🏦 FinSight Bank

Politique de Sécurité de l'Information et de Protection des Données
Version 2025 – Document interne confidentiel

Préambule

La présente *Politique de Sécurité de l'Information et de Protection des Données* définit le cadre global adopté par **FinSight Bank** pour garantir la confidentialité, l'intégrité, la disponibilité et la traçabilité des informations qu'elle détient ou traite.
Elle vise à assurer la protection des systèmes d'information et des données personnelles contre toute forme d'altération, de perte, d'accès non autorisé ou d'utilisation frauduleuse.
Cette politique s'inscrit dans le respect de la **Loi tunisienne n°2004-63** relative à la protection des données à caractère personnel, des exigences de l'**Instance Nationale de Protection des Données Personnelles (INPDP)**, ainsi que des principes du **Règlement Général sur la Protection des Données (RGPD)** et des standards internationaux **ISO/IEC 27001** et **ISO 27701**.

Elle constitue un pilier fondamental du dispositif de gouvernance, garantissant la confiance des clients, la conformité réglementaire et la résilience opérationnelle de la Banque dans un environnement numérique en constante évolution.

I. Objectifs et portée

L'objectif de cette politique est de protéger les actifs informationnels de FinSight Bank, qu'ils soient matériels, logiciels, organisationnels ou humains, contre tout risque de compromission.
Elle définit les principes, responsabilités et contrôles nécessaires pour assurer une gestion rigoureuse des données et des systèmes d'information, tout en respectant les droits des personnes concernées.

Son champ d'application couvre :

- Toutes les informations détenues ou traitées par la Banque, quel qu'en soit le support (numérique, papier, audio ou visuel) ;
- Tous les collaborateurs, prestataires et partenaires ayant accès à ces informations ;
- L'ensemble des systèmes, infrastructures, applications et réseaux utilisés dans le cadre des activités de FinSight Bank.

Aucune activité de traitement de données personnelles ou confidentielles ne peut être effectuée en dehors des règles édictées par la présente politique et ses annexes opérationnelles.

II. Principes fondamentaux de sécurité

La sécurité de l'information chez FinSight Bank repose sur quatre principes cardinaux : la **confidentialité**, l'**intégrité**, la **disponibilité** et la **traçabilité**.
Ces principes guident l'ensemble des actions techniques et organisationnelles déployées pour prévenir les incidents et garantir la continuité des services.

Principe	Définition	Objectif opérationnel
Confidentialité	Les informations sont accessibles uniquement aux personnes autorisées.	Empêcher les fuites ou divulgations non autorisées.
Intégrité	Les données doivent être exactes, complètes et protégées contre toute altération non légitime.	Garantir la fiabilité des informations et la validité des transactions.
Disponibilité	Les systèmes et informations doivent rester accessibles aux utilisateurs autorisés, selon les besoins métiers.	Assurer la continuité des activités même en cas d'incident.
Traçabilité	Toute action significative doit être enregistrée et vérifiable.	Permettre l'audit et la reconstitution des événements.

Ces principes s'appliquent de manière transversale à toutes les entités de la Banque, qu'il s'agisse des directions opérationnelles, techniques ou de support.

III. Gouvernance et responsabilités

La gouvernance de la sécurité de l'information repose sur une structure claire et hiérarchisée, garantissant la supervision stratégique et la mise en œuvre opérationnelle du dispositif.

Acteur	Rôle et responsabilités principales
Conseil d'Administration	Valide la politique globale de sécurité et en assure le suivi stratégique.
Comité des Risques et de la Conformité	Supervise les incidents majeurs de sécurité et les programmes de conformité RGPD.
Direction Générale	Détient la responsabilité ultime de la sécurité et affecte les ressources nécessaires.

Acteur	Rôle et responsabilités principales
Chief Information Security Officer (CISO)	Définit la stratégie de sécurité, pilote les projets de cybersécurité et gère les incidents.
Data Protection Officer (DPO)	Assure la conformité au RGPD/INPDP, gère les droits des personnes et les notifications aux autorités.
Utilisateurs et collaborateurs	Respectent les règles de sécurité, signalent tout incident et assurent la protection de leurs identifiants.

Cette gouvernance garantit l'équilibre entre la supervision stratégique et la réactivité opérationnelle, tout en assurant une indépendance des fonctions de contrôle.

IV. Classification et gestion de l'information

FinSight Bank classe ses informations selon leur niveau de sensibilité et de criticité, afin d'adapter les mesures de protection et les droits d'accès.

Niveau de classification	Type d'information	Exemples	Mesures de sécurité associées
Confidentiel – Stratégique	Informations critiques pour la Banque	Rapports de risque, prévisions financières, plans stratégiques	Chiffrement fort, accès restreint, audit régulier
Confidentiel – Client	Données personnelles ou financières identifiables	Dossiers KYC, relevés de compte, historiques de crédit	Masquage des données, stockage sécurisé, anonymisation partielle
Interne – Restreint	Données opérationnelles non publiques	Notes internes, procédures, rapports internes	Contrôle d'accès par profil, sauvegarde automatique
Public	Informations destinées à la diffusion externe	Communiqués, brochures, rapports publics	Publication contrôlée par la Direction Communication

Toute création, modification, diffusion ou destruction de données est soumise à une procédure de validation et de traçabilité documentée.

V. Protection des données personnelles

FinSight Bank s'engage à traiter les données personnelles de manière licite, loyale et transparente.
Chaque traitement fait l'objet d'une déclaration ou d'une notification auprès de l'**INPDP**, conformément à la réglementation tunisienne.
Les données collectées sont limitées au strict nécessaire, conservées pour une durée déterminée et sécurisées selon leur niveau de sensibilité.

Les personnes concernées disposent des droits suivants :

- Droit d'accès à leurs données personnelles ;
- Droit de rectification en cas d'erreur ;
- Droit d'opposition au traitement dans les conditions légales ;
- Droit à l'effacement et à la portabilité des données, lorsque cela est applicable.

Ces demandes sont centralisées et traitées par le **Data Protection Officer (DPO)**, qui assure le suivi des registres et le respect des délais de réponse réglementaires.

VI. Sécurité technique et cybersécurité

FinSight Bank adopte une approche de **défense en profondeur** pour protéger ses systèmes contre les cybermenaces et les intrusions non autorisées.
Les infrastructures critiques sont segmentées, redondées et sécurisées par des dispositifs de pare-feu, d'antivirus, de détection d'intrusion et de surveillance continue (*Security Operation Center – SOC*).

Les accès aux systèmes sont strictement contrôlés par des mécanismes d'authentification forte (MFA), de gestion centralisée des identités et de révocation automatique des droits en cas de départ d'un collaborateur.
Les données sensibles en transit et au repos sont systématiquement chiffrées.
Un **Plan de Réponse aux Incidents de Sécurité (PRIS)** est mis en œuvre pour assurer une réaction rapide, incluant les étapes de détection, confinement, éradication, reprise et retour d'expérience.

Type d'incident	Exemples	Procédure de réponse
Cyberattaque externe	Tentative de phishing, ransomware, DDoS	Activation PRIS, isolement réseau, notification CISO/DPO
Fuite de données	Envoi d'un fichier client non autorisé	Analyse d'impact, signalement INPDP sous 72h
Panne critique	Indisponibilité serveur,	Bascule PCA, restauration à partir des

Type d'incident	Exemples	Procédure de réponse
système	corruption base de données	sauvegardes
Violation interne	Utilisation abusive d'accès par un employé	Suspension immédiate, enquête disciplinaire, mise à jour des droits

---

VII. Formation, sensibilisation et culture de sécurité

La culture de sécurité constitue un élément déterminant de la résilience de FinSight Bank. Chaque collaborateur est tenu d'adopter des comportements responsables et de suivre les formations périodiques organisées par la Direction Sécurité Informatique et la Direction des Ressources Humaines.
Ces formations portent sur la cybersécurité, la protection des données, la gestion des mots de passe, la prévention du phishing et les bonnes pratiques numériques.

Des campagnes de sensibilisation internes, des tests de vulnérabilité et des simulations d'incidents sont régulièrement organisés afin de renforcer la vigilance collective.
Tout manquement grave ou récurrent aux règles de sécurité peut donner lieu à des mesures disciplinaires, conformément au règlement intérieur de la Banque.

VIII. Audits, contrôles et amélioration continue

La sécurité de l'information fait l'objet d'un suivi permanent et d'audits réguliers.
La **Direction Sécurité de l'Information** procède à des contrôles techniques trimestriels tandis que l'**Audit Interne** évalue annuellement l'efficacité du dispositif global.
Les résultats des audits sont présentés au Comité des Risques et font l'objet de plans de correction formels assortis de délais précis.

La Banque applique le principe d'**amélioration continue (PDCA – Plan, Do, Check, Act)** afin d'adapter son dispositif aux nouvelles menaces et aux évolutions réglementaires.
Toute modification majeure du système d'information ou du cadre juridique déclenche une révision de la présente politique.

IX. Révision et entrée en vigueur

La présente politique est révisée au minimum une fois par an ou à la suite d'un incident majeur, d'une inspection réglementaire ou d'une évolution technologique significative.
Les mises à jour sont préparées conjointement par le **CISO**, le **DPO** et la **Direction Générale**, puis validées par le **Comité des Risques et de la Conformité**.

Elle entre en vigueur à compter du **1er janvier 2025**, et son application est obligatoire pour l'ensemble du personnel, des filiales et des partenaires de FinSight Bank.