La présente charte s'applique à l'ensemble des Administrateurs du Système d'Information de Commercial Bank - Cameroun

# Charte des Administrateurs du système d'information

**Référence : CHA-GSI-RSSI-261-V01**

## TEXTES DE LOIS ET REGLEMENTS, DOCUMENTS ET INSTRUCTIONS DE TRAVAIL

- Politique de Sécurité du Système d'Information de la CBC ;
- Norme ISO/IEC 27001 ;
- Procédure de Gestion des Documents et Enregistrements ;
- Règlement COBAC LC-COB/04 du 21 janvier 2022 sur le renforcement du dispositif de maitrise des risques informatiques ;
- Règlement COBAC R-04/2016 du 16 avril 2016 portant sur le contrôle interne dans les établissements de crédit et les holdings financières ;
- Payment Card Industry (PCI) Data Security Standard (DSS) 3.2.1.

## OBJET

Le présent document présente les règles de bonne conduite et obligations que chaque administrateur ou personnel ayant des droits administrateurs sur des actifs informatiques doit respecter lors de leurs utilisations afin de contribuer à minimiser les risques auxquels pourrait être exposé le Système d'Information de la Commercial Bank-Cameroun.

## DOMAINE D'APPLICATION

La présente charte s'applique à l'ensemble des administrateurs du Système d'Information de Commercial Bank - Cameroun

## INDICATEURS DE QUALITE

Nombre d'administrateurs n'ayant pas signé de lettre d'engagement : zéro.

## CLASSIFICATION

☐ **Confidentiel** ☒ **Restreint** ☐ **Interne** ☐ **Public**

## TABLE DES MATIERES

# 1 GENERALITES

## 1.1 Rôles et responsabilités

| ACTEURS | RESPONSABILITES |
|---|---|
| **RSSI** | Revue et mise à jour du document |
| **Administrateur actif du SI** | Respect des règles de sécurité évoquées dans le document |

## 1.2 Définitions

- DPC (Données de porteurs de cartes) : il s'agit des informations stockées sur la carte bancaire, classées en 2 catégories :
  - CHD (Card Holder Data) :
    - PAN (Numéro de compte) ;
    - Nom du titulaire de la carte ;
    - Code service ;
    - Date d'expiration de la carte.
  - SAD (Sensitive Authentication Data) :
    - Données de pistes magnétiques ;
    - Cryptogramme visuel ;
    - Code/Bloc PIN.
- CDE (Card holder Data Environment): ensemble des individus, processus et technologies du système d'informations de Commercial Bank - Cameroun, capable de traiter, stocker et/ou transmettre les DPC.
- Périmètre PCI-DSS : le périmètre regroupe le CDE et l'ensemble des composants du système d'informations de Commercial Bank - Cameroun, susceptibles d'impacter la sécurité du CDE.

## 1.3 Acteurs concernés

- **Administrateur** d'un système ou d'un réseau de la Commercial Bank - Cameroun : toute personne, employée ou non, à laquelle a été confiée explicitement et par écrit, sous la forme d'une lettre de mission, d'un profil de poste annexé au contrat de travail ou d'un contrat de prestations de service, la responsabilité d'un système informatique, d'un réseau ou d'un sous-réseau administré par une entité de la Commercial Bank - Cameroun.

- Une personne à qui a été conférée une telle responsabilité sera désignée dans la suite de ce document par le terme administrateur. L'ensemble des éléments sur lesquels s'exerce cette responsabilité constitue le périmètre d'activité de l'administrateur.

❖ **Comité de coordination de sécurité du système d'information (SSI)** : constitué de responsables chargés de :

- Émettre des règles et des recommandations dans le domaine SSI,
- Prendre les mesures appropriées pour qu'elles soient mises en vigueur,
- Organiser les activités de formation, d'information et de sensibilisation de nature à améliorer les conditions de leur application.
- Les membres de ce comité de coordination sont le RSSI de la Commercial Bank - Cameroun, le Directeur de la Transformation Digitale et du Système d'Information (DTDSI) de la Commercial Bank - Cameroun, et d'autres personnes désignées par la Direction Générale.

Les devoirs, les pouvoirs et les droits de l'administrateur, définis dans la présente Charte, constituent ensemble les responsabilités de sécurité du SI de l'administrateur. Les consignes du Comité de Coordination du SSI s'imposent aux administrateurs des composants du Système d'Information pour l'exercice de leurs responsabilités SSI dans leur périmètre d'activité.

## 2 OBLIGATIONS

### 2.1 Surveillance et audit

Le Comité de coordination SSI organise la surveillance et l'audit de toutes les activités des systèmes et de tous les trafics réseau sur les infrastructures administrées par la Commercial Bank - Cameroun.

Pour ce faire, le Comité de coordination SSI est habilité à donner des consignes de surveillance, de recueil d'information et d'audit aux administrateurs concernés.

### 2.2 Contrôle d'accès

Le Comité de coordination SSI définit des règles de contrôle d'accès aux systèmes et aux réseaux conformes à la présente Charte et à la Charte de l'utilisateur des ressources informatiques de la Commercial Bank - Cameroun.

### 2.3 Vérifications

Le Comité de coordination SSI et les administrateurs concernés sont habilités à entreprendre toute action appropriée pour vérifier la bonne application des règles de contrôle d'accès aux systèmes et aux réseaux définies à l'article précédent, ainsi que pour détecter leurs vulnérabilités.

### 2.4 Enregistrement des incidents de sécurité

L'administrateur conserve une trace écrite des incidents de sécurité survenus dans son périmètre d'activité. Cette trace doit comporter les indications de date et d'heure des événements considérés, et une description de ces événements.

### 2.5 Journalisation et archivage

L'administrateur active sur les systèmes dont il a la responsabilité les journaux nécessaires à l'identification et à la reconstitution des séquences d'événements qui pourraient constituer un incident de sécurité, ou qui pourraient faire l'objet d'une commission rogatoire émise par les autorités judiciaires. Il archive les données ainsi recueillies dans des conditions propres à en assurer l'intégrité, la disponibilité, l'authenticité et la confidentialité.

Il mène cette activité de journalisation et d'archivage dans des conditions qui garantissent le respect des lois et des règlements relatifs aux libertés publiques et privées, au secret des correspondances, au droit d'accès à l'information, et il veille notamment à détruire tous les journaux qui comportent des données nominatives à l'expiration d'un délai qui ne peut excéder un an, ou le délai légal à la date considérée.

### 2.6 Examen des journaux

L'administrateur examine régulièrement les journaux mentionnés à l'article ci-dessus.

### 2.7 Dérogations aux règles SSI

Les règles SSI mentionnées dans la présente Charte, dans la Charte des utilisateur du SI de la Commercial Bank - Cameroun, ou édictées par le RSSI, au sein de la Direction de la Transformation Digitale et du Système d'Information ou par le Comité de coordination SSI s'imposent à tous les utilisateurs du Système d'Information du Commercial Bank - Cameroun, qu'ils soient ou non des employés de Commercial Bank - Cameroun.

Les administrateurs de systèmes et de réseaux ont pour mission de les mettre en œuvre et de les faire respecter dans leur périmètre d'activité.

Les responsables d'entités qui voudraient passer outre ces règles SSI, ou entreprendre des actions qui dérogeraient à ces règles, doivent remettre à l'administrateur responsable des infrastructures concernées un document écrit et signé par lequel il assume explicitement la responsabilité de cette dérogation, des risques qui en découlent, et de leurs conséquences.

Les utilisateurs qui ne seraient pas responsables d'entités et qui voudraient bénéficier de telles dérogations doivent obtenir qu'elles soient endossées par leur responsable d'entité, dans les conditions indiquées à l'alinéa précédent.

Identification des utilisateurs et contrôles d'accès dans leur périmètre d'activité, les administrateurs responsables sont seules habilités à mettre en place et à administrer les systèmes d'identification et d'authentification des utilisateurs conformes aux directives du comité de coordination SSI. Il en va de même pour les dispositifs de contrôle d'accès aux systèmes, aux réseaux et aux données.

Sauf exception formulée par un document écrit signé d'un responsable d'entité, seuls l'administrateur local et ses collaborateurs immédiats possèdent les droits d'administrateur sur les postes de travail des utilisateurs des SI de la Commercial Bank - Cameroun.

### 2.8 Audits périodiques

Les administrateurs procèdent deux fois par an à un audit des comptes des utilisateurs et des droits d'accès associés, pour vérifier leur validité et leur exactitude.

### 2.9 Mise en œuvre et litiges

Rapport des violations des règles SSI Pour toute violation des règles SSI qu'il est amené à constater, l'administrateur établit un rapport écrit destiné au Comité de coordination SSI et à ses responsables hiérarchiques.

### 2.10 Veille SSI

Les Administrateurs exercent régulièrement une activité de veille scientifique et technologique dans le domaine SSI. Ils sont abonnés aux listes de diffusion qui publient les découvertes de vulnérabilités. Ils participent notamment aux activités de formation, d'information et de sensibilisation entreprises par le Comité de coordination SSI.

### 2.11 Attitude à l'égard des violations des règles SSI

La Direction Générale de la Commercial Bank - Cameroun, ou son représentant qualifié, peut révoquer le compte et les droits d'accès au réseau et aux données d'un utilisateur qui aurait violé les règles SSI mentionnées dans la Charte des utilisateurs du SI de la Banque.

### 2.12 Obligations particulières

- Respecter ses engagements de confidentialité ;
- Éviter d'isoler, arrêter ou reconfigurer des équipements ou applications informatiques pouvant compromettre la sécurité du Système d'Information dans son ensemble, sauf en cas d'autorisation formelle ;
- N'utiliser le compte administrateur que pour les activités et besoins directement liés aux tâches d'administrations ou d'exploitation ;
- Configurer et utiliser uniquement des comptes nominatifs pour accéder aux systèmes qu'il administre et se connecter sur le compte administrateur par défaut des systèmes d'exploitation qu'à partir de la session de son compte nominatif ;

- S'assurer de la protection logique et physique des postes de travail à partir desquels il exerce sa fonction (mot de passe robuste, verrouillage de session, laisser son poste sans surveillance…) ;
- Changer régulièrement ses mots de passe d'accès au système d'information de la banque conformément aux politiques de sécurité ;
- Informer le RSSI de tout incident de sécurité ou risque élevé dans le respect de la procédure de gestion des incidents de sécurité ;
- Utiliser des logiciels approuvés et acquis sous licence d'utilisation par la banque ;
- Préserver les traces nécessaires à la résolution d'un incident et à toute investigation ultérieure dans le respect de la politique de sécurité.

## 3 ACTIONS PROSCRITES

- Les Administrateurs ne doivent accéder aux données du Système d'Information que dans un cadre strictement professionnel ;
- Il ne doit pas communiquer :
  - Les configurations des systèmes administrés à des tiers ou à des collaborateurs non habilités ;
  - Ses droits d'accès (identifiants et mots de passe) à un autre administrateur, utilisateur, ou tiers ;
  - Un mot de passe d'usage par courrier électronique ; utiliser un autre canal : SMS, WhatsApp, etc….
- Il ne doit pas utiliser :
  - L'accès d'un autre administrateur,
  - Un poste de travail personnel pour accéder à des plateformes ou données de la banque ;
- Il ne doit pas contourner les mesures de sécurité ou les procédures en vigueur ;
- Il ne doit pas utiliser les droits privilégiés à des fins personnelles ;
- Il ne doit pas créer des comptes dotés de privilèges sans respecter la procédure de gestion des habilitations de la banque ;
- Il ne doit pas extraire les données d'un système d'information sans autorisation du (ou des) responsable(s) de ces données ;
- Il ne doit pas copier des données de la banque sur un support amovible sans autorisation formelle du (ou des) responsable(s) de ces données ;
- Il ne doit pas désactiver les fonctions de journalisation ou effacer les journaux générés par les systèmes d'information dont il a la charge ;
- Il ne doit pas procéder à des tests d'intrusion sur le réseau de la banque sans autorisation ;

- Il ne doit pas prendre des consignes venant d'une personne non identifiée et doit se référer à son responsable hiérarchique pour toute requête lui paraissant inappropriée ;
- Il ne doit pas se connecter à un poste de travail d'un utilisateur sans son autorisation, notamment dans le cas de l'utilisation d'un logiciel de prise en main à distance (bureau à distance).

## 4 APPLICATION ET SUIVI DOCUMENT

### 4.1 Date d'application

La présente charte a été soumise pour avis à la Direction Générale et adoptée le……..

Cette charte administrateur entre en vigueur dès le premier accès aux ressources informatiques et aux services réseaux, Internet/Intranet de la Commercial Bank-Cameroun, et/ou la première utilisation de matériels informatiques ou de logiciels appartenant à la Commercial Bank-Cameroun Les administrateurs du SI s'engagent à respecter les dispositions de la charte en signant un exemplaire de celle-ci.

Pour tout renseignement complémentaire, vous pouvez vous adresser au RSSI.

La signature de cette charte est obligatoire pour tous les administrateurs du SI identifiés de la Commercial Bank-Cameroun.

### 4.2 Mise à jour du document

La Direction Générale de la Commercial Bank-Cameroun se réserve le droit de changer à tout moment la présente charte.

Aucun changement, même mineur, entraînant une diminution de vos droits ne pourra avoir lieu sans votre consentement exprès.

Les changements seront signalés (notamment, pour certains services par le biais d'une notification par courrier électronique), chaque version de cette charte sera identifiée en haut de page par sa date d'entrée en vigueur.

## 5 ANNEXE : LETTRE D'ENGAGEMENT D'UN ADMINISTRATEUR

Je, soussigné_____

Matricule_____, occupant la fonction de _____

déclare avoir pris connaissance du contenu de la charte de sécurité des administrateurs et m'engage à respecter les principes y définis. Je suis également conscient (e) que le non-respect des engagements contenus dans la présente charte peut impliquer d'éventuelles mesures disciplinaires allant jusqu'aux poursuites judiciaires.

Entité : _____

Direction/Département : _____

**Signature de l'administrateur**

*(Précéder de la mention manuscrite "Lu et approuvé").*

Nombre total de pages de la présente charte : **10**

Fait à :_____, le : _____

***NB : Veuillez retourner l'original de cette lettre signée et datée à la Sous-Direction Développement du Personnel et la copie à la Sous-Direction Sécurité des Systèmes d'Information***