Politique de Sécurité de l'Information (Version abrégée)

UBA Congo Brazzaville s'engage à garantir la sécurité de ses informations et de ses actifs informationnels, et a mis en place un Système de Management de la Sécurité de l'Information (SMSI) conforme à la norme **ISO/IEC 27001:2022**. Le SMSI aide UBA à protéger ses données et ses actifs informationnels.

La haute direction de la banque témoigne de son engagement envers la sécurité de l'information en établissant des objectifs et politiques de sécurité de l'information, et en fournissant les ressources nécessaires pour maintenir et améliorer continuellement la sécurité de l'information dans la banque.

La banque veille au respect de toutes les réglementations, normes et obligations contractuelles applicables en matière de sécurité de l'information.

Déclaration de politique de sécurité de l'information

- Le Conseil d'Administration et la Direction de **United Bank for Africa Congo** s'engagent à préserver la **confidentialité**, l'**intégrité** et la **disponibilité** de tous les actifs informationnels physiques et électroniques (données, ressources) de la Banque, afin de maintenir son avantage concurrentiel, sa trésorerie, sa rentabilité, sa conformité légale, réglementaire et contractuelle, ainsi que son image institutionnelle.
- Cet engagement se concrétisera par la mise en place, le fonctionnement, la révision systématique et l'amélioration continue d'une **politique de gestion de la sécurité de l'information** garantissant que les exigences de sécurité de l'information restent alignées sur les objectifs stratégiques de la Banque, tout en facilitant le partage d'informations, la communication électronique, les services bancaires/commerce en ligne, les médias sociaux, et en réduisant les risques liés à l'information à des niveaux acceptables.
- Le plan stratégique de l'entreprise et le cadre de gestion des risques de la Banque serviront en tout temps de contexte pour **l'identification, l'évaluation et le traitement des risques liés à l'information**, ainsi que pour la sélection des objectifs de contrôle et la mise en œuvre des mesures de sécurité appropriées.
- En particulier, des **plans de continuité d'activité et de secours**, des **procédures de sauvegarde et de restauration des données**, le **contrôle contre les logiciels malveillants et les intrusions**, le **contrôle d'accès aux systèmes**, et le **signalement et la gestion des incidents de sécurité de l'information** sont fondamentaux dans cette politique de sécurité. Les objectifs de contrôle pour chacun de ces domaines sont détaillés dans le **Manuel de Sécurité de l'Information** et seront appuyés par des politiques et procédures documentées spécifiques.
- Le **Management de la Sécurité de l'Information** est responsable de la gestion et du maintien du plan de traitement des risques liés à la sécurité de l'information. Le **Comité de Pilotage IT & Cybersécurité** et le **Comité de Gestion des Risques** soutiennent la mise en œuvre, le fonctionnement et la maintenance du cadre du SMSI, et procèdent à des revues périodiques de la politique de sécurité.

- **Tous les employés**, le personnel contractuel engagé, et les **prestataires tiers** de la Banque sont tenus de respecter cette politique de sécurité. Une **formation, une sensibilisation et une éducation** appropriées leur seront fournies à cette fin.
- La politique de sécurité de l'information fera l'objet d'une **révision systématique et continue**. La Banque s'engage à **se conformer et à obtenir la certification ISO/IEC 27001:2022**, norme internationalement reconnue pour les systèmes de management de la sécurité de l'information.
- La politique de sécurité de l'information sera revue **au moins une fois par an**, ou en réponse à tout changement majeur dans les évaluations ou les plans de traitement des risques.
- Le **Conseil d'Administration** est propriétaire de cette politique de sécurité et est responsable de sa revue, conformément aux exigences du **Manuel de Sécurité de l'Information**.
- Cette politique a été **approuvée par le Conseil d'Administration** et est publiée sous **contrôle de version**, **signée par le Président du Conseil**.

Objectifs de sécurité de l'information et de protection des données

- Assurer une **gestion efficace de la sécurité de l'information et de la protection des données personnelles** au sein de la Banque, via un cadre de gouvernance adapté.
- Obtenir le soutien de la Direction pour la sécurité de l'information et la protection des données, via l'**attribution de rôles**, la **coordination** et la **revue de la mise en œuvre des politiques** de sécurité, ainsi que la **présentation des politiques au Conseil d'Administration**, via le **Comité de Gestion des Risques**.
- Développer des relations avec des **experts externes en cybersécurité**, des **autorités compétentes** et d'autres groupes pertinents pour **rester informé des tendances**, surveiller les normes et méthodes d'évaluation, et garantir des points de contact efficaces pour la gestion des incidents.
- Encourager une approche **pluridisciplinaire** en matière de cybersécurité et de protection des données.
- Maintenir la **sécurité des données personnelles**, des **informations** et des **installations de traitement de l'information** qui sont **accédées, traitées, communiquées ou gérées par des parties externes**.
- Veiller à ce que **l'introduction de produits ou services externes** ne compromette pas la sécurité des données personnelles et des informations de la Banque.
- Contrôler **l'accès aux données personnelles**, aux **installations de traitement de l'information**, et à la **communication d'informations** par des tiers.
- **Évaluer les interactions** commerciales avec les tiers qui impliquent l'accès ou l'échange de données personnelles ou d'informations critiques afin de **déterminer les risques de sécurité et les exigences de contrôle** appropriées.