POLITIQUE D'INFORMATION ET DE CYBERSÉCURITÉ

Le Conseil d'Administration et la Direction de FirstBank DRC, située au 191 avenue de l'Équateur, Kinshasa Gombe, opérant dans le secteur financier, s'engagent à préserver la confidentialité, l'intégrité et la disponibilité de tous les actifs informationnels physiques et électroniques au sein de l'organisation. Cet engagement vise à protéger l'avantage concurrentiel, les actifs, la rentabilité, ainsi que la conformité légale, réglementaire et contractuelle, tout en préservant l'image commerciale de la banque.

Les exigences en matière de cybersécurité et de sécurité de l'information continueront d'être alignées sur les objectifs stratégiques de l'organisation. Le Système de Gestion de la Sécurité de l'Information (SMSI) a pour vocation de faciliter le partage d'information, les opérations électroniques, le commerce en ligne, et de réduire les risques liés à la cybersécurité à un niveau acceptable.

Le SMSI de FirstBank DRC est conforme aux normes suivantes :

- ISO 27001 – Norme internationale de sécurité de l'information
- PCI DSS – Norme de sécurité des données pour l'industrie des cartes de paiement
- Exigences légales et réglementaires en vigueur

Gestion des Risques de Sécurité d'informations et de Cybersécurité

La stratégie actuelle de FirstBank DRC ainsi que son cadre de gestion des risques liés à la sécurité de l'information et à la cybersécurité permettent d'identifier, évaluer et contrôler les risques grâce à l'établissement et à la maintenance du SMSI.

- L'évaluation des risques, la déclaration d'applicabilité et le plan de traitement des risques déterminent la manière dont ces risques sont gérés.
- Le Directeur des Risques est responsable de la gestion et de la mise à jour du plan de traitement des risques.
- Si nécessaire, des évaluations de risques supplémentaires pourront être effectuées afin de déterminer les mesures de contrôle adaptées aux risques spécifiques.

Principes Fondamentaux de la Sécurité de l'Information

FirstBank DRC met en place des mesures clés pour assurer une cybersécurité robuste :

- Plans de continuité d'activités et de gestion des crises
- Sauvegarde et protection des données
- Prévention contre les virus et attaques de pirates informatiques
- Contrôle d'accès aux systèmes et aux informations

- Gestion des incidents de cybersécurité

Tous les employés de FirstBank DRC ont la responsabilité de signaler toute violation de sécurité.

Respect des Règles de Cybersécurité

Tous les employés et certaines parties externes identifiées dans le SMSI sont tenus de se conformer à cette politique et aux procédures mises en place.

- Des formations spécifiques seront dispensées aux employés et aux parties externes concernées afin d'assurer le respect des normes en vigueur.

Amélioration Continue et Gouvernance

- FirstBank DRC mettra régulièrement à jour ses politiques et pratiques de gestion des risques en cybersécurité pour s'aligner aux normes du secteur et aux nouvelles menaces émergentes.
- Une communication transparente sera maintenue avec le Conseil d'Administration sur les risques liés aux technologies et à la cybersécurité, afin de garantir des décisions stratégiques alignées avec les priorités de l'entreprise.
- Le SMSI fera l'objet d'un examen continu et d'améliorations, si nécessaire.

Responsabilités et Comité de Sécurité

FirstBank DRC a mis en place des comités de gestion des risques, composés de membres issus de différents départements de la banque.

Principaux Responsables :

- Le Responsable de la Sécurité des Systèmes d'Information est chargé de la mise en œuvre et du suivi du programme et de la stratégie de cybersécurité de la banque. Il est également responsable de la réduction des risques liés à la cybersécurité.
- Le Directeur National de la Gestion des Risques a la responsabilité ultime du respect des normes PCI DSS et ISO 27001.
- Le Directeur National de la Gestion des Risques est également responsable de l'actualisation et de la validation annuelle de cette politique par le Conseil d'Administration, notamment en cas de modifications importantes ou d'incidents critiques.

Une version à jour de ce document est disponible pour tous les employés sur l'intranet de l'entreprise.