.google.com/spreadsheets/d/1yGk0x0TJYqEMc5hUMTbS0LuzpDlcgXvyPx5DD06Vhus/edit?usp=sharing

L'entretien de départ doit être réalisé conformément aux lignes directrices figurant dans la feuille Excel mentionnée ci-dessus. À la fin de l'entretien, les résultats doivent être utilisés pour déterminer les mesures à prendre. Par exemple, si l'employé a accès aux données de connexion des plateformes des clients, cela doit être indiqué dans la feuille d'enregistrement de l'entretien de départ et les mesures nécessaires doivent être prises au moment prévu pour s'assurer que tous les accès sont révoqués.

3. **Examen du compte**

Les comptes d'utilisateur et les privilèges d'accès de l'employé à divers systèmes doivent être examinés, y compris la messagerie électronique, le réseau, les bases de données, les applications et toute autre plateforme pertinente. L'accès aux systèmes qui ne sont plus nécessaires pour le rôle de l'employé sortant doit être immédiatement désactivé ou révoqué.

Actions à entreprendre:

Le département informatique doit nommer des personnes chargées de procéder à un examen à 360 degrés de tous les accès et de veiller à ce que tous les accès qui ne sont plus nécessaires soient désactivés ou révoqués à la date prévue. Après avoir confirmé que l'employé n'a plus d'accès, le personnel informatique doit envoyer un courriel au responsable des ressources humaines, confirmant que l'examen est terminé. Si des problèmes de sécurité sont identifiés, ils doivent être communiqués au responsable des ressources humaines et au responsable de la sécurité de l'information.

4. **Réinitialisation du mot de passe**

Réinitialisez les mots de passe de l'employé pour tous les systèmes pertinents afin de vous assurer qu'il ne peut plus accéder aux ressources de l'entreprise après son départ. Cette étape comprend la désactivation ou la modification de tout compte partagé ou de service associé à l'employé. Il s'agit d'une étape importante, en particulier lorsque l'employé quittant l'entreprise occupe un poste donnant accès à un compte partagé.

Actions à entreprendre :

Les chefs d'équipe ou les chefs de service doivent s'assurer que, dans le cas décrit ci-dessus, le(s) mot(s) de passe est/sont réinitialisé (s).

5. **Récupérer les actifs de l'entreprise**

Veiller à ce que l'employé qui quitte l'entreprise restitue tous les biens matériels appartenant à l'entreprise, tels que les ordinateurs portables, les smartphones, les cartes d'accès, les clés USB et tout autre équipement ou support de stockage qui lui ont été fournis pendant son emploi.

Actions à entreprendre:

Le personnel informatique doit se concerter avec le chef d'équipe ou le chef de service pour s'assurer que tous les biens de l'entreprise sont restitués et qu'ils sont entretenus en conséquence si cela s'avère nécessaire.

6. **Transfert de données ou Handover**

Si l'employé sortant était responsable de projets critiques ou d'informations sensibles, facilitez le transfert des connaissances et des responsabilités à son remplaçant ou à d'autres membres de l'équipe. Ce processus minimise les lacunes en matière de connaissances et réduit le risque de perte ou de mauvaise manipulation des informations.

Actions à entreprendre:

Le chef d'équipe ou le chef de service doit faciliter le transfert d'informations si cela s'avère nécessaire. Il convient de noter que cela doit être fait pendant la période de préavis afin de ne pas avoir à le faire après avoir quitté l'entreprise.

7. **Sauvegarde des données**

Effectuez une sauvegarde des fichiers et des données liés au travail de l'employé qui quitte l'entreprise, en particulier s'il était impliqué dans des projets uniques ou critiques. Cette mesure de précaution permet de préserver des informations précieuses et de s'y référer plus facilement en cas de besoin.

Actions à entreprendre:

Les informations relatives au projet dont l'employé sortant était responsable doivent être sauvegardées par le chef d'équipe ou le département afin d'éviter la perte d'informations importantes.

8. **Formation des employés**

Renforcer la sensibilisation à la sécurité parmi les employés, y compris ceux qui quittent l'organisation. Rappelez à ces employés leurs obligations en matière de protection des informations sensibles, même après leur démission.

Actions à entreprendre:

Le personnel des ressources humaines doit veiller à rappeler à l'employé sortant la nécessité de rester discret sur les informations confidentielles ou sensibles de l'entreprise, même après son départ.

9. **Audit de sécurité**

Envisagez de procéder à un audit ou à une évaluation de la sécurité après le départ de l'employé pour vous assurer que tous les privilèges d'accès ont été révoqués de manière appropriée et qu'il n'y a pas de failles de sécurité ou de points d'accès non autorisés.

Actions à entreprendre:

Le responsable de la sécurité de l'information (ISO) examinera tous les documents résultant de la procédure de vérification de chaque employé sortant afin de s'assurer que ce qui doit être fait l'a été de manière exhaustive.

10. **Informer la direction générale de la sortie**

Enfin, un courriel formel doit être envoyé à Sylvain et Varadha, avec le responsable de la sécurité de l'information (Rudo) en copie. Le courriel doit être conforme au modèle ci-dessous.

Sujet : Annonce : Départ de [nom de l'agent/nom de l'employé]

Chère [équipe de direction],

Je vous écris pour vous informer d'un changement important au sein de notre équipe. [Nom de l'agent/Nom du salarié], qui a été un membre précieux de notre équipe, quittera l'entreprise le [dernier jour de travail, par exemple le MM/DD/YYYY].

[Nom de l'agent/nom du salarié] était responsable des projets ou du département suivants

- [Insérer le nom du projet ou du service]
- [Insérer le nom du projet ou du service]
- Ajoutez-en d'autres si l'ancien employé travaillait dans plusieurs projets ou départements.

La procédure de sortie a été mise en œuvre et l'entretien de sortie a également été mené.

Si vous avez des questions ou des préoccupations concernant cette transition, n'hésitez pas à contacter [Vos coordonnées ou le point de contact désigné].

Nous vous remercions de votre compréhension et de votre soutien pendant cette période de changement.

Veuillez recevoir mes salutations les plus distinguées,

[Nom de l'expéditeur]

Le personnel des ressources humaines, le personnel désigné par le département informatique, le chef de département ou d'équipe et le responsable de la sécurité de l'information seront chargés d'appliquer la procédure de départ des employés. Il s'agit d'un processus intense qui doit être mené à bien afin d'assurer une transition sûre et sécurisée tant pour les employés sortants que pour Solumada elle-même.

----------Fin de document----------