ACCROPRINT

# Mesures techniques et organisationnelles de cybersécurité

## Protection des données et sécurité des solutions numériques

| | |
|---|---|
| **Organisation** | ACCROPRINT |
| **Version** | 1.0 |
| **Date** | 1 janvier 2026 |
| **Classification** | Document de référence officiel |

### Objet

Le présent document décrit le cadre de sécurité appliqué aux sites web, applications, logiciels et solutions numériques développés ou exploités par ACCROPRINT. Il constitue le référentiel général destiné notamment aux collectivités publiques, communes, partenaires et clients souhaitant comprendre les mesures mises en œuvre pour réduire les risques cyber et protéger les données.

### Version officielle du référentiel

La version officielle est celle mise à disposition sur le site internet officiel d'ACCROPRINT. Toute copie téléchargée, imprimée, transmise par e-mail ou conservée localement doit être considérée comme une copie de consultation susceptible de ne plus correspondre à la dernière version publiée.

Seule la version publiée sur le site internet d'ACCROPRINT fait foi, sauf lorsqu'un document, une annexe, une offre, un contrat ou des échanges écrits prévoient expressément des mesures, responsabilités ou modalités différentes pour un client ou un projet particulier. Dans ce cas, les dispositions spécifiques convenues pour ce client ou ce projet prévalent pour le périmètre concerné.

# Table des matières

# 1. Objet, principes et périmètre

- ACCROPRINT applique une approche de sécurité par conception (« security by design ») et de protection des données par défaut aux développements numériques concernés.
- Les objectifs fondamentaux sont la confidentialité des informations, l'intégrité des données et traitements, la disponibilité des services ainsi que la traçabilité des opérations sensibles.
- Les mesures sont adaptées au niveau de criticité, aux données traitées, aux fonctionnalités exposées et aux exigences contractuelles du projet.
- Le présent référentiel définit un socle général. Des mesures supplémentaires peuvent être appliquées à une solution ou à un client lorsque son contexte l'exige.

# 2. Socle de sécurité obligatoire des applications web

- Chiffrement des communications par HTTPS/TLS et redirection des accès HTTP lorsque l'environnement le permet.
- Validation côté serveur des données reçues ; aucune donnée provenant du navigateur n'est considérée comme fiable par défaut.
- Utilisation de requêtes préparées ou paramétrées pour réduire le risque d'injection SQL.
- Encodage et échappement adaptés des contenus affichés afin de réduire le risque XSS.
- Protection CSRF sur les opérations modifiant des données ou l'état d'un compte.
- Contrôle des autorisations côté serveur pour chaque opération sensible ; masquer un élément dans l'interface ne constitue pas une autorisation.
- Contrôle strict des fichiers téléversés : type, extension, taille, destination et accès selon les besoins du projet.
- Mise en place de headers HTTP de sécurité appropriés, notamment contre le clickjacking et l'interprétation indésirable de contenus ; politique CSP lorsque compatible avec l'application.
- Réduction des informations techniques inutilement exposées au public et traitement contrôlé des erreurs.

# 3. Authentification, comptes et sessions

- Stockage des mots de passe sous forme de hash sécurisé ; aucun mot de passe utilisateur ne doit être conservé en clair.
- Gestion des rôles et permissions selon le principe du moindre privilège.
- Authentification à deux facteurs activée pour les environnements ou profils qui le nécessitent.
- Protection contre les tentatives répétées de connexion : limitation, temporisation ou blocage selon le contexte.
- Sessions générées et contrôlées côté serveur ; expiration et révocation prévues.
- Cookies de session configurés avec les attributs Secure, HttpOnly et SameSite lorsque techniquement applicables.
- Révocation des accès lors d'un changement de rôle, d'un départ ou d'un incident de sécurité.

# 4. Protection des données

- Collecte limitée aux informations nécessaires à la finalité du service.
- Accès aux données limité aux utilisateurs et fonctions autorisés.
- Durées de conservation définies selon le besoin opérationnel, légal ou contractuel ; suppression ou anonymisation lorsque les données ne sont plus nécessaires.
- Exports et téléchargements protégés par les mêmes contrôles d'autorisation que l'application.
- Les journaux techniques sont conçus pour éviter l'enregistrement inutile de mots de passe, secrets ou données sensibles.
- Les sauvegardes contenant des données sont considérées comme des données à protéger au même titre que les systèmes de production.
- Le traitement est organisé en tenant compte de la Loi fédérale suisse sur la protection des données (LPD) et, lorsqu'il est applicable au traitement concerné, du RGPD.

## 5. Infrastructure et hébergement

- Sauf indication contraire convenue pour un projet particulier, les solutions numériques développées et exploitées par ACCROPRINT utilisent l'infrastructure d'hébergement FlowHardware.
- Les environnements sont configurés pour limiter l'exposition réseau aux services nécessaires.
- Les accès d'administration sont réservés aux personnes autorisées et protégés par des mécanismes adaptés au niveau de risque.
- Les systèmes, composants applicatifs et dépendances font l'objet de mises à jour de sécurité selon leur criticité et selon la répartition des responsabilités techniques.
- Les secrets techniques, identifiants, clés et mots de passe ne doivent pas être intégrés dans le code public ou exposés dans les interfaces.
- Lorsque l'architecture le permet, les environnements de développement, test et production sont séparés.

## 6. Journalisation et traçabilité

- Les applications critiques peuvent journaliser les connexions, échecs de connexion, opérations administratives, changements de permissions et actions sensibles.
- Les journaux sont accessibles uniquement aux personnes autorisées et conservés pendant une durée proportionnée à leur finalité.
- Les traces doivent permettre d'analyser un incident sans créer une copie excessive des données métier.

## 7. Sauvegardes et continuité

- Les projets nécessitant une continuité de service disposent d'une stratégie de sauvegarde adaptée aux données et à leur criticité.
- Les sauvegardes couvrent, selon le projet, les bases de données, fichiers applicatifs ou données nécessaires à une restauration.
- Plusieurs générations peuvent être conservées afin de réduire le risque lié à une corruption ou à une suppression découverte tardivement.
- Une sauvegarde n'est considérée comme réellement exploitable que si sa restauration peut être réalisée et contrôlée.
- Les objectifs de reprise et les délais de restauration sont déterminés en fonction du service et des engagements convenus.

## 8. Menaces prises en compte

- Les mesures de sécurité sont conçues pour réduire notamment les risques d'injection SQL, XSS, CSRF, brute force, détournement de session, accès non autorisé, téléversement malveillant, automatisation abusive, exploitation de composants vulnérables et exfiltration de données.
- Le niveau de protection est réévalué lorsque la nature du service, son exposition ou les données traitées évoluent.

## 9. Gestion d'un incident cyber

- Détection : identification d'un comportement anormal, d'une alerte ou d'une compromission potentielle.
- Confinement : limitation de l'accès ou isolation du composant concerné afin d'empêcher l'extension de l'incident.
- Analyse : examen des journaux, comptes, modifications et systèmes concernés afin d'établir l'origine et l'étendue.
- Correction : suppression de la cause, correction de la vulnérabilité et rotation des secrets ou identifiants compromis.
- Restauration : remise en service à partir d'un état contrôlé ou d'une sauvegarde saine lorsque nécessaire.
- Contrôle : vérification du fonctionnement et surveillance renforcée après remise en service.
- Documentation : conservation des éléments utiles à l'analyse et amélioration des mesures préventives.
- Notification : évaluation des obligations contractuelles et légales de communication aux personnes, clients ou autorités concernées.

# 10. Gestion des vulnérabilités et développement sécurisé

- Les dépendances et composants utilisés sont maintenus à jour en fonction des correctifs disponibles et de leur criticité.
- Les corrections de sécurité sont prioritaires lorsqu'une vulnérabilité exploitable affecte un service exposé.
- Les fonctionnalités sensibles sont testées avant leur mise en production.
- Des revues de code, contrôles automatisés, audits ou tests de sécurité peuvent être ajoutés selon le niveau de risque du projet.
- Une application n'est pas déclarée conforme au socle ACCROPRINT tant que les contrôles obligatoires applicables n'ont pas été vérifiés.

# 11. Prestataires, hébergement et services externes

## 11.1 Hébergement de référence : FlowHardware

Sauf indication contraire expressément définie lors des échanges avec le client, l'ensemble des solutions numériques développées et exploitées par ACCROPRINT sont hébergées sur une infrastructure fournie par FlowHardware. FlowHardware constitue le prestataire d'hébergement de référence d'ACCROPRINT pour ses applications web, logiciels, plateformes et autres services numériques nécessitant une infrastructure serveur.

Lorsqu'un projet nécessite un autre hébergement en raison d'une exigence technique, contractuelle, réglementaire ou formulée par le client, cette exception est définie spécifiquement dans la documentation ou les échanges relatifs au projet concerné. En l'absence d'une telle indication, l'hébergement FlowHardware constitue l'environnement utilisé par défaut.

## 11.2 Principe de responsabilité partagée

- FlowHardware : intervient comme prestataire technique pour les éléments relevant de l'infrastructure et du service d'hébergement conformément aux prestations effectivement souscrites.
- ACCROPRINT : assure les éléments relevant du développement, de la configuration applicative, de l'authentification, des permissions, de la protection fonctionnelle des données et des composants placés sous sa responsabilité.
- Client / Commune : conserve les responsabilités relevant de son organisation, notamment la désignation des utilisateurs autorisés, l'attribution appropriée des comptes et l'utilisation correcte de la solution.

## 11.3 Infrastructure des solutions ACCROPRINT

- Limitation des services exposés publiquement au strict nécessaire.
- Restriction des accès administratifs et protection des identifiants techniques.
- Suppression ou révocation des accès devenus inutiles.
- Séparation logique des applications lorsque l'architecture ou la criticité l'exige.
- Maintenance des composants logiciels relevant du périmètre administré par ACCROPRINT.
- Protection des fichiers de configuration et limitation de l'exposition des bases de données.
- Les accès techniques à l'infrastructure sont distincts des comptes utilisateurs disponibles dans les applications.

## 11.4 Protection des communications

Les solutions web ACCROPRINT sont destinées à être accessibles au moyen de connexions sécurisées HTTPS/TLS. Le chiffrement protège les informations échangées entre l'utilisateur et le serveur contre leur lecture ou leur modification pendant la transmission. Les applications sont également conçues afin d'éviter l'exposition inutile de mots de passe, clés API, identifiants de bases de données, secrets applicatifs ou autres informations techniques sensibles.

## 11.5 Protection des bases de données

- Accès limité aux services et personnes autorisés.
- Protection des identifiants de connexion.
- Limitation de l'exposition publique directe des services de base de données lorsqu'elle n'est pas nécessaire.
- Utilisation de requêtes préparées ou paramétrées.
- Contrôle des droits accordés aux applications.
- Sauvegarde selon les exigences du projet et révocation des accès devenus inutiles.

### 11.6 Sauvegardes

La stratégie de sauvegarde peut comprendre plusieurs niveaux complémentaires : sauvegardes proposées au niveau de l'infrastructure FlowHardware selon les prestations souscrites, sauvegardes des bases de données, sauvegardes applicatives organisées par ACCROPRINT et sauvegardes spécifiques définies avec le client lorsque nécessaire. Les sauvegardes contenant des données sont protégées au même titre que les données de production.

### 11.7 Gestion d'un incident lié à l'hébergement

- Identifier si l'origine est applicative ou liée à l'infrastructure.
- Restreindre temporairement l'accès à la solution lorsque la sécurité l'exige.
- Analyser les journaux et événements disponibles.
- Solliciter FlowHardware lorsqu'une intervention du prestataire est nécessaire.
- Corriger les composants relevant d'ACCROPRINT.
- Révoquer ou remplacer les identifiants et secrets potentiellement compromis.
- Restaurer une sauvegarde considérée comme saine lorsque nécessaire.
- Vérifier l'intégrité et le fonctionnement avant le retour complet en production.

### 11.8 Services externes complémentaires

- Fournisseurs de noms de domaine ou DNS.
- Services d'envoi d'e-mails.
- API externes.
- Services cartographiques ou météorologiques.
- Systèmes de notification.
- Services de stockage, supervision ou journalisation.
- Autres services nécessaires au fonctionnement de l'application.

ACCROPRINT cherche à limiter les données transmises à ces services au strict nécessaire et à éviter la transmission de données personnelles lorsqu'elles ne sont pas nécessaires à la fonctionnalité concernée.

### 11.9 Documentation des exceptions

FlowHardware constitue l'hébergement de référence. Lorsqu'une solution est hébergée totalement ou partiellement auprès d'un autre prestataire, cette situation constitue une exception au modèle standard ACCROPRINT et doit être identifiée dans les échanges, la documentation technique, l'offre, le contrat ou tout autre écrit relatif au projet.

### 11.10 Protection des données auprès des prestataires

- Nature du service fourni et catégories de données concernées.
- Finalité du traitement et accès techniques potentiels.
- Localisation pertinente de l'hébergement ou du traitement lorsque cette information est requise.
- Éventuels sous-traitants supplémentaires.
- Mécanismes de suppression, restitution ou révocation des accès.
- Exigences contractuelles ou réglementaires applicables au projet.

## 12. Répartition des responsabilités

- ACCROPRINT est responsable des mesures de sécurité relevant du code, de la configuration applicative et des opérations qui lui sont confiées.
- Le client reste responsable des usages relevant de son organisation : attribution des comptes, choix des utilisateurs autorisés, exactitude des données saisies et respect de ses propres obligations internes, sauf disposition spécifique différente.
- FlowHardware et les autres fournisseurs externes restent responsables des couches techniques relevant de leurs prestations effectivement souscrites.
- La répartition exacte des responsabilités peut être précisée pour chaque projet par contrat, offre, annexe ou échanges écrits.

## 13. Registre de sécurité par application

Chaque solution importante peut être documentée au moyen de la fiche suivante afin de distinguer le socle commun des mesures propres au projet.

| | |
|---|---|
| **Application / service** | |
| **Client / responsable métier** | |
| **URL / environnement** | |
| **Hébergement** | FlowHardware par défaut / exception documentée |
| **Données traitées** | |
| **Niveau de criticité** | Faible / Moyen / Élevé / Critique |
| **Authentification** | |
| **2FA** | Oui / Non / Non applicable |
| **Rôles et permissions** | |
| **Sauvegardes** | |
| **Journalisation** | |
| **Services externes** | |
| **Mesures spécifiques** | |
| **Dernière vérification sécurité** | |
| **Statut** | Appliqué / En cours / Prévu / Non applicable |

## 14. Checklist de mise en production

☐ HTTPS/TLS actif et redirections vérifiées.

☐ Mode debug et erreurs détaillées désactivés en production.

☐ Secrets absents du code public et des journaux.

☐ Requêtes SQL paramétrées vérifiées.

☐ Validation serveur des entrées.

☐ Échappement des sorties et contrôles XSS.

☐ Protection CSRF des opérations sensibles.

☐ Autorisations testées avec plusieurs rôles et comptes.

☐ Cookies et sessions sécurisés.

☐ Protection des connexions et limitation des tentatives.

☐ Uploads contrôlés et stockage vérifié.

☐ Headers HTTP de sécurité contrôlés.

☐ Sauvegarde et procédure de restauration définies.

☐ Journalisation des actions sensibles configurée.

☐ Dépendances mises à jour et vulnérabilités critiques traitées.

☐ Comptes de test, données temporaires et accès inutiles supprimés.

☐ Protection des données et durées de conservation vérifiées.

☐ Prestataires externes et flux de données documentés.

☐ Hébergement FlowHardware confirmé ou exception documentée.

☐ Procédure de contact en cas d’incident identifiée.

☐ Fiche de sécurité de l’application mise à jour.

## 15. Suivi et amélioration continue

La sécurité numérique n’est pas considérée comme un état définitif. Les mesures décrites dans ce document évoluent avec les menaces, les technologies, les exigences légales et les changements apportés aux solutions. ACCROPRINT peut réviser ce référentiel à la suite d’un incident, d’un audit, d’une modification importante d’architecture ou de l’apparition d’une vulnérabilité pertinente.

## 16. Statut des mesures et gestion des versions

Ce document constitue le référentiel général de sécurité d’ACCROPRINT. Seules les mesures effectivement vérifiées doivent être présentées comme appliquées. Une mesure non encore déployée doit être identifiée comme « en cours », « prévue » ou « non applicable ».

La version officielle en vigueur est exclusivement celle publiée sur le site internet officiel d’ACCROPRINT. Les exemplaires téléchargés, imprimés ou transmis constituent des copies de consultation. En cas de différence entre une copie et la version publiée sur le site, la version publiée sur le site prévaut.

Exception : lorsqu’un client ou un projet fait l’objet de dispositions spécifiques convenues par contrat, offre, annexe, cahier des charges ou échanges écrits, ces dispositions particulières prévalent sur le référentiel général uniquement pour le périmètre auquel elles se rapportent.