

I. Objectif et champs d'application

Cette procédure a pour objet de définir les règles, les responsabilités et les modalités pratiques de classification des informations numériques de la Banque de l'Union – Côte d'Ivoire (BDU-CI). Elle vise à garantir que chaque donnée numérique, quel que soit son format ou son environnement de stockage, fasse l'objet d'un niveau de classification approprié, proportionné à sa sensibilité, à sa valeur et à l'impact potentiel de sa divulgation, de son altération ou de sa perte. L'objectif est d'assurer une protection adaptée des données numériques, en renforçant la confidentialité, l'intégrité et la disponibilité des actifs critiques, tout en assurant une utilisation cohérente et efficace des moyens de sécurité.

Cette procédure s'applique à l'ensemble des collaborateurs (employés, managers, direction), prestataires, sous-traitants et partenaires de la BDU-CI, ainsi qu'à toute personne ou entité disposant d'un accès aux ressources numériques, dans les cas suivants :

- Création, modification ou diffusion d'une donnée numérique au sein de la Banque ;
- Échange de données numériques avec des tiers (clients, partenaires, prestataires) ;
- Conservation, archivage ou suppression définitive de données numériques ;
- Transfert de données numériques via un support ou un canal de communication ;
- Toute situation nécessitant de déterminer ou de réviser le niveau de classification d'une donnée numérique existante.

II. Objectifs de la procédure

L'objectif de cette procédure est de définir les rôles, responsabilités et mécanismes opérationnels permettant d'assurer une classification rigoureuse, cohérente et traçable des données numériques de la Banque de l'Union – Côte d'Ivoire (BDU-CI).

Elle s'inscrit dans une démarche proactive de maîtrise des risques liés à la mauvaise manipulation, à la diffusion non autorisée ou à la protection insuffisante des données numériques, et permet :

- D'appliquer un niveau de protection proportionné à la sensibilité et à la criticité des données numériques ;
- De réduire les risques de divulgation, d'altération ou de perte des informations ;
- De favoriser une utilisation optimale et cohérente des moyens de sécurité de la Banque;
- De renforcer la conformité réglementaire et la protection des données personnelles ;
- D'améliorer la sensibilisation et la responsabilisation des collaborateurs face aux enjeux de classification des données numériques.

Cette procédure couvre les domaines suivants :

- Définition des niveaux de classification des données numériques ;
- Attribution et révision des niveaux de classification ;
- Modalités de diffusion, d'échange et de partage des données numériques classifiées ;
- Conservation, archivage et déclassification des données ;
- Sensibilisation, contrôle et traçabilité de l'application des règles de classification.

III. Rôles et responsabilités

RÔLE	RESPONSABILITÉ
Direction Générale	S'assurer que les ressources nécessaires à la classification des données numériques au sein de la BDU-CI sont disponibles.
RSSI	Superviser la mise en œuvre de la procédure, contrôler régulièrement son application, définir les lignes directrices de classification et sensibiliser les collaborateurs.
DSI	Appliquer et faire appliquer les mesures techniques permettant la mise en œuvre de la classification (droits d'accès, chiffrement, outils de protection, etc.). Assurer l'accompagnement des métiers dans l'application opérationnelle des règles de classification.
Managers et Directeurs métiers	Veiller à la bonne application de la procédure par leurs équipes, s'assurer que chaque donnée produite ou gérée dans leur périmètre est correctement classifiée.

USER	Respecter les règles de classification, appliquer les niveaux attribués aux informations manipulées et signaler toute anomalie ou incohérence constatée.	
Direction de l'Audit Interne	Réaliser un contrôle annuel (niveau 3) afin d'identifier les écarts et de vérifier l'efficacité de la mise en œuvre de cette procédure.	

Acteurs impliqués dans la classification des données numériques

- ✓ Équipe RSSI / SSI
 - Définir et mettre à jour les règles de classification des données numériques.
 - Réaliser une veille réglementaire et normative.
 - Former et sensibiliser les utilisateurs.
 - Assurer le suivi et la traçabilité des données classifiées.
- ✓ Equipe DSI
 - Mettre en œuvre les solutions techniques de protection (chiffrement, contrôles d'accès, sauvegarde, etc.).
 - Garantir l'intégration des niveaux de classification dans les systèmes et applications.
 - Accompagner les utilisateurs dans l'application des règles.
- ✓ Managers métiers
 - Identifier les données produites ou gérées par leur équipe.
 - Attribuer ou valider le niveau de classification approprié.
 - S'assurer du respect du principe du « besoin d'en connaître ».
- ✓ Utilisateurs
 - Appliquer les niveaux de classification attribués.
 - Protéger les données numériques conformément à leur classification.
 - Signaler toute donnée mal classifiée ou divulgation non autorisée.
- ✓ Le Direction de l'Audit interne
 - Contrôler annuellement la bonne application de cette procédure.
 - Identifier les écarts et recommander des actions correctives.

IV. Sigles et Définitions

➤ Définitions

Classification des données : Processus consistant à catégoriser les informations (Publique, Interne, Confidentielle, Secrète) en fonction de leur sensibilité, de leur criticité et de leur impact potentiel en cas de divulgation, altération ou perte.

Marquage : Action consistant à apposer visuellement ou techniquement un label (ex. : "Confidentiel", "Interne") sur un document, un e-mail ou une donnée pour signaler son niveau de classification.

Étiquetage automatique : Fonctionnalité intégrée aux outils bureautiques ou de messagerie permettant d'attribuer automatiquement une classification aux données numériques en fonction de leur contenu ou du modèle appliqué.

Partage sécurisé : Ensemble de pratiques et d'outils visant à assurer que les données classifiées sont transmises uniquement aux personnes autorisées (ex. : chiffrement des e-mails, partage restreint sur SharePoint).

Sigles

MIP : Microsoft Information Protection (outil de classification et marquage)

DLP : Data Loss Prevention (prévention des fuites de données)

IRM : Information Rights Management (gestion des droits sur l'information)

Sommaire de la procédure

I. Objectif et champs d'application	1
II. Objectifs de la procédure.....	1
III. Rôles et responsabilités	2
IV. Sigles et Définitions.....	4
V. Références / Règles de gestion.....	5
VI. Narratif de la procédure	12

V. Références / Règles de gestion

❖ Documents de références

- Norme ISO/IEC 27001 : 2022 ;
- Politique de sécurité des systèmes d'information de la BDU-CI ;
- Politique de classification des actifs informationnels et technologiques de la BDU-CI

❖ Règles de gestion (Processus de classification des données numériques)

➤ Les Données concernées

La procédure s'applique aux données numériques produites, stockées, transmises ou traitées par la BDU-CI, quel que soit leur support (serveurs, postes de travail, mobiles, cloud, e-mails, bases de données, documents numériques, applications métiers).

➤ Objectifs de la classification

- Déterminer le niveau de sensibilité des données numériques ;
- Appliquer un niveau de protection approprié et proportionné ;
- Garantir la confidentialité, l'intégrité et la disponibilité des données ;
- Réduire les risques de perte, de divulgation non autorisée ou d'utilisation abusive.

➤ Niveaux de classification des données numériques

- **Niveau 1 – Public** : Données pouvant être rendues publiques sans impact négatif pour la Banque (ex. : brochures, informations commerciales diffusées, communiqués, etc.).
- **Niveau 2 – Interne** : Données destinées uniquement à un usage interne, dont la divulgation peut avoir un impact limité (ex. : notes internes, procédures standards, etc.).
- **Niveau 3 – Confidential** : Données sensibles dont la divulgation ou la perte aurait un impact significatif (ex. : données financières, plans stratégiques, données clients, etc.).
- **Niveau 4 – Strictement Confidential / Critique** : Données critiques dont la divulgation ou la perte aurait un impact grave sur la Banque (ex. : données personnelles sensibles, accès administrateurs, codes sources stratégiques, rapports d'incidents majeurs, etc.).

➤ **Processus de classification**

1. Identification des données numériques

Chaque manager métier identifie les données créées, reçues ou traitées par son service.

2. Attribution du niveau de classification

Le responsable métier **donne** un niveau de classification en fonction de la sensibilité et des critères définis dans la politique.

3. Étiquetage et traçabilité

Chaque donnée doit être étiquetée avec son niveau de classification (ex. en-tête, métadonnées, mention explicite, note de bas de page, etc.).

Les systèmes informatiques doivent enregistrer le niveau attribué (logs de classification).

4. Révision et mise à jour

Les niveaux de classification doivent être revus par les responsables métier régulièrement (au moins une fois par an) ou lors d'un changement du statut/usage des données.

➤ **Surveillance et contrôle de la classification**

Surveillance technique :

- Contrôles automatisés d'accès aux données et de gestion des habilitations.
- Vérifications régulières des règles de chiffrement et de sauvegardes.

Surveillance organisationnelle :

- Revues périodiques par les managers métiers pour s'assurer de la classification.
- Suivi par le RSSI via des audits internes afin d'identifier toute non-conformité.

➤ **Signalement des anomalies de classification**

Tout collaborateur ou prestataire constatant une erreur de classification ou une donnée sensible classifiée et mal protégée doit en informer immédiatement le **RSSI** et le **manager concerné**.

Les anomalies sont consignées dans un registre de suivi des non-conformités.

➤ Analyse et catégorisation des écarts de classification

Écart de niveau 1 (mineur) : Erreur de classification sans impact sur la sécurité. Correction par le manager et son collaborateur.

Écart de niveau 2 (modéré) : Données internes sensibles mal classifiées avec un risque limité. Correction rapide avec suivi du RSSI (incident possible si divulgation).

Écart de niveau 3 (majeur) : Données confidentielles mal classifiées, pouvant impacter la Banque. Traitement prioritaire par le RSSI et rapport au Comité Sécurité.

Écart de niveau 4 (critique) : Données secret exposées publiquement ou accessibles sans autorisation. Escalade immédiate au Comité Sécurité et actions urgentes.

➤ Traitement des écarts de classification

Mesures immédiates : restriction d'accès, retrait temporaire des données mal protégées.

Investigation : analyse par le manager métier, le RSSI, la SSI et la DSi pour identifier l'origine de l'erreur.

Mesures correctives : reclassement, ajustement des habilitations, chiffrement, sensibilisation des équipes.

Suivi post-incident : mise à jour des procédures, communication des leçons apprises.

NB : Un écart de niveau 3 ou 4 qui a exposé une donnée confidentielle ou secret à un public non autorisé doit faire l'objet d'un incident de sécurité de niveau 3 au moins.

❖ **Règles de gestion opérationnelles de classification des données numériques**

➤ Classification dans les emails (Outlook / OWA / Messagerie interne)

Objet et mention obligatoire :

Tout courriel contenant des données classifiées doit porter le niveau dans l'objet.

Exemples :

- **[Interne]** Compte rendu de réunion ;
- **[Confidentiel]** Liste des clients BDU-CI ;
- **[Secret]** Rapport d'incident critique de niveau 4 - accès restreint.

NB : Cette règle est **obligatoire** que pour les données **confidentielles et secrètes**.

Outil de marquage :

- Utiliser les **étiquettes de sensibilité (Sensitivity Labels / Microsoft Purview Information Protection)** mises en place dans Outlook.
- Sélectionner le niveau de classification du mail avant envoi (Public / Interne / Confidential / Secret).

Bonne pratique :

- Ne pas envoyer de données Confidentialles ou Secrètes à des adresses personnelles (Gmail, Yahoo, etc.).
 - Utiliser le chiffrement de mail pour **Confidentiel et Secret** (Options → Chiffrer).
- **Classification dans la production de documents (Word, Excel, PowerPoint, PDF)**

Marquage obligatoire :

- Les documents classifiés doivent afficher leur niveau de classification :
En-tête/pied de page : Indiquer le niveau sur chaque page (ex. : *Confidentiel – BDU-CI*).
- **Première page** : Mention explicite du niveau de classification du document.

Outils de marquage :

- Utiliser les modèles de documents officiels BDU-CI (Word/Excel/PowerPoint, etc.) intégrant automatiquement des filigranes (ex. : CONFIDENTIEL en arrière-plan).
- Utiliser l'option **Labels Sensibilité** de la suite Office pour assigner un niveau de classification permanent au fichier.

Bonne pratique :

- Ne jamais supprimer ou modifier un marquage officiel d'un document.
 - Pour les données **Confidentielles et Secret**, activer la **protection par mot de passe ou chiffrement** (Fichier → Protéger le document → Chiffrer avec mot de passe).
- **Classification dans les partages et stockages (SharePoint, OneDrive, GED, Serveurs internes (files server), etc.)**

Règles de stockage :

- **Public & Interne** : autorisés sur SharePoint ou OneDrive d'entreprise.
- **Confidentiel** : stockage uniquement dans des espaces sécurisés (dossiers avec droits restreints aux personnes autorisées).
- **Secret** : stockage uniquement dans les environnements à haut niveau de sécurité (serveur chiffré, GED avec contrôle strict d'accès, etc.) avec le concours du RSSI.

Outils de marquage :

- Utilisation d'étiquettes automatiques dans SharePoint et OneDrive (classification appliquée dès l'upload).
- Les fichiers **Secrets** doivent être protégés par **IRM (Information Rights Management)** pour interdire copie/impression/partage non autorisé.

Bonne pratique :

- Ne jamais stocker de documents classifiés secrets dans un support non sécurisé (clé USB non chiffrée, disque externe personnel, etc.) non validé par le RSSI.
- **Classification dans les communications instantanées et collaboration (Teams, Chat interne, WhatsApp pro si autorisé)**

Teams / Chat :

- Utiliser uniquement Teams ou outils internes pour échanger des données sensibles.
- Indiquer explicitement le niveau si des données sensibles sont échangées ([Confidentiel]).

Bonne pratique :

- Ne pas transmettre de données Secrets par chat.
- Éviter le copier/coller de données sensibles dans des canaux publics ou non protégés.

Bonnes pratiques transversales (tous supports numériques)

- **Toujours classifier avant de diffuser** : tout fichier ou email doit avoir un niveau de classification attribué.
- **Principe du moindre privilège** : partager uniquement avec les personnes qui en ont besoin.
- **Surveillance automatique** : les systèmes de la DSI (DLP – Data Loss Prevention) bloquent ou alertent en cas d'envoi de données classifiées en dehors des canaux autorisés.
- **Revue régulière** : chaque responsable métier doit vérifier que les données de son périmètre sont correctement classifiées et protégées.
- **Sensibilisation continue** : les collaborateurs doivent suivre les formations obligatoires sur la classification et le marquage des informations numériques.

Exemples concrets pour les collaborateurs :

Donnée Publique

Je rédige une brochure institutionnelle → je l'étiquette **Publique** dans Word avec le modèle BDU-CI → aucun filigrane n'est appliqué → je l'enregistre dans le dossier

SharePoint « Communication » (accès ouvert à tout le personnel) → je peux la diffuser librement par mail, sur le site web de la banque ou via des supports externes.

Donnée Interne

Je prépare un compte rendu hebdomadaire d'équipe → je l'étiquette **Interne** dans Word avec le modèle BDU-CI → un bandeau « Interne – BDU-CI » s'insère automatiquement → je l'enregistre dans le SharePoint de mon département (accès restreint aux employés internes) → si je l'envoie par mail, j'utilise Outlook avec l'étiquette Interne (chiffrement recommandé mais **non obligatoire**).

Donnée Confidentielle

Je rédige un rapport client → je l'étiquette **Confidentiel** dans Word avec le modèle BDU-CI → j'insère automatiquement le filigrane → je l'enregistre dans un dossier sécurisé SharePoint (accès limité à l'équipe projet) → si je dois l'envoyer par mail, j'utilise Outlook avec étiquette "Confidentiel" et chiffrement.

Donnée Secrète

Je manipule un fichier contenant des clés cryptographiques → je l'étiquette **Secret** avec le modèle BDU-CI → un filigrane rouge « SECRET – ACCÈS STRICTEMENT CONTRÔLÉ » est inséré automatiquement → je l'enregistre uniquement sur un serveur chiffré et cloisonné (accès nominatif restreint) → il est interdit de l'envoyer par mail, seul un canal sécurisé validé par la DSI et le RSSI est autorisé.

VI. Narratif de la procédure

PRO-RSSI-SSI-07	Procédure de gestion de la classification des données numériques	RSSI, DSI, Direction audit interne, Managers, users, Direction générale.
-----------------	--	--

Acteurs	Descriptions des tâches	Outils et interfaces
I. Identification et classification des données numériques initiales		
Managers métiers / Responsables de données	<ul style="list-style-type: none"> - Identifier les données numériques créées, reçues ou traitées par leur service. - Attribuer un niveau de classification (Public, Interne, Confidentiel, Secret) selon la politique. - Mettre à jour le registre de classification. 	Modèles BDU-CI (Word, Excel, PowerPoint), Bases de données métiers, Registre de classification interne
Utilisateurs (tous collaborateurs)	<ul style="list-style-type: none"> - Appliquer la classification au moment de la création du document ou du courriel. - Vérifier le niveau de classification avant toute diffusion. - Respecter le principe du moindre privilège. 	Microsoft Office (Labels Sensibilité), Outlook (étiquetage et chiffrement), SharePoint, OneDrive
II. Marquage et traçabilité des données numériques		
Utilisateurs / Propriétaires des données	<ul style="list-style-type: none"> - Étiqueter systématiquement les fichiers et courriels avec le niveau approprié. - S'assurer que les marquages visuels (bandeaux, filigranes, mentions explicites) apparaissent correctement. - Ne pas modifier ou supprimer les marquages automatiques. - Déclarer toute anomalie de marquage au RSSI. 	Labels Sensibilité (Microsoft Purview), Modèles BDU-CI, Filigrane automatique, Metadata Classification
III. Stockage et partage des données		
Utilisateurs / Administrateurs systèmes	<ul style="list-style-type: none"> - Stocker les données numériques en respectant leur classification. - Public & Interne → SharePoint / OneDrive standard. 	SharePoint, OneDrive, GED sécurisée, Serveurs chiffrés, HSM, Active

Acteurs	Descriptions des tâches	Outils et interfaces
	<ul style="list-style-type: none"> - Confidentiel → Espaces sécurisés (SharePoint restreint, GED sécurisée). - Secret → Serveurs chiffrés, cloisonnés, accès nominatif restreint. - Gérer les droits d'accès selon le principe du moindre privilège. - Appliquer IRM (Information Rights Management) pour interdire la copie/impression de documents sensibles. - Assurer la sauvegarde chiffrée et traçable des données critiques. 	
IV. Diffusion et communication des données		
Utilisateurs / Managers	<ul style="list-style-type: none"> - Vérifier le respect de la classification avant diffusion. - Utiliser les canaux autorisés selon le niveau : - Public → diffusion libre (site web, mail externe). - Interne → mails internes / intranet. - Confidentiel → Outlook avec chiffrement, Teams restreint. - Secret → interdiction de diffusion par mail, uniquement via canaux validés par RSSI/DSI. - Indiquer la classification dans l'objet des mails (obligatoire pour Confidentiel et Secret). 	Outlook (étiquetage + chiffrement), Teams, Outils de transfert sécurisé (SFTP/FTPS), Canaux approuvés DS/RSI
V. Révision et mise à jour des classifications		
Managers métiers	<ul style="list-style-type: none"> - Réviser régulièrement la classification des données numériques (au moins une fois par an). - Mettre à jour la classification si le statut ou l'usage de la donnée numériques change. - Transmettre les mises à jour au RSSI. 	Registre de classification, Outil ITSM, Rapports métiers
VI. Surveillance et contrôle		
RSSI / SSI	<ul style="list-style-type: none"> - Superviser le respect des règles de classification des données numériques. - Réaliser des audits internes réguliers. 	SIEM, DLP, ITSM, Rapports d'audit, Registre des anomalies

Acteurs	Descriptions des tâches	Outils et interfaces
	<ul style="list-style-type: none"> - Déployer et maintenir les contrôles techniques automatiques : - DLP (prévention des fuites de données) - SIEM (traçabilité des accès). - Former et sensibiliser régulièrement les collaborateurs. - Gérer le registre des anomalies de classification. 	

VII. Signalement et traitement des écarts de classification

Utilisateurs	<ul style="list-style-type: none"> - Signaler toute anomalie de classification ou donnée sensible mal protégée au RSSI/Manager. - Fournir les informations contextuelles (type de donnée, emplacement, usage). 	Email professionnel, Outil ITSM
RSSI / DSi / Comité Sécurité	<ul style="list-style-type: none"> - Analyser et catégoriser l'écart (Niveau 1 à 4). - Appliquer les mesures correctives : restriction d'accès, reclassement, chiffrement, sensibilisation. - En cas d'écart critique (niveau 4), escalade immédiate au Comité Sécurité et activation du plan de crise. 	ITSM, Réunions de crise, Rapports d'incident, Procédures internes

VIII. Suivi et amélioration continue

Direction Audit Interne	<ul style="list-style-type: none"> - Réaliser des contrôles périodiques de conformité. - Vérifier la bonne application de la politique de classification. - Identifier les écarts et proposer des mesures correctives. - Assurer le suivi des recommandations. 	Rapports d'audit, Documentation interne, Grilles de contrôle
-------------------------	--	--

Annexes / Enregistrements

Liste des ampliations

N°	Structures	Date	Visa	Observations
01				
02				

Liste des modifications

N°	Nature de la modification	Date	Chapitre ou page concerné (e)	Observations
01				
02				

Rédigé par : RESPONSABLE
DE LA SECURITE DES
SYSTEMES D'INFORMATION

Date : 05/11/2025

Signature :

Validé par : COMITE
PROCEDURES

Date : 05/11/2025

Signature :

Approuvé par : DIRECTION
GENERALE

Date :

Signature :

