Objet et champs d'application

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

Elle s'applique à :

- Tous les collaborateurs de la banque (employés, stagiaires, intérimaires).
- Les visiteurs, prestataires et partenaires externes.
- Tous les locaux bancaires, notamment :
- Agence du siège
- La salle du Coffre-fort principal
- Les Agences de quartiers
- Les Agences de provinces
- Le Datacenter du siège
- Les salles d'archivage (Treichville, Anyama)
- Les différentes plateformes de travail au siège

Objectifs de la procédure

Garantir la sécurité des personnes, des biens, des infrastructures et des informations en encadrant strictement l'accès physique aux bâtiments et zones sensibles de la banque.

Rôles et responsabilités

- **Responsable de la Sécurité physique**: définit les droits, administre le système de contrôle et surveille les alarmes.
- **Manager hiérarchique** : valide les demandes d'accès de ses collaborateurs.
- **Employé**: utilise son badge personnel de manière responsable et respecte les règles de sécurité.

- **Prestataire / visiteur** : accède uniquement aux zones autorisées et sous supervision si nécessaire.

Sigles et Définitions

- Définitions

- **Accès physique** : toute entrée dans un bâtiment ou une zone sécurisée.
- **Zone sensible** : espace critique nécessitant un contrôle renforcé (salles serveurs, coffres, back-office, centre de traitement des chèques, etc.).
- **Badge d'accès** : dispositif personnel, nominatif et sécurisé permettant l'entrée.
- **Visiteur** : toute personne n'appartenant pas au personnel de la banque.
- **Badge visiteur** : dispositif temporaire d'identification et d'accès.

- **Sigles**

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 v3.2.1 :** exigences de sécurité applicables aux environnements traitant des données de cartes bancaires
- **Politique de Sécurité des Système d'Information de la BDU-CI**
- **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

- Les accès aux bureaux et locaux de travail de la banque se font via l'ouverture de la porte des plateformes par clé et l'utilisation de badge.
- Une fois la porte de la plate-forme ouverte à clé, l'Agent utilise son badge pour accéder à la plateforme sur la base de ses habilitations.
- Les portes des plates-formes permettant l'accès aux bureaux et locaux de travail sont ouvertes chaque matin et fermées chaque soir à la descente selon les périodes et horaires autorisés à l'aide de clé et code anti-intrusion détenus par plusieurs membres du staff de la banque.
- Une clé d'ouverture et code anti-intrusion de la plateforme sont attribués à chaque Directeur et de Service de la plate-forme. Chaque Chef de service est responsable de la gestion de cette clé et code et doit s'assurer que son dernier collaborateur à quitter les bureaux de son Service dispose de la clé et du code ;
- L'Agent quittant la plateforme doit fermer la plateforme à clé et activer l'alarme anti-intrusion ;
- Les doubles de ces clés sont confiés à la Direction de l'Audit Interne.
- La demande d'attribution ou modification de badge émane du Responsable de service du collaborateur concerné.
- Le badge montre la photo, le matricule et le nom du collaborateur, et est doté d'un ensemble de droits d'accès.

- En cas de perte du badge, le personnel doit signaler l'incident immédiatement au Service des Moyens Généraux et au Service Capital Humain.
- Il est Interdit de partager ou prêter son badge ;
- Il est Interdit de faire du tailgating (passage groupé derrière un badge valide) ;
- Les accès aux zones sensibles se font via double authentification (badge + code PIN).
- Le système de contrôle d'accès conserve les journaux d'événements (logs) pendant au moins 1 an ;
- Des audits internes sont réalisés régulièrement ;
- Toute anomalie (accès refusé répété, tentative d'intrusion) fait l'objet d'une alerte et d'une enquête.

❖ **Horaire d'accès aux bureaux et locaux de travail**

(Énumérer les différents Site et plate-forme de travail de BDU-CI)

Ex : Plateformes de travail du siège

➢ **Du lundi au vendredi**

- Visiteurs : de 08h 00 mn à 16h30mn ;
- Service de nettoyage : de 07h 00 mn à 17h30mn ;
- Prestataires de services et partenaires : de 08h00mn à 18h00mn ;
- Membre du personnel des Moyens Généraux et le RSSI : de 07h00mn à 20h00mn ;
- Directeurs membres du CODIR : 24H/24
- Le personnel de l'Agent : 06h30

➢ **Samedi**

- Membre du personnel des Moyens Généraux et le RSSI : de 08h00mn à 18h00mn ;
- Directeurs membres du CODIR : de 08h00mn à 20h00mn ;

➢ **Dimanche et jours fériés**

- Membre du service des Moyens Généraux : de 08h00mn à 18h00mn ;

Narratif de la procédure		
PRO-RSSI-SSI-04	Gestion des accès physiques	AD/RP/RE/DCHMG

Acteurs	Descriptions des tâches	Documents et interfaces
I. Gestion des droits d'accès du personnel		
I.1. Demande de création ou de modification d'un accès physique		
AD/RP	– Renseigner la fiche de demande d'accès physique – Transmettre la fiche de demande d'accès physique au RE pour validation	Fiche de demande d'accès physique
RE	– Apposer sa signature sur la fiche renseignée et motivée – Transmettre la fiche de demande d'accès physique au DCHMG pour validation	Fiche de demande d'accès physique
DCHMG	– Recevoir la fiche de demande d'accès physique **C1** : Vérifier la pertinence et cohérence des informations décrites – Si non conforme, mentionner les observations sur la fiche de demande d'accès physique et la transmettre au demandeur pour corrections : – Si conforme et si corrections apportées, signer la fiche de demande d'habilitation et la transmettre au RSSI pour validation – En cas de demande de création d'un nouveau badge, transmettre les informations de l'Agent (Photo, nom et prénoms, poste,…) au Responsable de la sécurité physique	Fiche de demande d'accès physique
RSSI	– Recevoir la fiche de demande d'accès **C2** : Sur la base de l'approbation du DCHMG, vérifier par un contrôle de niveau 2 les risques que pourraient engendrer ces accès demandés – Si des risques existent, mentionner les recommandations sur la fiche de demande d'accès et la signer	Fiche de demande d'accès physique

Acteurs	Descriptions des tâches	Documents et interfaces
	– Si pas de risque, apposer sa signature sur la fiche de demande d'accès physique – Transmettre au Responsable de la Sécurité Physique la fiche de demande d'accès physique signée	
Le Responsable de la Sécurité Physique	– Recevoir la fiche de demande d'accès signée – Envoyer la fiche de demande au Chef de Division Réseau	Système de contrôle d'accès
Chef de division réseau	– Attribuer sur la base de la fiche signée et des informations reçues, un badge nominatif (non transférable) et les accès nécessaires. – S'il s'agit d'une modification, procéder à la modification des accès par badge. – Informer le Responsable de la Sécurité Physique et la DCHMG de la création ou modification des accès de l'Agent	Mail
AD/RP	– Récupérer son badge – Signer dans le registre de transmission de badge	Registre de transmission de badge
I.2. Désactivation des droits d'accès		
En cas de départ d'un Agent de la banque		
Chef de service capital humain	– Informer le Responsable de la sécurité physique de la fin du contrat de l'Agent avec en copie le Chef de Division Réseau	Mail
Chef de division réseau	– procéder à la désactivation des accès accordés à l'Agent	Système de gestion des badges
En cas de perte de badge		
AD/RP	– Informer par mail, le Responsable de la sécurité physique de la fin du contrat de l'Agent avec en copie le Chef de Division Réseau de la perte du badge	Mail
Chef de division réseau	– procéder à la désactivation des accès accordés à l'Agent – Créer un nouveau badge pour l'Agent – Informer l'Agent et le Responsable de la Sécurité Physique de la création du nouveau badge	Système de gestion des badges

Acteurs	Descriptions des tâches	Documents et interfaces
AD/RP	– Récupérer son badge – Signer dans le registre de transmission de badge	Registre de transmission de badge
II. <u>Gestion des visiteurs et prestataires</u>		
II.1. Enregistrement à l'arrivée		
Agent de sécurité	– Vérifier l'identité du visiteur (carte nationale, passeport ou pièce officielle). – Inscrit dans le registre (papier ou électronique) : o Nom et prénom o Numéro de pièce d'identité o Organisme représenté o Personne visitée o Motif de la visite o Date et heure d'entrée	Registre des visiteurs.
Visiteur	– Signer dans le registre visiteur.	Registre des visiteurs.
II.2. Attribution d'un badge temporaire		
Agent de sécurité	– Attribuer un badge visiteur numéroté. – Rappeler les consignes de sécurité (interdiction d'accès aux zones sensibles, usage du téléphone limité, confidentialité,…)	Politique de gestion des badges Badge visiteur
II.3. Accompagnement du visiteur		
Agent de sécurité	– Accompagne le visiteur	
II.4. Accès aux zones sensibles		
Responsable de la sécurité physique/Responsable de site	– Autoriser l'accès au prestataire, auditeur – Attribuer un badge auditeur numéroté. – rappeler les consignes de sécurité (interdiction d'accès aux zones sensibles, usage du téléphone limité, confidentialité – Accompagner le visiteur	

Acteurs	Descriptions des tâches	Documents et interfaces
Prestataire/ auditeur	– S'enregistrer dans le registre d'accès o Nom et prénom o Entreprise o Motif de l'accès o Date et heure d'accès.	Registre des visiteurs.
II.5.	**Départ du visiteur**	
Visiteur	– Passer par la réception. – Restituer le badge visiteur à l'Agent de sécurité	Registre des visiteurs.
Agent de sécurité	– Inscrire l'heure de sortie dans le registre. – Vérifier que le visiteur n'a laissé aucun document ou matériel non autorisé	Registre des visiteurs
II.6.	**Révocation et mise à jour des accès**	
Responsable de la Direction ou service demandeur de la prestation	– Informer le Responsable de la sécurité physique de la fin des travaux	mail
Responsable de la Sécurité Physique	– procéder à la désactivation des exceptions accordées au partenaire, auditeur	Système de gestion des badges

Annexes / Enregistrements

- Fiche de demande d'accès physique
- Registre des visiteurs
- Système de gestion des badges
- Politique de gestion des badges
- Badge visiteur
- Mail

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 DES SYSTEMES D'INFORMATION	Validé par : COMITE PROCEDURES	Approuvé par : DIRECTION GENERALE
Date : 05/11/2025	Date : 05/11/2025	Date :
Signature :	Signature :	Signature :