

GUIDE DE GESTION DES ENTREES-SORTIES ET MOUVEMENTS DE PERSONNELS

Revision History

Last updated	Janvier 2021
--------------	--------------

GROUPE MEDIA CONTACT SA

 Avenue Dorothée LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 **+229 95 17 00 16**
contact@groupmediacontact.com

 **RCCM N° : RB/COT/13B 10291**
IFU N° : 3201300930112

Sommaire

I-	INTRODUCTION	3
II-	LA GESTION DES ENTREES / ADMISSIONS DANS L'ENTREPRISE.....	4
III-	LA GESTION DU CHANGEMENT DE FONCTION	5
IV-	LA GESTION DU DEPART DE L'EMPLOYE	5
V-	CONTROLE ET REPORTING.....	7

GRUPE MEDIA CONTACT SA

 Avenue Dorothée LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 **+229 95 17 00 16**
contact@groupmediacontact.com

 **RCCM N° : RB/COT/13B 10291**
IFU N° : 3201300930112

I- INTRODUCTION

Evolution du monde et des générations oblige, les mouvements de personnel au sein des entreprises se multiplient tellement qu'il devient essentiel de mettre en place de vrais processus informatisés pour fluidifier les entrées-sorties de l'entreprise et éviter fraudes, piratages et pertes de données.

L'objectif de cette procédure, dont la responsabilité globale dépend logiquement des Ressources Humaines, est de pouvoir confirmer que tous les employés présents dans l'entreprise sont bien ceux qui ont signés un contrat et sont employés par celle-ci. Pour des raisons de simplicité de fonctionnement, il arrive que le compte d'un employé ayant quitté l'entreprise soit maintenu pour faciliter les procédures internes. Parfois même, le manager n'informe pas l'informatique du départ d'un salarié espérant pouvoir régulariser la situation rapidement. Enfin, pour les changements / mutations en interne (transfert d'un département à l'autre ou changement de fonction), les Ressources Humaines ne sont pas régulièrement informées.

Les risques relatifs à une mauvaise gestion de la cohérence des listes des employés et de la liste des droits d'accès aux Systèmes d'Information sont :

- * **Sécurité physique** : une personne pourrait utiliser un badge d'un employé ayant quitté l'entreprise pour effectuer des actes de fraude, vols d'effets personnels, vols de propriété intellectuelle, usurpation d'identité et en cas d'incendie, faire prendre des risques à des secouristes pour une personne qui n'est pas dans l'entreprise ou encore de provoquer un conflit avec l'assurance suite à la présence d'une personne non déclarée, ...
- * **Sécurité logique** : usurpation d'identité/profil informatique pour bypasser les contrôles anti-fraude, effectuer des transactions engageant la responsabilité

d'une personne inexistante dans l'entreprise, ...

* **Sécurité informationnelle** : cas d'une personne usurpant une identité d'un employé pour communiquer des fausses informations à l'extérieur de l'entreprise, ...

Les cas sont nombreux et peuvent porter un préjudice fort à l'entreprise. Le contrôle de cette procédure est donc primordial ... mais est aussi compliquée car trois acteurs au moins, RH, Systèmes d'Information et département de l'employé sont co-responsables de ce risque.

II- LA GESTION DES ENTREES / ADMISSIONS DANS L'ENTREPRISE

Cette procédure a comme point de départ le processus de recrutement. En effet, avant l'admission d'un nouvel employé, il est nécessaire de noter des informations le concernant. Il est préférable d'utiliser les systèmes d'information RH qui comportent de telles fonctionnalités et conservent de manière confidentielle les données à caractère personnel des candidats dans un premier temps de manière temporaire et des futurs employés.

Souvent en amont du premier jour d'arrivée dans l'entreprise, la signature du contrat de travail et du règlement intérieur auquel est annexée la **charte utilisateur** avec les recommandations et exigences de sécurité informatique, est importante et confirmera alors sa prise en charge vis-à-vis de l'assurance de l'employé.

- Afin que les personnes concernées soient informées des collaborateurs qui arrivent prochainement, des notifications sont envoyées aux managers, aux équipes IT et équipes RH
- Ces notifications sont envoyées par le canal mail professionnel par

GROUPE MEDIA CONTACT SA



Avenue Dorothee LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou



+229 95 17 00 16
contact@groupmediacontact.com



RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

les RH donnant les informations sur le département et fonction de la personne.

- Ensuite, il est conduit aux ressources humaines afin de remplir les toutes les informations administratives ;
- Son manager devra lui apporter les recommandations de sécurité physique nécessaires à la prise de fonction ainsi que les accès au SI.
- Enfin, les accès (emprunte digital) est créé par une ressource de l'équipe IT en présence du nouvel employé. Cet accès définit sont périmètres d'accès physique

III- LA GESTION DU CHANGEMENT DE FONCTION

Dans le cas d'un changement de fonction ou de responsabilité (y compris une promotion) dans la même entité juridique de l'entreprise, l'étape la plus importante est de revoir les droits d'accès physiques et logiques aux ressources de l'entreprise. Cette revue est gérée **<<comme un départ de la précédente affectation et une nouvelle arrivée dans le nouveau service>>**.

Cela permet d'éviter les problèmes récurrents constaté lors des revues des droits d'accès :

- S'apercevoir qu'un ancien employé possède toujours les droits d'accès de sa précédente fonction.
- Un problème de communication du changement organisationnel ainsi que de responsabilité entre les deux managers (ancien et nouveau), à la RH qui doit organiser ce déplacement et ordonner l'application de la procédure de revue des séparations des fonctions.

IV- LA GESTION DU DEPART DE L'EMPLOYE

C'est sans doute la procédure qui doit être la plus contrôlée par une

co-responsabilité : Manager et Ressources Humaines ; l'informatique quant à elle, appliquera les modifications de droits d'accès en conséquence. Comme tous les mouvements dans l'entreprise, il y a dans la phase de préparation, des étapes à respecter :

- Le manager de l'employé au départ informe la RH qui calculera le solde de tout compte et préparera les documents à signer via la procédure de sortie de personnel,
- Le manager informera le gestionnaire des droits d'accès physique (sécurité des locaux) pour mettre à jour en temps réel les droits. Il informera aussi la Direction des Systèmes d'Information pour la mise à jour des droits d'accès logiques.
- L'employé terminera son parcours de sortie en remettant à la RH un document engageant l'employé sur son interdiction de communiquer des informations dont il a eu connaissance durant son parcours professionnel dans l'entreprise.
- Enfin, le départ du salarié doit être sous la responsabilité commune du Manager et des RH qui effectueront le contrôle de l'application de la procédure de sortie de l'entreprise dont la mise à jour des droits d'accès. Cette co-responsabilité doit diminuer le risque d'information ou de matériel conservé par l'employé (pc ou téléphone non rendu par exemple).

Le formulaire de sortie avec la liste des documents et droits d'accès physique aux locaux sensibles et logiques aux Systèmes d'Information doit être mis à jour régulièrement. Pour ce qui est des droits d'accès logiques, la liste des droits doit être recalculée à partir de ce qui est constaté dans les Systèmes d'Information. Une attention particulière sera apportée pour les accès à distance et les systèmes d'identification sur l'Active Directory interne

et autre Directory dans le Cloud de l'entreprise (Microsoft ou Google).

V- CONTROLE ET REPORTING

Pour assurer les contrôles relatifs à cette procédure, il est nécessaire de mettre en place un reporting périodique qui facilitera l'auditabilité du processus :

TYPE DE CONTROLE	RAPPORT DE CONTROLE	PERIODICITE	PROCESS OWNER (S)
Extraction automatique	Liste des employés pour chaque Système d'information	Mensuelle	Direction Informatique
Extraction automatique	Liste des employés présents dans l'entreprise (avec date d'effet)	Mensuelle	RH
Déclaratif	Rapport de synthèse des écarts entre les listes des employés : RH et Direction Informatique	Mensuel	RH

GROUPE MEDIA CONTACT SA

 Avenue Dorothée LIMA, rue 11010
Gbamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

 +229 95 17 00 16
contact@groupmediacontact.com

 RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112