Procédure de gestion du roulement du personnel

ATTAM

DROITS - JUSTICE - ÉQUITÉ

Adoptée le 26 septembre 2023

1. Aperçu

Le départ d'un membre du personnel peut entraîner des dommages intentionnels, accidentels ou une perte de données. Avec une liste de rôles et de leurs accès ainsi que d'une politique à appliquer avant un départ, vous pourrez éviter la plupart de ces pertes.

2. Objectif

Le but de cette politique est d'établir une liste de contrôle au sein de l'organisation pour encadrer le départ d'un membre de l'équipe.

3. Portée

La portée de cette procédure inclut tous les individus qui quittent l'organisation et qui possédaient des accès physiques aux appareils et systèmes de l'organisation, ou aux comptes et différentes plateformes de l'organisation.

4. Procédure

4.1 Entrevue de départ ou mise à pied

4.1.1 Éteindre les ordinateurs et appareils professionnels de l'employé.

4.1.2 Désactiver l'accès de l'employé à tous les systèmes. Suivre la liste des rôles et des accès.

4.1.3 Supprimer les données professionnelles des appareils appartenant aux employés :

Observer l'utilisateur supprimer les comptes de messagerie de son téléphone.

Une personne de l'équipe informatique peut le faire par effacement à distance, ce qui peut potentiellement supprimer des données personnelles (à utiliser avec prudence).

4.1.4 S'assurer que l'employé retourne tout équipement appartenant à l'organisation : ordinateurs portables, tablettes, clés USB, etc.

4.1.5 Compiler une liste de tous les emplacements où l'employé a stocké des données professionnelles, y compris les plateformes de stockage infonuagiques.

4.2 Téléphone

4.2.1 S'assurer que le numéro de téléphone de l'employé n'est pas transféré à un numéro externe, tel qu'un téléphone portable personnel.

4.2.2 Changer le mot de passe de la messagerie vocale.

4.2.3 Modifier le message vocal sortant conformément à vos directives de communication.

4.2.4 Désigner une personne pour surveiller la messagerie vocale jusqu'à ce que ce numéro de téléphone puisse être supprimé ou réaffecté.

4.3 Accès aux courriels

4.3.1 Idéalement, ne jamais supprimer le compte courriel d'un employé. La bonne pratique serait de créer une boîte courriel partagée et de bloquer les accès tel que mentionné plus bas.

4.3.2 Modifier le mot de passe du compte dans le système de courriels de l'organisation. Passer en revue la section 4.4 Accès au réseau et au Cloud avant de réactiver le compte.

4.3.3 Si l'employé a utilisé un téléphone mobile personnel ou une tablette pour accéder à sa messagerie professionnelle, effacer ou supprimer le compte de messagerie si ce n'est déjà fait.

4.3.4 Créer un message d'absence pour le compte de messagerie conformément aux directives de communication de votre organisation. Par exemple: Désolé cette boite courriel n'est plus attitré à un employé temporairement, veuillez écrire à la coordination à l'adresse courriel suivante: coordoattam@gmail.com

4.3.5 Supprimer l'employé des listes de diffusion de courriels internes.

4.3.6 Supprimer l'employé des listes de diffusion de courriels spécialisées. S'assurer que quelqu'un d'autre est membre pour ne pas manquer ces communications.

4.3.7 Contacter les fournisseurs avec lesquels l'employé a travaillé pour les informer du départ et leur fournir un nouveau contact.

4.3.8 Désigner quelqu'un et lui donner les accès pour surveiller le courrier électronique de l'employé. Déterminer combien de temps la boîte de courriels restera disponible- Jusqu'à l'arrivé d'un nouvel employé qui prendra en charge et utilisera cette adresse courriel professionnelle

4.3.9. S'assurer de changer les données dans le profile google de l'adresse courriel professionnel et de créer le message courriel temporaire de redirection.

4.4 Accès au réseau et/ou au Cloud

4.4.1 Supprimer l'employé de tous les groupes de contrôle d'accès pour la connexion au domaine de l'organisme, VPN, bureau à distance, système d'organisation et autres systèmes.

4.4.2 Déplacer tous les fichiers de travail qui ont pu être stockés en dehors des dossiers de sauvegarde principaux de l'organisation vers un emplacement central.

4.4.3 Révoquer l'accès de l'employé au compte infonuagique d'organisation.

4.4.4 Supprimer les fichiers de travail de tout compte de stockage personnel.

4.4.5 Passer en revue les règles d'accès au pare-feu pour confirmer que l'utilisateur ne dispose d'aucun autre accès, tel qu'un VPN direct depuis son pare-feu personnel à la maison.

4.4.6 Confirmer qu'aucun logiciel d'accès à distance n'est installé sur les appareils (LogMeIn ou TeamViewer), que l’employé pourrait utiliser pour accéder à l'ordinateur ou au réseau.