

## I. Objet et champs d'application

La procédure <>gestion des habilitations>> a pour mission de décrire les processus de gestion des habilitations en vigueur la Banque de l'Union Côte d'Ivoire (BDU-CI)

La gestion des habilitations consiste à gérer le cycle de vie du personnel de la banque (embauche, promotion, départ) et leur impact sur le système d'information de la BDU-CI (création des comptes utilisateurs, attribution de profil métiers, mise en œuvre de contrôle d'accès, etc ;)

Cette procédure s'applique l'ensemble des applications métiers et systèmes de la banque, notamment:

- **L'application core banking en production** : Amplitude ;
- **L'application monétique** : PowerCard ;
- **L'application gestion de transferts internationaux** : SWIFT/RTGS
- **L'application de télé compense** : WebClearing ;
- **L'application de signature** : VSIGN/VSCAN
- **L'application de paie** : Sage ;
- **L'application de gestion des courriers électronique** : Messagerie sur poste de travail
- **Le système d'exploitation des postes de travail** : Windows utilisateurs ;
- **Le contrôleur du domaine** : Active Directory ;
- **L'application de gestion des produits** : BANK TO WALLET ;
- **Les extranets de la monétique** : Extranet Mastercard;
- **Les systèmes spécialisés** : Informis, Windows server, Routeur, Switch, Firewall,...;
- Etc.

Cette procédure couvre principalement les étapes suivantes :

- Création d'une habilitation ;
- Modification d'une habilitation ;
- Suppression d'une habilitation ;
- Gestion des profils personnalisés

## **II. Objectifs du contrôle interne**

- Assurer le respect du principe du moindre privilège : chaque utilisateur doit disposer uniquement des droits nécessaires pour accomplir ses missions, ni plus ni moins. L'objectif est de réduire les risques de sécurité en limitant les droits d'accès ;
- Assurer le respect de la séparation des tâches : éviter que la même personne puisse effectuer des tâches incompatibles ou potentiellement frauduleuses ;
- Protéger le Système d'Information contre les dysfonctionnements liés au facteur humain, aux utilisateurs frauduleuses et à la perte ou au vol de données ;
- Assurer que les employés disposent des certifications, des autorisations et des compétences nécessaires pour leurs fonctions.

## **III. Rôles et responsabilités**

### **Direction Générale**

Sous la responsabilité du Conseil d'Administration, elle a en charge de :

- S'assurer de la mise en place d'un système intégré de gestion des risques ;
- S'assurer à travers les missions confiées au Service Organisation en matière de gestion des habilitations que les procédures en la matière sont suivies et respectées

**Service des Ressources Humaines** est chargé de :

- Informer les administrateurs des applications métiers de la reprise de l'Agent après son absence

### **Chef de Service Organisation**

est en charge de :

- Créer, suspendre, modifier ou désactiver les habilitations sur les applications suivantes
  - o Amplitude

#### **IV. Sigles et Définitions**

- **Définitions**
- **Gestion des habilitations** : la gestion des habilitations est un élément clé dans la sécurité du système d'information d'une banque. Elle permet de renforcer son niveau de sécurité globale en garantissant la cohérence des droits d'accès aux ressources informatiques

La gestion efficace des habilitations est également une réponse à une exigence réglementaire, notamment, la garantie de la traçabilité. C'est donc un moyen d'optimiser la gestion des droits et des privilèges informatiques accordés à un agent.

La gestion des habilitations doit également permettre à la banque de gérer ses relations avec ses partenaires extérieurs, ses clients, ses fournisseurs.

Par habilitation, il convient donc d'entendre l'ensemble des procédures automatisées permettant à une personne autorisée, d'accéder au système d'information de la banque, de consulter des informations et de réaliser des opérations qui, selon les privilèges données, seront prises en compte, ou non, par le système concerné.

##### **- Profil :**

Pour faciliter la gestion des habilitations, il est courant de lier l'attribution d'un ensemble d'habilitations à l'obtention d'un profil <>fonctionnel<>. Un profil fonctionnel regroupe un ensemble de rôles nécessaires à l'exécution d'une fonction métier. Un utilisateur peut avoir un ou plusieurs profils fonctionnels.

Le profil d'habilitation, auquel sont rattachés, via les rôles, les droits d'accès aux applications, est déterminé par le poste opérationnel. A chaque poste, est associé un ou plusieurs profils d'habilitation.

Le profil correspond généralement à la fonction exercée par l'acteur affecté au poste opérationnel ainsi qu'à son niveau d'expertise. Il peut aussi correspondre à un ensemble d'habilitations spécifiques.

Chaque métier ou fonction de la banque donnera lieu à la création d'au moins un profil. Il existera un profil pour le Directeur Général, un pour le Directeur du Système d'Information, un autre pour les Chargés d'Affaire etc ...

De concert avec les concernés, les profils métiers seront établis par le Responsable de l'Audit Interne en Collaboration avec le Responsable du Service Organisation. Toutefois, les opérations de modifications se feront selon la procédure mise en place.

Il doit donc exister un profil pour chaque fonction de l'organigramme ayant un besoin d'utilisation des moyens informatiques

➤ **Sigles**

**BDU-CI** : Banque de l'Union de Cote d'Ivoire

**DAI** : Directeur de l'Audit Interne

**AE/AD** : Agent Entité/Agent Demandeur

**DCHMG** : Directeur du Capital Humain et des Moyens Généraux

**DCPC** : Directeur du Contrôle Permanent et de la Conformité

**RE** : Responsable de l'Entité

**RP** : Responsable du Prestataire

**CDR** : Chef de Division Réseau

**CDI** : Chef de Division Infrastructure

**CCM** : Chef de Cellule Monétique

**CSO** : Chef de Service Organisation

**PV** : Procès-Verbal

**RSSI** : Responsable de la Sécurité du Système d'Information ;

## Sommaire de la procédure

I.	Objet et champs d'application.....	1
II.	Objectifs du contrôle interne.....	2
III.	Rôles et responsabilités .....	2
IV.	Sigles et Définitions.....	3
V.	Références / Règles de gestion.....	5
VI.	Narratif de la procédure.....	9

## V. Références / Règles de gestion

- **Documents de références**
  - **Normes ISO/IEC 27001 : 2022 et ISO/IEC 27002:2022** exigences et mesures de sécurité relatives au système de management de la sécurité de l'information;
  - **PCI-DSS v3.2.1** : exigences de sécurité applicables aux environnements traitant des données de cartes bancaires
  - **Politique de Sécurité des Système d'Information**

### ➤ **Règles de gestion**

La gestion courante des habilitations doit pouvoir être faite ou initiée d'un point de vue opérationnel par des agents n'appartenant pas à la Direction des Systèmes d'Informations (DSI) ('utilisateur lui-même, la direction des ressources humaines) et d'un point de vue technique pour appui par l'administrateur systèmes.

- La procédure de gestion des habilitations à la BDU-CI se résume ainsi en cinq (5) phases essentielles qui sont les suivantes :
  - i. **Définition de la politique de gestion des habilitations** : C'est la phase pendant laquelle la banque définit au préalable les profils métiers à créer, les pouvoirs d'autorisation (montant autorisation, accès exploitants, accès services, accès

- type de clients) qui se rattachent directement à l'utilisateur ainsi que les conditions de réalisation d'une opération dans un applicatif donné.
- ii. Gestion de la signalétique de l'utilisateur : C'est la phase d'identification de l'utilisateur de la solution informatique. Elle a donc pour objectif, la gestion du cycle de vie de l'entité utilisateur ou de gérer la relation de la banque avec son partenaire externe. La gestion de la signalétique constitue après la mise en place de manière formelle de la politique de gestion des habilitations la seconde étape importante de la procédure de gestion des habilitations. En effet, tout agent utilisant les moyens informatiques, doit disposer d'une fiche signalétique de l'utilisateur conforme à son contrat de travail.
- iii. La fiche signalétique comporte au moins, les attributs ci-après :
- Nom et prénoms
  - Numéro matricule
  - Date d'embauche
  - Nature du contrat (CDI, CDD, Stagiaire)
  - Durée du contrat s'il s'agit d'un contrat de type CDD ou stagiaire
  - La Direction ou Service de l'Agent
  - La fonction de l'Agent
  - La description des tâches de l'Agent
  - La signature de l'Agent
  - Le visa du supérieur hiérarchique de l'Agent ;
- iv. La fiche fonction prenant en compte les aspects ci-dessus énumérées peut tenir lieu de fiche signalétique :
- Création d'une habilitation : Une fois la fiche signalétique renseignée, on peut procéder à la création d'une habilitation. Le processus de création d'une habilitation concerne un agent nouvellement embauché, un stagiaire, un consultant externe ou un partenaire externe de la banque. Il s'appuie donc sur la fiche signalétique de l'Agent préalablement renseignée, et sur la politique de gestion des habilitations qui a défini au préalable, les différents profils métiers créés, leur contenu et les pouvoirs et les autorisations qui s'y rattachent.

- Modification d'une habilitation : La procédure de modification d'une habilitation concerne un Agent embauché, un stagiaire, un consultant externe ou un partenaire externe de la banque disposant déjà d'un compte utilisateur et d'un profil qui est associé. La modification peut être consécutive à l'affectation de l'Agent à un autre poste ou exercice d'un interim.
  - Désactivation d'une habilitation : Les comptes utilisateurs ne sont pas supprimés mais plutôt désactivés. Ponctuellement, lors d'un départ ou d'une mutation, la Direction du Capital Humain et des Moyens Généraux informe par mail ou par courrier le/la Responsable des Habilitations qui procède à la désactivation des comptes après consultation.
  - Groupe mail administrateur informatique : Groupe de messagerie crée et intégrant tout Agent en charge de l'administration d'un système ou applications métiers de la banque. Ce groupe sert à recevoir des mails de désactivation et de réactivation des habilitations informatique.
- v. La création, la modification et la désactivation d'une habilitation doivent être formalisée sur la fiche de demande d'habilitation. Cette fiche comprend au moins les attributs ci-après :
- Type de demande : Création, modification, désactivation
  - Date de la demande
  - Nom du demandeur.
  - Fonction du demandeur
  - Nom du bénéficiaire
  - La durée de validité de la demande. Préciser si elle est permanente
  - Le progiciel ou logiciel concerné
  - Profil métier demandé
  - Le montant d'autorisation
  - Le commentaire ou la motivation du demandeur
  - Le visa du demandeur, de son supérieur hiérarchique et du Responsable des Ressources humaines lorsqu'il s'agit d'une création

Les fiches de demande d'habilitation et les fiches signalétiques doivent être archivées numériquement ou physiquement

- Attribution des pouvoirs d'autorisation : L'autorisation est le pourvoir donné à un agent de rendre un compte débiteur ou au-delà de son pouvoir. Si par exemple l'opération a pour effet de porter le compte en dépassement, celle-ci ne pourra être validée que par le gestionnaire disposant dans son profil d'un montant d'autorisation ou de dépassement autorisé qui viendra s'ajouter à l'autorisation en cours.  
Des montants d'autorisation seront attribués aux agents par la Direction Générale. Ceux-ci interviendront donc dans la validation des transactions.  
Sur proposition de la Direction Générale, les montants d'autorisation pourront être actualisés pour répondre à des exigences circonstancielles ou temporaires.  
Ces montants d'autorisations seront inscrits dans le profil de chaque utilisateur, ou directement rattaché à celui-ci.

**VI. Narratif de la procédure**

PRO PP1 005

GERER LES HABILITATIONS INFORMATIQUES

Acteurs	Descriptions des tâches	Documents et interfaces
<b>I. Création de nouveaux profils métiers dans Amplitude</b>		
RE	<p>Pour le nouveau poste créer au sein de la banque</p> <ul style="list-style-type: none"> <li>- Elaborer la fiche de poste</li> <li>- Transmettre la fiche de poste au DCHMG pour validation</li> </ul>	Fiche de poste
DCHMG	<ul style="list-style-type: none"> <li>- Valider la fiche de poste</li> <li>- Transmettre la fiche de poste au DCPC</li> </ul>	Fiche de poste
DCPC	<ul style="list-style-type: none"> <li>- Procéder à une identification des transactions correspondant au nouveau poste</li> <li>- Faire valider les niveaux d'autorisations de transaction</li> <li>- Transmettre la fiche au CSO</li> </ul>	Fiche d'identification des transactions à autoriser
CSO	<ul style="list-style-type: none"> <li>- Réceptionner la fiche d'identification des transactions à autoriser</li> <li>- Créer le nouveau profil métier dans Amplitude</li> <li>- Archiver la fiche d'autorisation des transactions</li> </ul>	Fiche d'identification des transactions à autoriser
<b>II. Demande de création d'une habilitation informatique</b>		
AD/RP	<ul style="list-style-type: none"> <li>- Renseigner la fiche de demande d'habilitation</li> <li>- Transmettre la fiche de demande d'habilitation au RE pour validation</li> </ul>	Fiche de demande d'habilitation
RE	<ul style="list-style-type: none"> <li>- Apposer sa signature sur la fiche renseignée et motivée</li> <li>- Transmettre la fiche de demande d'habilitation DCHMG pour validation</li> </ul>	Fiche de demande d'habilitation
DCHMG	<ul style="list-style-type: none"> <li>- Recevoir la fiche de demande d'habilitation</li> <li>- C1 : Vérifier la pertinence et cohérence des informations décrites</li> <li>- Si non conforme, mentionner les observations sur la fiche de demande d'habilitation et la transmettre au DS1 pour corrections :</li> <li>- Si conforme et si corrections apportées, signer la fiche de demande d'habilitation et la transmettre au DS1 (qui constitue un premier niveau de contrôle des habilitations à</li> </ul>	Fiche de demande d'habilitation signée

Acteurs	Descriptions des tâches	Documents et interfaces
	donner en tant que responsable de la gestion du système d'information) pour validation	
RSSI	<ul style="list-style-type: none"> <li>- Recevoir la fiche de demande d'habilitation</li> <li>C2 : Sur la base des approbations des 3 premières étapes Vérifier par un contrôle de niveau 2 les risques que pourraient engendrer ces habilitations demandées</li> <li>- Si des risques existent, mentionner les recommandations sur la fiche de demande d'habilitation et la signer</li> <li>- Si pas de risque, apposer sa signature sur la fiche de demande d'habilitation</li> <li>- Sensibiliser le demandeur sur les risques liées à la sécurité des systèmes d'information en général et à l'octroi de ces habilitations en particulier</li> <li>- Transmettre au CSO/CDR/CDI/CCM et selon le périmètre d'intervention, la fiche de demande d'habilitation signée</li> </ul>	Fiche de demande d'habilitation signée
CSO/CDR/CDI/CCM	<ul style="list-style-type: none"> <li>- Recevoir la fiche de demande d'habilitation signée</li> <li>- Attribuer sur la base de la fiche signée, les habilitations nécessaires</li> </ul>	Fiche de demande d'habilitation signée  Applications métiers

### III. Demande de modification d'une habilitation informatique

AD/AE	<ul style="list-style-type: none"> <li>- Renseigner la fiche de demande de modification d'habilitation</li> <li>- Transmettre la fiche de demande de modification d'habilitation au RE pour validation</li> </ul>	
RE	<ul style="list-style-type: none"> <li>- Apposer sa signature sur la fiche renseignée et motivée</li> <li>- Transmettre la fiche de demande de modification au DCHMG pour validation</li> </ul>	Fiche de demande de modification d'habilitation
DCHMG	<ul style="list-style-type: none"> <li>- Recevoir la fiche de demande de modification d'habilitation</li> <li>C3 : Vérifier la pertinence et cohérence des informations décrites</li> <li>- Si non conforme, mentionner les observations sur la fiche de demande de modification d'habilitation et la transmettre au DSI pour corrections :</li> <li>- Si conforme et si corrections apportées, signer la fiche de demande de modification d'habilitation et la transmettre au DSI pour validation</li> </ul>	Fiche de demande de modification d'habilitation
DSI	<ul style="list-style-type: none"> <li>- Recevoir la fiche de demande de modification d'habilitation</li> <li>C4 : Vérifier par un contrôle de niveau 1, la pertinence et la cohérence des modifications demandées et la disponibilité des ressources</li> </ul>	Fiche de demande de modification d'habilitation signée

Acteurs	Descriptions des tâches	Documents et interfaces
	<ul style="list-style-type: none"> <li>- Si non conforme, mentionner les observations sur la fiche de demande de modification d'habilitation et la transmettre au AD pour corrections :</li> <li>- Si conforme et si corrections apportées, signer la fiche de demande de modification d'habilitation et la transmettre au RSSI pour approbation</li> </ul>	
RSSI	<ul style="list-style-type: none"> <li>- Recevoir la fiche de demande de modification d'habilitation</li> <li><b>C5</b> : Sur la base des approbations des 3 premières étapes Vérifier par un contrôle de niveau 2 les risques que pourraient engendrer ces modifications demandées</li> <li>- Si des risques existent, mentionner les recommandations sur la fiche de demande de modification et la signer</li> <li>- Si pas de risque, apposer sa signature sur la fiche de demande de modification d'habilitation</li> <li>- Sensibiliser le demandeur sur les risques liées à la sécurité des systèmes d'information en général et à l'octroi de ces modifications en particulier</li> <li>- Transmettre au CSO/CDR/CDI/CCM et selon le périmètre d'intervention, la fiche de demande de modification d'habilitation signée</li> </ul>	Fiche de demande de modification d'habilitation signée
CSO/CDR/CDI/CCM	<ul style="list-style-type: none"> <li>- Recevoir la fiche de demande de modification d'habilitation signée</li> <li>- Effectuer sur la base de la fiche signée et selon le périmètre d'intervention, les modifications nécessaires</li> </ul>	Fiche de demande de modification d'habilitation signée  Applications métiers

#### IV. Demande de suspension d'une habilitation informatique

AD/RE	<ul style="list-style-type: none"> <li>- Selon le planning de congés, ou en cas d'absence prolongée (mise en indisponibilité, etc...) de plus d'un (01) semaine, renseigner une fiche de départ en congés ou d'absence prolongée, signée par le Supérieur hiérarchique</li> <li>- Transmettre la fiche de départ en congés ou d'absence prolongée, au DCHMG pour traitement</li> </ul>	Fiche de départ en congés ou d'absence prolongée
DCHMG	<ul style="list-style-type: none"> <li>- Recevoir la fiche de départ en congés ou d'absence prolongée et la signer ;</li> <li>- Etablir une fiche de suspension d'habilitation et la signer ;</li> <li>- Transmettre au CSO/CDR/CDI/CCM la fiche de départ en congés/absence prolongée et la fiche de suspension d'habilitation pour traitement</li> </ul>	Fiche de départ en congés /d'absence prolongée
CSO/CDR/CDI/CCM	<ul style="list-style-type: none"> <li>- Recevoir la fiche de départ en congés ou d'absence prolongée ;</li> <li>- Recevoir la fiche de demande de suspension d'habilitation signée</li> </ul>	Fiche de départ en congés/d'absence prolongée

Acteurs	Descriptions des tâches	Documents et interfaces
	<ul style="list-style-type: none"> <li>- Effectuer sur la base de la fiche signée ou du mail de suspension reçu et selon le périmètre d'intervention, les suspensions nécessaires</li> </ul>	Fiche de suspension d'habilitation  Applications métiers

#### V. Demande de désactivation d'une habilitation informatique

DCHMG	<ul style="list-style-type: none"> <li>- En cas de démission ou de licenciement ou de fin de mission de l'Agent, établir une fiche de désactivation d'habilitation et la signer ;</li> <li>- Transmettre au CSO/CDR/CDI/CCM la fiche de désactivation d'habilitation pour traitement</li> </ul>	Fiche de désactivation d'habilitation
CSO/CDR/CDI/CCM	<ul style="list-style-type: none"> <li>- Recevoir la fiche de désactivation d'habilitation ;</li> <li>- Effectuer sur la base de la fiche signée et selon le périmètre d'intervention, les désactivations nécessaires</li> </ul>	Fiche de désactivations d'habilitation  Applications métiers

#### VI. Demande de réactivation d'une habilitation informatique

DCHMG	<ul style="list-style-type: none"> <li>- Dès la reprise de l'Agent dont les habilitations avaient été suspendues pour cause d'absence de plus d'une semaine, informer par courrier électronique le groupe administrateurs informatiques (CSO/CDR/CDI/CCM) afin de réactiver les habilitations de ce dernier de toute application et système</li> </ul>	Mail de réactivation d'habilitation
CSO/CDR/CDI/CCM	<ul style="list-style-type: none"> <li>- Recevoir le mail de réactivation des habilitations de l'agent;</li> <li>- Effectuer sur la base du mail et selon le périmètre d'intervention, les réactivations nécessaires</li> </ul>	Mail de réactivation d'habilitation  Applications métiers

#### VII. Demande de réinitialisation de mot de passe

AD/RE	<ul style="list-style-type: none"> <li>- Envoyer un mail de réinitialisation de mot de passe à l'administrateur de l'application métier concerné</li> <li>- S'il s'agit de la réinitialisation du pot de passe de la messagerie, appeler au téléphone, l'administrateur de la messagerie pour la réinitialisation du mot de passe</li> </ul>	Mail/Appel de réinitialisation de mot de passe
CSO/CDR/CDI/CCM	<ul style="list-style-type: none"> <li>- Recevoir le mail de réinitialisation. Si la réinitialisation concerne la messagerie, recevoir l'appel téléphonique de réinitialisation</li> <li>- Réinitialiser le mot de passe du demandeur</li> <li>- Informer l'Agent de la réinitialisation de son mot de passe</li> </ul>	Mail de réinitialisation de mot de passe  Applications métiers

**Annexes / Enregistrements**

- Fiche de poste
- Fiche d'autorisation des transactions
- Fiche de demande /modification/Suspension/Désactivation d'habilitation

**ANNEXE : FICHE DE DEMANDE D'HABILITATION**

**Liste des ampliations**

N°	Structures	Date	Visa	Observations
01				
02				

**Liste des modifications**

N°	Nature de la modification	Date	Chapitre ou page concerné (e)	Observations
01				
02				

Rédigé par : RESPONSABLE SECURITE SYSTEME D'INFORMATION  Date : 06/11/2025  Signature :	Validé par : COMITE PROCEDURES  Date : 06/11/2025  Signature :	Approuvé par : DIRECTION GENERALE  Date :  Signature :
---	--	--

