ALGERIAN UNION BANK بنك الاتحاد الجزائري — ثقة LA CONFIANCE SANS FRONTIÈRES	REFERENCE DE LA PROCEDURE	DATE DE CREATION	Version
	Politique N° 01 /2023	14/11/2023	01

Sécurité des Systèmes d'Information

Politique Générale de Sécurité de l'Information

Diffusion Générale

Signature

Date d'entrée en vigueur : 14/11/2023

Algerian Union Bank ☆ Direction Générale ☆ AUB

ALIANE Merouane
Directeur Général

Algerian Union Bank, SA au Capital Social de 1 850 000 000 MRU
Siège social : Lot n°80 de l'Ilot HMS - BP N°8581, Tevragh Zeina, Nouakchott, Mauritanie
RC N° 3909 / 119863, Agrément N° 16
NIF : 01323633

MS AB

Glossaire

Abréviations

AUB	Algerian Union Bank
GED	Gestion Electronique des Documents.
SMSI	Système de Management de la Sécurité de l'Information.
GEC	Gestion électronique des courriers
SSSI	Structure Sécurité des Systèmes d'Information.
ERP	Enterprise Ressource Planning (Progiciel de Gestion Intégré).
VLAN	Virtual Local Area Network (Réseau Local Virtuel).
VoIP	Voice Over Internet Protocol (Voix sur le Protocol Internet).

Sommaire

Algerian Union Bank Direction Générale AUB

I. Objet

Le présent texte a pour objet de décrire la Politique Générale de Sécurité de l'Information de la Banque.

II. Présentation et Contexte

Nul doute que l'information, quels que soient sa forme, son support, sa présentation, et les systèmes permettant son traitement, son stockage, son partage et sa communication, sont des actifs que AUB doit protéger contre les non-conformités, les usages frauduleux, les modifications incontrôlées et abusives, les divulgations de ses secrets confidentiels, car il y va de sa survie.

AUB, de par son activité de banque, est soumise à un cadre légal et règlementaire strict régissant son activité. Elle est, aussi, soumise à d'autres textes régissant la sécurité de l'information auxquels elle doit se conformer autant que la présente politique de sécurité de l'information.

AUB est, aussi, soumise, de par la concurrence, à être performante dans la réalisation de ses activités pour demeurer compétitive et gagner davantage en parts de marché.

A cet effet, la Direction Générale de la banque a émis des orientations stratégiques choisies et décidées pour la mise en ligne de toutes les informations aux ayants droits pour qu'elles soient accessibles sans délais.

Ainsi, il est prévu que :

- Tous les documents sont gérés par un système de gestion électronique des documents qui permet de numériser les dossiers depuis leur création et jusqu'à la fin de leur cycle de vie, en passant par les archives, avec une procédure pour le classement approprié des documents contractuels et la gestion des archives.
- Tous les systèmes d'information exploités par AUB, qu'ils soient techniques, financiers ou de contrôle de gestion, sont accessibles moyennant les contrôles d'accès adéquats et mis à la disposition des acteurs concernés afin de leur permettre de piloter leurs activités et gagner, ainsi, en productivité.
- AUB doit être dotée d'un outil qui permet la gestion électronique des courriers. Cet outil permet l'échange sécurisé de tous les courriers au sein de la banque toute en automatisant les Workflow qui en découlent.
- La banque doit mettre en place un moteur de Workflow (BPM) afin d'automatiser l'ensemble des Workflow extra le Core Banking System.
- AUB met en place un outil de Reporting (BI) de l'ensemble de l'activité de la Banque.

Pour intégrer toutes les modifications de l'environnement de fonctionnement dans son

Algerian Union Bank, SA au Capital Social de 1 850 000 000 MRU
Siège social : Lot n°80 de l'Ilot HMS - BP N°8581, Tevragh Zeina, Nouakchott, Mauritanie
RC N° 3909 / 119863, Agrément N° 16
NIF : 01323633

Algerian Union Bank Direction Générale AUB

MS

système de management de la sécurité de l'information, la Banque doit élaborer, mettre en œuvre, faire fonctionner, surveiller et améliorer, continuellement, la Sécurité de l'Information, afin de contenir et maitriser les risques encourus à un niveau de risque acceptable.

III. Introduction

La Politique de Sécurité de l'Information est considérée comme la concrétisation de l'engagement de la Direction Générale de la banque à apporter à la sécurité de l'information, une orientation et une vision stratégique conformément aux exigences métiers et aux dispositions législatives, règlementaires et contractuelles.

Le présent texte est un document de haut niveau, qui doit résister le plus longtemps aux changements de l'environnement, traduisant l'ensemble des principes, des objectifs et des exigences métier en matière de protection de l'information (manipulation, traitement, stockage, communication et archivage) nécessaire à son activité.

Cette présente Politique n'est pas unique, elle est complétée par d'autres procédures de gestion (manuels) concernant les politiques connexes ou spécifiques d'usage et les chartes, qui sont définies, par type d'utilisation ou domaine ou par type d'utilisateurs, et parfois accompagnées par des procédures opérationnelles, qui peuvent faire l'objet de modifications plus récurrentes en fonction des changements de l'environnement d'application.

L'ensemble des procédures (manuels) connexes fournissent les lignes directrices relatives aux contrôles de sécurité spécifiques détaillés de la Banque, qui permettent de guider tous les acteurs internes ou externes, dans leur comportement quotidien vis-à-vis de la sécurité de l'information.

L'ensemble des procédures relatives aux politiques connexes doivent être, périodiquement, revues au besoin pour la prise en compte des changements opérés dans l'environnement touchant à la sécurité de l'information.

IV. Objectifs

Les objectifs de la sécurité de l'information sont multiples et concourent à ce que les risques liés à la sécurité de l'information soient compris et traités, pour être acceptables, en symbiose avec la stratégie de la Banque.

La politique de sécurité de l'information vise à promouvoir une culture de sécurité de l'information, et ce, afin de :

- Contribuer au maintien et au développement de l'image de marque de la Banque par la maîtrise des risques, notamment ceux liés à la sécurité de l'information, l'application des bonnes méthodes et l'utilisation des bonnes pratiques, en disposant d'une Politique en la matière.

Algerian Union Bank, SA au Capital Social de 1 850 000 000 MRU
Siège social : Lot n°80 de l'Ilot HMS - BP N°8581, Tevragh Zeina, Nouakchott, Mauritanie
RC N° 3909 / 119863, Agrément N° 16
NIF : 01323633

Algerian Union Bank Direction Générale AUB

- Rester, toujours, en conformité aux dispositions des textes législatifs et à la réglementation en vigueur, mais aussi à l'état de l'art (définir, mettre en œuvre, documenter, déployer, contrôler, mettre à jour d'une manière continue) et l'approche pour les satisfaire.
- Protéger le patrimoine informationnel tout entier : données et informations, processus de traitement, de stockage, de transmission, d'archivage et de fin de vie, savoir-faire et droits d'auteur (tout est inclus dans l'axe de prévention dans une vision stratégique).
- Protéger les données à caractère personnel, notamment celles relatives aux clients (sensibilisation aux exigences réglementaires, formation sur l'application des règles, développement des moyens de protections préventifs, établissement des responsabilités des personnes traitant ce type de données).
- Appliquer une approche systémique et globale de sécurisation de l'information (organisationnelle, physique et environnementale, juridique et technique).
- Maîtriser les risques (classification des actifs, analyse des risques, maturité de l'organisme vis-à-vis des mesures et contrôles normalisés, gestion des incidents, confidentialité et confiance en l'intégrité de l'information sont suffisamment assurées, disponibilité de l'information conforme aux exigences métier).
- Maîtriser les applications informatiques et leur exploitation en disposant d'une documentation de toutes les phases (documentation existante depuis la conception, le développement ou l'acquisition, les tests de conformité aux besoins et d'acceptation, l'exploitation, la gestion des changements) et d'enregistrement de tous les évènements, (administration, sauvegardes et leurs supports, incidents d'exploitation, Backups,...).
- Maîtriser les accès physiques (aux bureaux, aux lieux où se trouvent les moyens d'utilisation et d'accès à l'information, aux sites d'hébergement des applicatifs et des bases de données).
- Participer à lutter contre la malveillance (habilitations précises, contrôle d'accès et utilisations avec des méthodes et des outils adéquats, gestion proactive des incidents, analyse des évènements, investigation) et contre la cybercriminalité.
- Assurer la disponibilité de l'information (mesures adéquates pour la continuité du service informatique : secours électriques, environnement climatique adéquat, maintenances évolutives et correctives, sauvegardes, plan de reprise, tests réguliers de reprise), et pour les informations nécessitant une disponibilité quasi-permanente (sites backup, réplication des données, plan de continuité d'activité).
- Maîtriser la documentation et le système GED, et les enregistrements (définir, documenter, mettre à jour).

Algerian Union Bank Direction Générale

Algerian Union Bank, SA au Capital Social de 1 850 000 000 MRU
Siège social : Lot n°80 de l'Ilot HMS - BP N°8581, Tevragh Zeina, Nouakchott, Mauritanie
RC N° 3909 / 119863, Agrément N° 16
NIF : 01323633

V. Domaine d'application

La politique de sécurité de l'information est déclinée de la stratégie et de la politique générale de la Banque.

Elle couvre tous les actifs d'information de la Banque, tels que présentés en Annexe N°01. Parmi ces actifs, certains sont sensibles, critiques voire vitaux au fonctionnement de l'AUB.

C'est pourquoi, il est nécessaire d'inventorier et de classifier tous les actifs de la Banque afin d'en identifier le degré de sensibilité par rapport aux critères fondamentaux de la sécurité, à savoir la confidentialité, l'intégrité et la disponibilité et leur appliquer la présente politique de sécurité.

La politique de sécurité de l'information s'applique à l'ensemble du personnel de la Banque, ainsi qu'au personnel de ses partenaires et de ses contractants.

VI. Principes fondateurs de la sécurité de l'information de la Banque

La politique de sécurité de l'information a un rôle de correction, en premier lieu, par l'adoption des recommandations du haut niveau, en s'appuyant sur les normes internationales de sécurité de l'information, puis de prévention selon le principe de l'amélioration continue pour préserver les actifs informationnels de tout risque et danger qui peut naître lors de la réalisation des différentes activités de la Banque.

La politique de sécurité de l'information est l'une des premières actions à mettre en œuvre dans la gestion de la sécurité de l'information.

La politique de sécurité de l'information comprend un ensemble de principes d'ordre juridique, organisationnel, technique et physique à caractère prioritaire. Elle est basée sur les principes suivants qui doivent être respectés :

1. Sécurité bien comprise

Le personnel de la Banque est régulièrement sensibilisé et formé aux aspects de la sécurité de l'information, ainsi qu'aux consignes de base relatives à l'utilisation des systèmes d'information de la Banque, énoncées dans la Charte de bonne conduite en matière de sécurité de l'information numérique.

2. Respect des normes et des bonnes pratiques

La politique de sécurité de l'information de la Banque est inspirée des normes standards et des bonnes pratiques internationalement reconnues et approuvées dans le domaine de la sécurité de l'information, notamment les normes de la série ISO/IEC 27000.

3. Approche basée sur le risque

Les mesures de sécurité de l'information sont sélectionnées en fonction d'une analyse de risque effectuée selon une méthode confirmée, de façon à minimiser les risques et à

maintenir les coûts de sécurité à un niveau acceptable.

La Banque cherche à réduire les risques selon le principe de la proportionnalité et de la nécessité, mais se réserve le droit d'assumer les risques résiduels.

En fonction de l'évaluation des risques et du niveau de résilience visé, un ensemble de mesures de prévention, de détection, de réponse et de récupération est mis en œuvre.

4. Ressources

AUB veille à consacrer à la sécurité de l'information, les moyens humains et financiers adaptés en fonction de la situation de risque spécifique.

5. Développement continu vers l'excellence

L'environnement de gestion de l'information de la Banque change continuellement.
Il convient d'adopter une approche itérative et une amélioration continue pour rester en phase avec les défis actuels et futurs.

6. Sécurité intégrée et transversale

La sécurité de l'information n'est pas une fin en soi, mais elle fait partie intégrante de toute activité de la Banque, de la conception à la maintenance en passant par la spécification, l'implémentation, le déploiement et la mise en service.

Selon le principe de « Security by design », elle est la pierre angulaire de la gestion de tous les projets, processus et activités quotidiennes.

Lors de la conception de systèmes traitant des données à caractère personnel, les principes de « Protection des données dès la conception » et « Protection des données par défaut » sont prises en charges.

7. Communication et collaboration

La politique de sécurité de l'information de la Banque, la Charte de Sécurité en matière de sécurité de l'information ainsi que les lignes directrices et circulaires relatives à la sécurité de l'information sont systématiquement communiquées à l'ensemble du personnel de la Banque.

La sécurité de l'information est l'affaire de tous. Les structures et l'ensemble des collaborateurs sont appelés à contribuer activement, à assurer la sécurité de l'information de la banque et à s'entraider mutuellement dans la réalisation des objectifs de sécurité de l'information.

8. Respect et traçabilité

Le personnel interne et externe doit connaître les règles émanant de la politique de sécurité de l'information de la Banque, reconnait l'importance de la sécurité de l'information et respecte les exigences de cette politique.

Algerian Union Bank Direction Générale

9. Culture de sécurité de l'information

La présente politique établit un point de départ pour une gestion appropriée de la sécurité de l'information. La Banque compte sur la coopération active de l'ensemble du personnel afin d'assurer un environnement de travail sécurisé.

La politique de sécurité de l'information contribue, ainsi, à instaurer progressivement une véritable culture de la sécurité de l'information.

10. Révision

La politique de sécurité de l'information de l'AUB est revue, en cas de changements législatifs, organisationnels, technologiques, respectivement sur la base de l'évolution de la situation des menaces et des risques.

VII. Responsabilités

La Politique de Sécurité de l'Information s'inscrit, dans le cadre de la stratégie et des directives émanant des lois publiées par l'état Mauritanien, visant l'adoption des bonnes pratiques de la gouvernance de la sécurité de l'information.

VIII. Principaux résultats attendus

La mise en place d'une culture de sécurité de l'information dans les habitudes de gestion et opérations de réalisation des activités de la Banque contribue à minimiser les risques d'indisponibilité, d'altération ou d'utilisation abusive ou frauduleuse de l'information.

Les principaux résultats attendus se résument comme suit :

- La préservation et le renforcement de l'image et de la crédibilité de la Banque ;
- La Protection du patrimoine informationnel, indispensable à la réalisation des activités, est pleinement ancrée dans les processus de fonctionnement d'AUB ;
- La minimisation de l'impact des incidents de sécurité de l'information sur les services et les activités de la Banque.
- Les pertes dues aux fraudes, aux vols et aux mauvaises manipulations seront connues et minimisées par le système de traces mis en place.

IX. Contrôle de la politique de la sécurité de l'information

Les intervenants dans les processus de traitement de la politique générale de sécurité de l'information mis en place par la Banque, à tous les niveaux, doivent s'assurer que tous les contrôles opérationnels et de conformité sont menés conformément au présent texte et dans le strict respect de la réglementation en vigueur.

Ces contrôles consistent, notamment, à :

- S'assurer du respect de l'application des dispositions de la politique de sécurité de l'information ;

Algerian Union Bank, SA au Capital Social de 1 850 000 000 MRU
Siège social : Lot n°80 de l'Ilot HMS - BP N°8581, Tevragh Zeina, Nouakchott, Mauritanie
RC N° 3909 / 119863, Agrément N° 16
NIF : 01323633

Algerian Union Bank Direction Générale

- S'assurer que la politique de la sécurité de l'information couvre tous les actifs primaires (données) et les actifs supports ;
- Veiller au respect des principes fondateurs de la sécurité de l'information de la Banque, d'ordre juridique, organisationnel, technique et physique ;
- Veiller à la revue périodique de la politique de la sécurité de l'information, en fonction des changements (législatifs, organisationnels, technologiques) opérés dans l'environnement et de l'évolution de la situation des menaces et des risques.

X. Annexe

Annexe : Liste des actifs et des services visés.

Algerian Union Bank Direction Générale NOUAKCHOTT

MS

ANNEXE

Liste des Actifs et des Services visés

La sécurité de l'information couvre l'ensemble des informations d'AUB avec toute la diversité que cela implique dans les usages :

- Les actifs primaires, représentés par les données, les informations et les processus métier, mais aussi tous les enregistrements des traces des évènements qui les concernent (identification, authentification, accès, opérations réalisées, date/heure, lieu d'accès, etc.…).

- Les actifs supports, représentés par tous les traitements de l'information de la Banque, sans exception, qu'ils soient manuels ou automatiques, réalisés en intranet local ou en extranet, et toutes les transactions effectuées.

- Les systèmes d'information et les applications y afférentes (Core Banking System ou applications métier ou de gestion, applications spécifiques, particulières et réglementaires, tels que le calcul d'actuariat, reportings, etc.…).

- Les applications informatiques : messagerie, portail, gestion du bureau d'ordre, gestion des archives, applications et publications Internet, stockage, Microsoft Office, sauvegarde…

- Les services associés (habilitations, droits d'accès, contrôles d'accès, administration, enregistrements, audits).

- L'infrastructure matérielle (serveurs de traitement, serveurs de données, serveurs d'annuaire, serveurs antivirus, autres serveurs, postes de travail).

- L'infrastructure réseau : les points de connexion, de concentration, de répartition, de routage, les réseaux virtuels (VLAN), les réseaux distants.

- Les lieux physiques d'hébergement des équipements serveurs et réseaux.

- Les bureaux, les salles de réunion.

- Les systèmes hors du champ informatique s'appuyant néanmoins sur les ressources, à savoir la téléphonie, VoIP, la visioconférence, la vidéosurveillance, les tableaux synoptiques de reproduction d'alarmes ou la visualisation des enregistrements des caméras de surveillance, etc.…

- Les contrôles d'accès physiques.

- Les interconnexions avec les partenaires.

Algerian Union Bank
Direction Générale
AUB

MS