



ETAT DE FRIBOURG
STAAT FREIBURG

Bibliothèque cantonale et universitaire BCU
Kantons- und Universitätsbibliothek KUB

Rue Saint-Michel 6, Case postale, 1701 Fribourg

T +41 26 305 13 33
www.fr.ch/bcu

Fribourg, le 18 août 2026 / ABO JMD

Bibliothèque cantonale et universitaire de Fribourg (BCU)

Règlement d'utilisation d'un système de vidéosurveillance avec enregistrement

vu

la loi du 7 décembre 2010 sur la vidéosurveillance (LVid) ;
l'ordonnance du 23 août 2011 sur la vidéosurveillance (OVid) ;
la loi du 12 octobre 2023 sur la protection des données (LPrD) ;
le règlement du 29 juin 1999 sur la sécurité des données personnelles (RSD),

adopte le règlement d'utilisation suivant :

Art. 1 Objet

1. Le présent règlement s'applique au système de vidéosurveillance avec enregistrement placé dans le site de la Bibliothèque cantonale et universitaire (BCU) de Fribourg à la Rue Saint-Michel 6 à 1700 Fribourg.
2. Le système de vidéosurveillance, objet du présent règlement, est composé de 14 caméras, fournies par Sécuriton SA ; marque et types de caméras : 3x Axis M 4318-PLVE, 5x Axis P3287-LV, 5x Axis P3287-LVE, 2x Axis P3827-PVE ; câblées et alimentées en PoE+ ; enregistrement sur détection de mouvements ; pas de zoom ; pas de visualisation en direct. (cf. annexe 1).
3. Ce système de vidéosurveillance a pour but de protéger la propriété et le patrimoine de l'Etat de Fribourg, de prévenir les atteintes aux personnes et aux biens, de prévenir des actes délictueux, notamment vols, agressions, dégradations, actes de vandalisme et fraudes, et de contribuer à la poursuite et à la répression des infractions. Il permet d'observer toute intrusion par des personnes non-autorisées et les mouvements à l'extérieur du bâtiment à la Rue Saint-Michel 6 (entrée principale pour le public), à la Rue Saint-Michel 8 (entrée pour le personnel), à la Rue Joesph-Piller 2A (entrée pour le personnel et pour les livraisons). Il permet également de prévenir la présence de personnes non-autorisées lorsque le bâtiment est fermé au public et d'observer les mouvements à l'intérieur du bâtiment dans le sas de



l'entrée principale publique, dans le hall d'accueil de l'entrée principale public, dans le hall d'accueil de l'entrée secondaire publique, dans les salles d'expositions et des activités culturelles, dans la salle de lecture des collections patrimoniales et précieuses.

4. Le dispositif permet de contribuer à la protection contre le vol des livres et d'autres supports patrimoniaux et précieux, notamment dans les vitrines patrimoniales d'exposition à l'étage 0, dans la salle de consultation du patrimoine. Il contribue également à la protection contre le vol de livres et d'autres supports généraux et universitaires et, notamment, des équipements techniques, des appareils et machines dans les espaces publics
5. Il fonctionne 7 jours sur 7, 24 heures sur 24 (déclenchement lorsqu'il y a des mouvements).

Art. 2 Organes et personnes autorisées

1. La direction de la BCU est l'organe responsable du système de vidéosurveillance.
2. Les personnes autorisées à consulter les données enregistrées (enregistrements) par le système de vidéosurveillance sont les suivantes :
 - le chef ou la cheffe du secteur Infrastructures de la BCU ;
 - le chef ou la cheffe du secteur Logistique de la BCU ;
 - le chef ou la cheffe du secteur Administration de la BCU ;
 - le collaborateur ou la collaboratrice du secteur Administration, répondant ou répondante Santé et Sécurité au travail de la BCU.
3. Les personnes susmentionnées sont soumises à l'obligation du respect du secret de fonction, respectivement de confidentialité. L'identité de ces personnes est consignée par l'organe responsable dans un document qui est actualisé si elles sont remplacées.

Art. 3 Données mises à disposition

1. Les données consultables par les personnes susmentionnées (art. 2 al. 2 ci-dessus) sont les images récoltées et enregistrées par l'installation de vidéosurveillance.
2. Il se peut que les images obtenues ainsi contiennent des données dites sensibles au sens de l'art. 4 al. 1 let. c LPrD, de sorte qu'un devoir de diligence accru s'applique (cf. art. 11 LPrD).

Art. 4 Traitement des données

1. Les données enregistrées ne doivent être utilisées que dans le cadre des buts définis à l'article 1 al. 3 et 4.
2. Les images enregistrées ne sont pas visionnées en temps réel.
3. Les titulaires d'autorisation personnelle ne consultent les images enregistrées qu'en cas de nécessité, à savoir en cas d'atteinte avérée.
4. Les personnes autorisées à consulter les données sont susceptibles d'être interrogées en tout temps, y compris au-delà de l'exercice de leurs fonctions, sur les données qu'elles auront visionnées ou sur leurs agissements en relation avec ces données.
5. Les données enregistrées sont automatiquement détruites après 7 jours. En cas d'atteinte avérée aux personnes ou aux biens, les données enregistrées sont extraites sur un support informatique et sont détruites après 100 jours au maximum sous réserve de leur transmission à une autorité judiciaire ou à la Police cantonale à des fins d'enquête. Un protocole de destruction est conservé.

6. Des copies ou impressions peuvent être effectuées mais doivent être détruites dans les mêmes délais que les originaux. Un protocole de copie est conservé.
7. La commercialisation d'éventuelles impressions et reproductions est interdite.
8. Toute communication de données est interdite, en dehors du cadre légal (art. 4 al. 1 let. e LVid).
9. Toute fonctionnalité permettant d'émettre et/ou d'enregistrer des sons est interdite. L'organe responsable n'est pas autorisé à utiliser de fonctionnalité permettant la reconnaissance faciale, l'analyse des données ou toute autre fonctionnalité relevant de l'intelligence artificielle (IA).

Art. 5 Mesures de sécurité

1. Les données informatiques sont protégées par l'organe responsable du fichier de la façon suivante :
 - une autorisation personnelle d'accès (mot de passe) est délivrée aux personnes autorisées (cf. art. 2) pour lesquelles un accès est nécessaire en raison de leur fonction ;
 - les titulaires d'autorisation personnelle reçoivent alors un mot de passe qu'ils modifient régulièrement ;
 - une double authentification est prévue.
2. Toute activité effectuée sur le système ou sur une des applications informatiques est automatiquement enregistrée et répertoriée à des fins de contrôle et/ou de reconstitution.
3. Les images sont stockées sur un cloud & SAS (Software as a Service) hébergé en Suisse et, en tant que back-up, sur une carte SD (Secure Digital) intégrées à chaque caméra afin de prévenir une coupure d'Internet.
4. Les systèmes de stockage et d'hébergement des données (et/ou le *back-up*) sont protégés dans un lieu adéquat en Suisse, fermé à clé et non-accessible aux personnes non autorisées. Une carte SD interne à chaque caméra, chiffrée et protégée physiquement, enregistre les images en back-up du cloud & SAS durant 7 jours.
5. Les images enregistrées et celles extraites doivent être stockées sur un support physique indépendant, sans accès à distance possible.
6. Le transfert ainsi que le stockage des données sont chiffrés par un protocole TLS de point à point (de la caméra à l'enregistreur se trouvant sur le cloud & SAS).
7. L'organe responsable s'assure de la conformité des mesures techniques et organisationnelles concernant l'accès des personnes autorisées à visionner les enregistrements, notamment s'agissant des appareils utilisés.

Art. 6 Droit d'accès

1. Toute personne peut demander au ou à la responsable du système l'accès à ses propres données.
2. Le ou la responsable du système répond à la demande tout en respectant les droits de la personnalité des autres personnes concernées (p. ex. en les floutant).

Art. 7 Signalement

Le système de vidéosurveillance est signalé à ses abords au moyen de panneaux informant sans équivoque les personnes se trouvant dans la zone surveillée sous la forme d'un

pictogramme et mentionnant le ou la responsable du système ainsi qu'un lien (QR-Code) vers le règlement publié sur le site web de la BCU.

Art. 8 Responsabilité

1. L'organe responsable demeure responsable de la protection des données envers d'éventuels mandataires et/ou sous-traitants. Il leur donne, à ce sujet, les instructions nécessaires et veille à ce que les données ne soient utilisées et/ou communiquées que conformément et pour l'exécution du contrat.
2. Le contrat est annexé au Règlement d'utilisation. Il contient les mesures organisationnelles et techniques exigées par l'organe responsable ainsi qu'une clause de confidentialité.
3. Les collaboratrices et les collaborateurs du contractant signent une clause de confidentialité. Celle-ci est annexée au Règlement d'utilisation.

Art. 9 Mesures de contrôle

a. Contrôles internes

1. Des contrôles techniques de l'installation ainsi que le contrôle du respect des mesures de sécurité sont effectués par Sécuriton SA une fois par année. Ces contrôles ont lieu sur le site, en présence d'une personne autorisée (cf. art. 2 ch. 2).
2. Il convient notamment de vérifier l'orientation de chaque caméra, le respect de leur programmation (horaire) et leur signalisation.
3. Chaque contrôle fera l'objet d'un protocole dûment signé par le ou la responsable de l'installation.

b. Contrôle général

1. La préfète ou le préfet exerce un contrôle général sur les installations de vidéosurveillance.
2. Les contrôles du ou de la préposé-e cantonal-e à la protection des données sont en outre réservés.

Art. 10 Entrée en vigueur

Le présent règlement entre en vigueur au moment de son approbation préfectorale.

Adopté par la Bibliothèque cantonale et universitaire, le 12 août 2026.


Angélique Boschung
Directrice BCU


Jean-Marc Dücrey
Chef de projet
de la nouvelle BCU

Approuvé par la Préfecture de la Sarine le

12 août 2026



