

Directive sur la classification et la protection des documents dans l'administration communale de la Ville de Fribourg (du 23 septembre 2025)

Le Conseil communal de la Ville de Fribourg

vu :

- la loi sur la protection des données (LPrD ; RSF 17.1) ;
- le règlement sur la sécurité des données personnelles (RSD ; RSF 17.15) ;
- l'ordonnance sur la sécurité de l'information (OSI ; RSF 17.16),

adopte les dispositions suivantes :

Préambule

La Ville de Fribourg traite un volume important de documents contenant des informations de tous types, dont certaines données personnelles sensibles (citoyen·ne·s, personnel communal, contrats, données sociales ou médicales). Dans le cadre de sa mission de service public, elle doit garantir la sécurité de ces informations, conformément à la législation cantonale en matière de protection des données.

Cette directive définit un modèle de classification des documents applicable à l'ensemble des collaborateurs et partenaires de la Ville. Elle constitue un pilier de la gouvernance de la sécurité de l'information et sera intégrée dans toutes les politiques internes de gestion documentaire.

Chapitre 1 : Dispositions générales

Champ d'application

Art. 1 Cette directive s'applique à tous les documents, quel que soit leur format (papier, électronique, GED, messagerie) et à tous les collaborateurs, aux membres du

Conseil communal, aux prestataires et partenaires ayant accès aux systèmes d'information de la Ville.

Buts

Art. 2 Les buts de cette directive sont les suivants :

- a) Etablir une stratégie claire et harmonisée de classification et de protection des documents de la Ville de Fribourg.
- b) Assurer la confidentialité, l'intégrité et la disponibilité des informations.
- c) Se conformer aux exigences légales cantonales.
- d) Réduire les risques liés aux fuites, aux accès non autorisés et à la perte de maîtrise.
- e) Inspirer la confiance des citoyens en matière de protection des données.

Classification des documents et mesures de sécurité obligatoires

Art. 3 ¹La classification des documents est déterminée selon l'annexe qui fait partie intégrante de la présente directive.

²Les mesures de sécurité obligatoires sont les suivantes :

- Chiffrement systématique des données sensibles (C3).
- Contrôle d'accès strict basé sur le principe du moindre privilège.
- Authentification forte (MFA) pour tout accès aux systèmes critiques.
- Prévention des fuites (DLP) intégrée dans la GED et la messagerie.
- Journalisation et audits réguliers pour garantir la traçabilité.
- Sauvegardes sécurisées et tests périodiques de restauration.
- Gestion des accès externes (prestataires, partenaires intercommunaux) avec clauses contractuelles spécifiques.

Traitement des données
personnelles

Art. 4 ¹Les données personnelles doivent être traitées selon les exigences légales.

² Lors du traitement des données personnelles et des données sensibles, les objectifs de sécurité de la confidentialité, de l'intégrité, de la disponibilité et de la traçabilité doivent être garantis.

Gouvernance et
responsabilités

Art. 5 ¹Le responsable sécurité assure la mise en œuvre de la directive, supervise les audits et gère les incidents de sécurité.

²Les responsables métiers attribuent la bonne classification aux documents créés ou reçus.

³Les collaborateurs appliquent les règles de classification et signalent toute anomalie.

Cycle de vie et gestion
des changements

Art. 6 ¹ L'attribution de la classe se fait lors de la création ou de l'importation du document de manière automatique ou manuelle.

² La classification se conserve tout au long du cycle de vie (consultation, modification, archivage).

³La reclassification d'un document est possible si le contenu évolue (ex. passage de C1 à C3).

⁴Les changements de classe doivent être validés par le responsable du document et le référent sécurité.

⁵La traçabilité est assurée par la journalisation.

Application concrète

Art. 7 ¹Le modèle de classification est intégré dans la GED avec une protection automatique sur tout le cycle de vie.

Formation et
sensibilisation

²Les envois non autorisés sont bloqués dans la messagerie, des protections automatiques sont mises en place.

³Les droits des flux documentaires sont contrôlés sans impact sur l'efficacité des services.

Art. 8 ¹ Une formation initiale obligatoire sur la classification des documents est mise en place pour toutes les collaboratrices et les collaborateurs.

²Chaque année, des sessions de rappel sont mises en place.

³En cas de changement du cadre légal, des sessions de rappel supplémentaires sont mises en place.

⁴ Des campagnes de sensibilisation (ateliers, e-learning, tests de phishing) seront mises en place.

Entrée en vigueur

Art. 9 La présente directive entre en vigueur dès son adoption par le Conseil communal.

Adopté par le Conseil communal le 23 septembre 2025

Au nom du Conseil communal de la Ville de Fribourg

Le Syndic:

Le Secrétaire de Ville:

Thierry Steiert

David Stulz