Objet et champs d'application

Cette procédure décrit le déroulement et toutes les dispositions pratiques permettant d'assurer une gestion efficace des accès aux systèmes informatiques de la banque afin de limiter les risques de fraudes informatiques.

Elle s'applique à :

- Tous les collaborateurs (employés, prestataires, stagiaires, partenaires).
- L'ensemble des systèmes d'information : postes de travail, serveurs, applications métiers, messagerie, réseau interne, solutions cloud, etc.

Objectifs de la procédure

Assurer la confidentialité, l'intégrité et la disponibilité des systèmes d'information de la banque en encadrant strictement la création, l'utilisation, la modification et la suppression des accès utilisateurs aux applications, bases de données, réseaux et systèmes

Rôles et responsabilités

- Tout utilisateur du SI de BDU-CI, manifestant un besoin d'accès distant ;
- Le RSSI ;
- Le Directeur du SI.

- **RSSI/Directeur du Système d'Information**: définit la politique d'accès logique, administre les droits, contrôle les accès
- Le Chef de division réseau ;
- **RE** : valide la demande de création, modification ou suppression d'accès de ses collaborateurs.
- **Utilisateur:** utilise ses identifiants de manière responsable, respecte la charte informatique.

- **Direction de l'Audit interne :** vérifie périodiquement le respect de la procédure

Sigles et Définitions

Définitions

- **Incident :** Tout événement qui ne fait pas partie du fonctionnement normal d'un service et qui provoque ou peut provoquer une interruption ou une diminution de la qualité de ce service ;
- **Partenaire :** Toute entité ne faisant pas partie de BDU-CI, avec qui il y a lieu de collaborer sur un projet ou une activité ou une opération ponctuelle à un moment donné ;
- **Utilisateur :** Personne qui utilise le système d'information de BDU-CI. Il s'agit aussi bien des utilisateurs internes que des utilisateurs externes (notamment les partenaires).
- **Accès logique** : droit d'utilisation d'un système informatique, contrôlé par identifiant, mot de passe ou autre mécanisme d'authentification.
- **Accès exceptionnel** : désigne une autorisation temporaire et particulière donnée à un utilisateur (personne, service ou application) pour accéder à des ressources, données ou systèmes informatiques auxquels il n'a normalement pas accès dans le cadre de ses droits habituels
- **Accès à haut privilège** : désigne un type d'autorisation attribuée à un utilisateur ou un compte qui lui permet d'effectuer des actions critiques sur un système informatique, au-delà des simples usages standards.
- **Accès distant :** Service permettant d'accéder à distance aux ressources informatiques de BDU-CI ;
- **Identifiant utilisateur (User ID)** : code unique attribué à un utilisateur.
- **Compte nominatif** : compte personnel attribué à une seule personne.
- **Compte technique** : compte utilisé par un service ou une application, géré sous contrôle.
- **Principe du moindre privilège** : l'utilisateur ne doit disposer que des droits nécessaires à sa mission.

- **Réseaux de plate-forme de transfert d'argent et de partenaires extérieurs : R**éseaux permettant de se connecter aux plate-formes de transfert d'argent et partenaires extérieurs.
- **Réseau internet par câble :** Il s'agit du réseau utilisé pour naviguer sur les différents sites et pages internet à travers le monde. La connexion à ce réseau est effectuée par un câble connecté au poste de travail. Ce réseau est l'une des principales sources d'infection des postes de travail (lorsque des sites web ou pages internet infectés par des hackers sont visités) et permet aux personnes malveillantes de se connecter à distance à nos systèmes d'information une fois infectés
- **Réseau d'accès à distance par liaisons VPN :** Ce sont les liaisons réseaux privée aux partenaires, prestataires ou administrateurs informatiques de la banque d'accéder à distance à une ressource informatique (serveurs, équipements réseaux) de la banque depuis leur site ou leur ordinateur. Il s'agit des réseaux suivants :
  - Réseaux VPN d'accès partenaire ;
  - Réseaux VPN d'accès administrateurs informatiques ;
  - Réseaux VPN d'accès utilisateurs.

- **Sigles**

RSSI : Responsable de la Sécurité du Système d'Information ;
RE : Responsable Entité
RP : Responsable de l'entité en charge du prestataire
DSI : Directeur du Système d'Information
DCPC : Directeur du Contrôle Permanent et de la Conformité
BDU-CI : Banque de l'Union de Cote d'Ivoire
CDE : Card holder Data Environment ;
CHD : Card Holder Data ;
DPC : Données de porteurs de cartes ;
FIM : File Integrity Monitoring ;
PAM : Privileged Access Management ;
SAD : Sensitive Authentication Data ;
SIEM : Security Information & Event Management.

Sommaire de la procédure

Table des matières

Références / Règles de gestion

➢ Documents de références réglementaires

- **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 v4.0 :** exigences de sécurité applicables aux environnements traitant des données de cartes bancaires
- Document <<Gérer les accès et les autorisations au réseau et au système informatique>>
- **Politique de Sécurité des Système d'Information**
- **BCEAO / UEMOA** : directives sur la sécurité des systèmes d'information bancaires
- **Loi locale sur la protection des données personnelles** (Loi ivoirienne n° 2013-450)

➢ Règles de gestion

L'accès aux réseaux informatiques de la banque est autorisé selon les jours suivants :

- **Du lundi au vendredi**
  - Prestataires de services et partenaires : de 08h00mn à 19h00mn ;
  - Membre du personnel : de 07h00mn à 20h00mn ;
  - Equipe d'astreinte cyber sécurité : 24H/24

- **Samedi**

- Membre du personnel des agences de quartier: de 08h00mn à 14h30mn ;
- Directeurs membres du CODIR : de 08h00mn à 20h00mn ;
- Equipe d'astreinte cyber sécurité : 24H/24

- **Dimanche et jours fériés**

- Equipe d'astreinte IT et cyber sécurité : 24H/24

- Toute demande d'accès aux réseaux informatiques d'un Agent, d'un partenaire d'un prestataire en dehors des périodes et horaires autorisés doit donner lieu à une demande d'accès exceptionnel signée par le supérieur de l'Agent ou le Responsable du service demandeur de la prestation. Cette fiche est envoyée au moins 24 heures avant le jour sollicité, au RSSI ;

- En cas d'astreintes IT, monétique, Cyber sécurité, chaque entité en charge devra diffuser au RSSI le planning d'astreinte du mois pour la modification des autorisations des Agents d'astreinte.

- En cas de travaux urgents non terminés par le prestataire devant aller au-delà de l'autorisation d'accès exceptionnel accordée :
  - Le Directeur Hiérarchique de l'Agent ou le Responsable du Service en charge du prestataire envoie un mail au RSSI avec en copie le Chef de Division Réseau, le DSI et le DCPC pour une autorisation ou prolongation des autorisations d'accès exceptionnel du prestataire;
  - En cas d'avis favorable du RSSI, le chef de division Réseau modifie les accès.
- En cas de tâche non terminée dans une Agence et devant aller au-delà de l'autorisation horaire accordée :
  - un mail est envoyé par l'Agent demandeur au Chef de Zone, avec en copie le Chef de Division Réseau, le DSI, le RSSI et le DCPC.
  - En cas d'avis favorable du Chef de Zone, le chef de division Réseau modifie les accès.
- **Accès à distance d'un Agent d'astreinte**

Toute connexion à distance d'un Agent d'astreinte en dehors des jours ouvrables et heures d'accès à distance autorisés aux Agents de la banque dans la procédure de gestion des accès distants (jours ouvrés entre 07h30mn et 19h00mn) doit être justifiée par courrier électronique au Chef de Division Réseau avec en copie le RSSI, le DCPC et le DSI.

Narratif de la procédure		
PRO-RSSI-SSI-03	Gestion des accès logiques	ARH, CSCH, Direction Générale, DCHMG

Acteurs	Descriptions des tâches	Documents et interfaces
I. Demande d'accès exceptionnel et validation des demandes		
I.1. Cas des accès aux systèmes en dehors des heures de travail		
Utilisateur/RP	- Remplir le formulaire de demande d'accès exceptionnel - Signer de la lettre d'engagement - Transmission de la fiche à son supérieur hiérarchique	Formulaire de demande d'accès exceptionnel Lettre d'engagement
RE	- Réceptionner le formulaire de demande d'accès exceptionnel - Signer du formulaire de demande d'accès exceptionnel - Transmettre la fiche signée au RSSI	Formulaire de demande d'accès exceptionnel Lettre d'engagement
RSSI	- Apprécier en liaison avec le Chef de Division Réseau et donne son accord pour l'ouverture de l'accès exceptionnel. - Le RSSI peut, le cas échéant, y ajouter des recommandations quant à l'ouverture de l'accès exceptionnel de l'agent ou du prestataire. - Transmettre la fiche d'accès exceptionnel au DCPC	Formulaire de demande d'accès exceptionnel Lettre d'engagement
DCPC	- Réceptionner le formulaire signé par le RSSI - Apprécier en liaison avec le RSSI et donne son accord pour la modification des accès. - Transmettre le formulaire de demande d'accès au Chef de Division Réseau	Formulaire de demande d'accès exceptionnel Lettre d'engagement
Chef de Division Réseau	- Réceptionner le formulaire d'accès signé - Sur la base du formulaire d'accès signé, procéder aux modifications des accès.	Formulaire de demande d'accès exceptionnel Lettre d'engagement

Acteurs	Descriptions des tâches	Documents et interfaces
I.2. Cas des accès distants aux systèmes		
Utilisateur/RP	- remplir le formulaire de demande d'accès à distance - Signer le formulaire d'accès à distance - Signer la lettre d'engagement - Transmettre le formulaire rempli et la lettre d'engagement signé à son supérieur hiérarchique pour signature	Formulaire de demande d'accès distant Lettre d'engagement
RE	- Réceptionner le formulaire rempli et lettre d'engagement singée - Signer le formulaire après analyse - Transférer le formulaire et la lettre au RSSI.	Formulaire de demande d'accès distant Lettre d'engagement
RSSI	Dès réception du formulaire de demande d'accès, - Etudier les points suivants : o La motivation de l'accès o La durée d'accès o La sensibilité des ressources pour lesquelles l'accès est demandé o L'impact de l'accès - Si manque d'informations, envoyer une demande d'informations complémentaires à l'utilisateur/partenaire ; - Marquer son avis favorable ou défavorable sur le formulaire - Transmettre le formulaire au Chef de Division Réseau	Formulaire de demande d'accès distant

Acteurs	Descriptions des tâches	Documents et interfaces
Chef de Division Réseau	- En cas d'avis défavorable, o informer l'utilisateur/Partenaire. o En concertation avec le RSSI et éventuellement l'utilisateur/partenaire chercher une solution de contournement ; - En cas d'avis favorable, o Créer les accès distants de l'utilisateur ou du prestataire. o Communiquer à l'utilisateur/Prestataire un login et un mot de passe, ainsi qu'un autre facteur d'authentification, tel que : • Token ; • Smartcard ; • Puce TPM ; • OTP Token.	Formulaire de demande d'accès distant
I.3. Cas des accès à haut privilège aux systèmes		
Utilisateur/RP	- Remplir le formulaire de demande d'accès à haut privilège. - Signer la charte d'engagement - Transmettre le formulaire de demande d'accès à haut privilège au à son supérieur hiérarchique	Formulaire de demande d'accès à haut privilège Charte d'engagement
RE	- Réceptionner la fiche de demande d'accès - Valider la fiche de demande d'accès - Transmettre la fiche de demande d'accès au RSSI	Formulaire de demande d'accès à haut privilège Charte d'engagement

Acteurs	Descriptions des tâches	Documents et interfaces
RSSI	- Réceptionner la fiche de demande d'accès - Après analyse de la demande, valider ou rejeter la demande d'accès à haut privilège - Transmettre le formulaire de demande et la charte d'engagement au RSSI	Formulaire de demande d'accès à haut privilège Charte d'engagement
Chef de Division Réseau	- Réceptionner le formulaire de demande signé par le RSSI - Si la demande d'accès est rejetée par le RSSI, informer l'utilisateur ou le prestataire et la procédure prend fin - Si la demande d'accès validée, Activer le compte à haut privilège de l'utilisateur/Prestataire - Archiver le formulaire de demande d'accès et la lettre d'engagement	Formulaire de demande d'accès à haut privilège Charte d'engagement
II. <u>Désactivation, désactivation des accès</u>		
Chef de Division Réseau	- A la fin des travaux de l'utilisateur/prestataire, désactiver les accès de l'utilisateur/Prestataire. Cette fermeture n'est pas subordonnée à un processus de validation.	

<u>Annexes / Enregistrements</u>

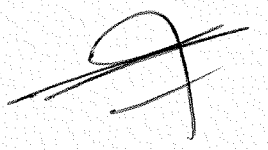
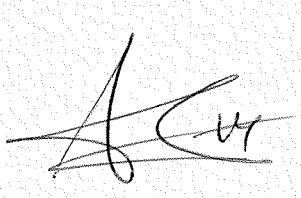
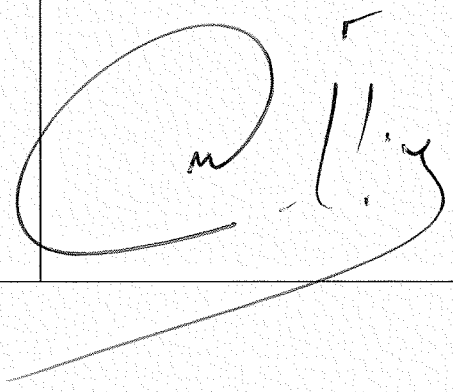
- Formulaire de demande d'accès exceptionnel
- Formulaire d'accès à distance
- Formulaire de demande d'accès à haut privilège
- Lettre d'engagement d'accès distant
- Charte d'engagement d'accès à haut privilège

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	Validé par : COMITE PROCEDURES	Approuvé par : DIRECTION GENERALE
Date : 05/11/2025	Date : 05/11/2025	Date :
Signature : 	Signature : 	Signature : 

➢ Demande d'accès à distance

1. Formulaire de demande d'accès distant

1-Type de la demande :

☐Création d'une liaison d'accès distant ☐ Suppression d'une liaison d'accès distant

☐ Activation d'une liaison d'accès distant ☐ Modification d'une liaison d'accès distant

2-Service demandé :

Type d'accès	**Ressources**	**Type d'authentification**	**Motif de la demande** :
☐ VPN ☐ FTP ☐ Bureau à distance ☐ Autres services Préciser :		☐ Clé Security ID (RSA) ☐ SafeNet (OTP) ☐ Autre (Préciser)	**Durée :** ☐ Déterminée de……à…… ☐ Indéterminée

3-Identification de l'utilisateur :

Société de l'utilisateur : Nom et prénom de l'utilisateur

Hostname (nom de l'ordinateur) : Courrier électronique :

Engagement de l'utilisateur : je prends acte des habilitations pour les services que je m'engage à utiliser conformément à la lettre d'engagement.

Approbation du RE	Nom & Prénom	Date d'approbation	Confirmation : ☐OUI ☐NON	Signature :
Approbation du RSSI	Nom & Prénom :	Date d'approbation	Confirmation : ☐OUI ☐NON	Signature :
Accès donné le : **Signature :**		**Par le chef de division réseau** **(Nom & Prénom**		

2. Lettre d'engagement de l'utilisateur

Engagement à la protection des données et à la sécurité des systèmes informatiques

Société de l'utilisateur :	Nom et prénom de l'utilisateur :
Hostname (nom de l'ordinateur) :	Courrier électronique :

Contexte d'utilisation de l'accès à distance

Le service d'accès par VPN rend possible le branchement au Réseau de BDU-CI, ce qui permet aux partenaires et utilisateurs d'accéder à distance aux applications et aux systèmes informatiques.

Afin de respecter les procédures internes de la banque, la mise en place de mesures de sécurité aussi bien pour protéger la confidentialité et l'intégrité des renseignements personnels pendant l'accès que pour limiter l'accès aux données critiques aux seules personnes autorisées est essentielle.

✓ **Objet du formulaire d'engagement**

Le formulaire d'engagement vise à informer les utilisateurs des mesures de sécurité à respecter pour assurer la protection des données et des systèmes informatiques ainsi que leurs obligations à cet effet.

✓ **Domaine d'application**

Le présent formulaire d'engagement s'applique aux informations et aux données détenues par le réseau et transmises dans le cadre du service d'accès à distance.

✓ **Principes de gestion de la sécurité des systèmes informatiques**

Les mesures de protection, de prévention, de détection, d'assurance et de correction sont mises en place afin d'assurer la sécurité des actifs informationnels du réseau de BDU-CI Ces mesures visent à assurer :

a) la **disponibilité**, laquelle est la caractéristique d'une information d'être accessible et utilisable en temps prévu et de la manière requise par une personne autorisée ;

b) l'**intégrité**, laquelle est la particularité d'une information ou d'une technologie de l'information de n'être ni modifiée, ni altérée, ni détruite sans autorisation ;

c) la **confidentialité**, laquelle est la caractéristique d'une information d'être inaccessible aux personnes non autorisées ;

d) l'**authentification**, laquelle est un acte permettant d'établir la validité de l'identité d'une personne ou d'un dispositif ;

Les mesures de sécurité énumérées dans le présent formulaire sont obligatoires et minimales.

L'utilisateur autorisé qui accède aux services de BDU-CI est responsable de la gestion sécuritaire de ces données. Il doit prendre les moyens nécessaires à la mise en œuvre et à la gestion de la sécurité des données qu'elle consulte sur son poste de travail.

Les droits d'accès aux actifs informationnels détenus par BDU-CI seront retirés s'il était prouvé que l'utilisateur autorisé ne se conforme pas aux mesures prévues au présent formulaire et rend, ou a rendu, vulnérable la sécurité des systèmes informatiques.

Mesures de sécurité des systèmes informatiques et des données que doit respecter la personne autorisée

L'utilisateur autorisé doit aviser le responsable du Service Sécurité de toute situation portée à sa connaissance qui est susceptible de compromettre la sécurité des actifs informationnels auxquels elle a accès.

L'utilisateur autorisé applique et respecte les lois et règlements qui s'appliquent à son domaine d'activité ainsi que toutes politiques, mesures et procédures en matière de sécurité des actifs informationnels auxquelles elle est assujettie.

Toute information traitant du processus et des mesures de sécurité doit être gérée de façon confidentielle.

L'accès aux données détenues par BDU-CI est accordé pour l'usage exclusif de l'utilisateur autorisé.

La configuration des outils de sécurisation (anti-virus, VPN, Firewall personnel, etc.) fournis avec le lien au partenaire ne doit pas être modifiée sans l'autorisation du RSSI.

Les documents imprimés qui contiennent des renseignements personnels et de nature sensible doivent faire l'objet de mesures de protection et de destruction qui assurent leur confidentialité.

Limites des droits d'accès aux systèmes informatiques

Les droits d'accès à distance sont approuvés par le RSSI. Ces droits sont mis à jour régulièrement et peuvent être révoqués ou suspendus en cas de non utilisation ou de mauvaise utilisation.

Résiliation

L'accord peut être résilié sur avis par l'une ou l'autre des parties. En ce cas, les droits accordés à l'utilisateur autorisé pour lui donner accès aux actifs informationnels seront révoqués.

Cession des accès

Les droits et obligations contenus dans le présent formulaire ne peuvent, sous peine de nullité de l'accord, être cédés, en tout ou en partie, sans informer au préalable le RSSI.

Mesures administratives et disciplinaires

Toute personne autorisée qui enfreint les dispositions du présent formulaire d'engagement s'expose à des mesures administratives ou disciplinaires, en fonction de la gravité et des conséquences du geste. Ces mesures peuvent inclure la révocation de ses droits d'accès aux actifs informationnels, une suspension ou un congédiement, et ce, conformément aux dispositions prévues par la banque.

Déclaration du requérant

Je m'engage à respecter les conditions d'accès lorsque j'utilise le service d'accès à distance. J'accepte aussi d'être soumis à une vérification informatique, si nécessaire.

Signature de l'utilisateur **Date**

➢ Demande d'accès à hauts privilèges

1. Fiche de demande

1-Type de la demande :		
☐ Ouverture d'un compte à hauts privilèges ☐ Désactivation d'un compte à hauts privilèges ☐ Modification d'un compte à hauts privilèges		
2-Service demandé :		
☐ Base de données : ..... ☐ Application monétique : ..... ☐ Application métier: ----------	☐ Autres services Préciser :	Authentification : ☐ Clé Security ID(RSA) ☐ SafeNet (OTP) ☐ Autre (Préciser) :
Motif de la demande : Durée : ☐ Déterminée : de.....à..... ☐ Indéterminée.....		
3-Identification de l'utilisateur :		
Nom et prénom de l'utilisateur : Nom du poste de travail : Courrier électronique :		
Engagement de l'utilisateur : je prends acte des habilitations pour les services que je m'engage à utiliser conformément à la charte d'engagement.		

Approbation du supérieur hiérarchique	Nom du N+1 :	Date d'approbation :	Confirmation : ☐OUI ☐NON	Signature :

Approbation du RSSI	Nom & Prénoms :	Date d'approbation :	Confirmation : ☐OUI ☐NON	Signature :
Accès donné le : **(Nom & Prénom) :**		**Par le Chef de Division SI Signature :**		

2. Charte d'engagement

Engagement pour l'utilisation des comptes à hauts privilèges Date :

Je soussigné,

…… , en tant qu'employé de BDU-CI, m'engage à :

- Reconnaître avoir lu et compris les politiques et procédures concernant la gestion des comptes à hauts privilèges, dans le but de les respecter.
- Ne jamais compromettre la sécurité du (ou des) compte(s) à hauts privilèges qui m'est (ou me sont) confié(s), de manière à nuire à BDU-CI à son système d'information. Le(s) compte(s) en question ne sera (ou seront) utilisé(s) que pour l'exercice de mes fonctions.
- Rapporter toute activité observée jugée suspecte, susceptible de nuire à la sécurité des comptes à hauts privilèges.

Signature

(Précédée de la mention « Lu et Approuvé »)