Annexe 1 au CCTP

Exigences en termes de cybersécurité

Sommaire

1. Objet et périmètre 3
2. Référentiels de référence 3
2.1 Règlement européen NIS2 (UE 2022/2555) 3
2.2 Référentiels et guides de l'ANSSI 3
2.3 Politique ministérielle 3
2.4 Normes ISO/IEC 27001 et 27002 3
2.5 OWASP Top 10 3
2.6 CIS Benchmarks 4
2.7 RGS et RGPD (UE 2016/679) 4
3. Gouvernance et responsabilité 4
3.1 Référent sécurité 4
3.2 Plan d'Assurance Sécurité (PAS) 4
3.3 Sous-traitance 4
3.4 Sécurité de la chaîne d'approvisionnement logicielle 4
3.5 Confidentialité 5
3.6 Sensibilisation et formation à la cybersécurité 5
3.7 Schéma d'escalade en cas d'incident 5
4. Gestion des identités et des accès 5
4.1 Comptes nominatifs 5
4.2 Authentification multifacteur (MFA) 6
4.3 Politique de mots de passe 6
4.4 Principe du moindre privilège 6
4.5 Revue périodique des droits 6
4.6 Gestion des comptes inactifs 6
4.7 Gestion des secrets et des clés d'accès 6
5. Sécurité des systèmes et du réseau 7
5.1 Segmentation des environnements 7
5.2 Filtrage et exposition Internet 7
5.3 Chiffrement des communications et des données 7
5.4 Accès administratifs 7
5.5 Journalisation, horodatage et synchronisation 7
6. Supervision et détection 8
6.1 Protection des postes et serveurs 8
6.2 Alertes de sécurité 8
6.3 Journalisation et conservation des logs 8
7. Gestion des vulnérabilités et mises à jour 8
7.1 Délais d'application des correctifs 8

7.2 Exigences complémentaires 9
7.2.1 Rapports de correctifs 9
7.2.2 Scans de vulnérabilités 9
8. Sécurité applicative et développement sécurisé 9
8.1 Cycle de développement sécurisé (Secure SDLC) 9
8.2 Analyse du code et tests de sécurité 9
8.3 Gestion des dépendances tierces 9
8.4 Sécurisation de la chaîne CI/CD 10
9. Sauvegardes et continuité 10
9.1 Exigences de sauvegarde 10
9.2 Tests de restauration 10
9.3 Exigences de continuité d'activité 10
10. Gestion des incidents 11
10.1 Notification des incidents 11
10.2 Rapport d'incident 11
10.3 Collaboration 11
11. Audit et contrôle 11
11.1 Audits programmés 11
11.2 Contrôles et tests d'intrusion 11
11.3 Livrables attendus du prestataire 12
12. Fin de contrat 12
12.1 Restitution et destruction des données 12
12.2 Délai maximal d'effacement 12
12.3 Attestation d'effacement 12
12.4 Suppression des accès 12
12.5 Interdiction de réutilisation 12
13. Sanctions et clauses 13
13.1 Mesures graduelles et proportionnées 13
13.2 Suspension temporaire des accès 13
13.3 Notification aux autorités compétentes 13
13.4 Application des dispositions contractuelles 13
14. Suivi et révision 13

1. Objet et périmètre

Ce document définit les exigences minimales de cybersécurité applicables à tout prestataire intervenant sur le système d'information de l'Établissement public du Palais de la Porte Dorée, ci-après « l'Établissement », ou traitant des données lui appartenant, quels que soient :

- le type de prestation (hébergement, développement, maintenance, infogérance, support, audit, etc.),
- le mode de mise en œuvre (API, SaaS, plateforme web, application métier, réseau, infrastructure, etc.),
- l'environnement technique utilisé (cloud, on-premise, hybride).

Ces exigences constituent le socle obligatoire que chaque prestataire doit respecter dès le lancement d'un projet et pendant toute la durée du contrat.

Elles complètent :

- les obligations légales (notamment RGPD),
- les obligations contractuelles (CCAP, clauses de sécurité),
- les directives internes de l'Établissement,
- et s'inscrivent dans le cadre de la Politique de Sécurité des Systèmes d'Information (PSSI) de l'Établissement, ou la politique de sécurité du numérique ministérielle (PSNum) à défaut.

Elles s'appliquent également aux sous-traitants du prestataire, qui doivent respecter un niveau équivalent d'exigences de sécurité.

2. Référentiels de référence

Les exigences définies dans ce document s'appuient sur les normes, réglementations et bonnes pratiques reconnues en cybersécurité et en protection des données. Elles constituent un référentiel d'inspiration permettant à l'Établissement d'orienter et d'évaluer le niveau de sécurité attendu des prestataires, sans imposer l'application exhaustive de l'ensemble des standards cités.

Les principaux référentiels applicables sont :

2.1 Règlement européen NIS2 (UE 2022/2555)

Obligations de sécurité, gestion des risques, continuité d'activité, notification des incidents.

2.2 Référentiels et guides de l'ANSSI

Politique de sécurité des systèmes d'information de l'État (PSSIE), guides techniques, bonnes pratiques de sécurisation, durcissement et supervision.

2.3 Politique ministérielle

Politique ministérielle de sécurité du numérique (PSNUM) (**NOR :** MICB2201459A)

2.4 Normes ISO/IEC 27001 et 27002

Management de la sécurité de l'information, mesures organisationnelles et techniques.

2.5 OWASP Top 10

Exigences de sécurité applicative et API lors des développements, mises à jour et audits.

2.6 CIS Benchmarks

Durcissement des systèmes, serveurs, configurations réseau et environnements d'hébergement.

2.7 RGS et RGPD (UE 2016/679)

Sécurisation des traitements, protection des données personnelles, conformité réglementaire.

3. Gouvernance et responsabilité

Le prestataire est responsable de la mise en œuvre et du maintien d'un niveau de sécurité conforme aux exigences de l'Établissement. À ce titre, il doit respecter les obligations suivantes.

3.1 Référent sécurité

Le prestataire désigne un point de contact sécurité responsable du suivi opérationnel et disponible en cas d'incident ou de demande urgente de l'Établissement. Il est chargé :

- de la coordination des actions de sécurité,
- du suivi des incidents,
- de la communication avec l'Établissement (RSSI, DPO, équipes techniques),
- de la validation des interventions ou changements impactant la sécurité.

3.2 Plan d'Assurance Sécurité (PAS)

Le prestataire doit élaborer, maintenir et tenir à disposition de l'Établissement un Plan d'Assurance Sécurité contenant au minimum :

- les mesures techniques et organisationnelles mises en œuvre,
- les procédures internes de sécurité,
- les processus d'escalade,
- la gestion des incidents,
- la gestion des changements,
- les contrôles internes effectués.

Le PAS doit être mis à jour à chaque évolution significative du service ou de l'architecture.

3.3 Sous-traitance

Toute sous-traitance impliquant un accès aux données ou systèmes de l'Établissement doit se faire dans les conditions légales applicables et notamment :

- doit être notifiée avant mise en œuvre,
- doit être soumise à validation écrite de l'Établissement,
- doit appliquer les mêmes exigences de sécurité que celles imposées au prestataire principal.

Le prestataire reste pleinement responsable des actions et manquements de ses sous-traitants.

3.4 Sécurité de la chaîne d'approvisionnement logicielle

Le prestataire doit maîtriser les risques liés aux composants logiciels tiers intégrés dans les solutions fournies ou opérées pour l'Établissement.

- Le prestataire doit maintenir un **inventaire à jour des composants logiciels tiers** utilisés (bibliothèques, frameworks, modules open source, outils d'infrastructure), formalisé sous la forme d'une **liste des composants logiciels (SBOM — Software Bill of Materials)**,
- Cet inventaire doit être transmis à l'Établissement sur demande, notamment en cas d'incident ou d'audit,
- Le prestataire doit assurer une veille active sur les vulnérabilités affectant ses composants tiers (CVE, bulletins CERT-FR, avis éditeurs) et appliquer les correctifs selon les délais définis à la section « Gestion des vulnérabilités »,
- Les composants tiers doivent provenir de sources officielles et vérifiées ; l'intégrité des artefacts téléchargés doit être contrôlée (signature, empreinte cryptographique),
- Le prestataire doit s'assurer que les composants utilisés sont activement maintenus ; tout composant en fin de vie (EOL) doit être remplacé dans les meilleurs délais.

3.5 Confidentialité

Le prestataire et ses éventuels sous-traitants sont soumis à :

- une obligation stricte de confidentialité,
- un engagement de non-divulgation,
- l'interdiction d'utiliser les données ou informations de l'Établissement à d'autres fins que celles prévues au contrat.

Cette obligation s'applique pendant toute la durée du marché ou contrat et au-delà de son échéance.

3.6 Sensibilisation et formation à la cybersécurité

Le prestataire doit s'assurer que l'ensemble des personnels intervenant dans le cadre de la prestation dispose d'un niveau de sensibilisation adapté aux risques cybersécurité.

3.7 Schéma d'escalade en cas d'incident

Le prestataire doit disposer d'un processus d'escalade clair en cas d'incident de sécurité, précisant :

- les contacts opérationnels du prestataire en cas d'incident,
- les modalités d'alerte et d'escalade selon la gravité,
- les rôles de chacun lors de la gestion d'incident (analyse, confinement, remédiation),
- les points de contact à activer côté établissement (RSSI, DPO, équipes techniques),
- les délais attendus pour les premières actions.

4. Gestion des identités et des accès

Le prestataire doit mettre en œuvre une gestion rigoureuse des identités et des accès afin de garantir la confidentialité, l'intégrité et la disponibilité des systèmes et données de l'Établissement. Les exigences suivantes s'appliquent à l'ensemble des environnements (production, test, administration, cloud, API, SaaS, etc.).

4.1 Comptes nominatifs

- Tous les accès doivent être associés à des comptes nominatifs.
- Les comptes génériques ou partagés sont interdits, sauf exception dûment justifiée et validée par l'Établissement.

4.2 Authentification multifacteur (MFA)

Le MFA est obligatoire pour :

- les comptes administrateurs,
- les accès distants,
- les interfaces d'administration ou consoles techniques.

4.3 Politique de mots de passe

Le prestataire doit appliquer une politique de mots de passe robuste sur l'ensemble des comptes utilisés dans le cadre de la prestation.

- Les mots de passe doivent respecter une **longueur minimale de 12 caractères**, combinant majuscules, minuscules, chiffres et caractères spéciaux.
- Les **mots de passe par défaut** des équipements, applications et comptes de service doivent être modifiés avant toute mise en production.
- La **réutilisation des anciens mots de passe** est interdite (historique minimum de 10 mots de passe).
- Les mots de passe ne doivent jamais être stockés en clair ; ils doivent être hachés avec un algorithme reconnu (bcrypt, Argon2 ou équivalent).
- En cas de suspicion de compromission, le mot de passe concerné doit être réinitialisé immédiatement.
- Ces exigences s'appliquent également aux comptes de service et aux comptes techniques.

4.4 Principe du moindre privilège

- Les droits d'accès doivent être limités au strict nécessaire, en fonction des rôles et responsabilités.
- Le prestataire doit pouvoir démontrer le respect de ce principe.

4.5 Revue périodique des droits

Une revue complète des droits d'accès doit être réalisée tous les 6 mois, incluant :

- les comptes utilisateurs,
- les comptes administrateurs,
- les accès API,
- les accès aux environnements techniques.

Le prestataire doit fournir les résultats de cette revue sur demande de l’Établissement.

4.6 Gestion des comptes inactifs

- Tout compte inactif depuis 90 jours doit être désactivé ou supprimé.
- Les comptes d'anciens collaborateurs doivent être désactivés immédiatement après départ.

4.7 Gestion des secrets et des clés d'accès

Le prestataire doit mettre en œuvre une politique stricte de gestion des secrets techniques utilisés dans le cadre de la prestation (clés API, tokens, mots de passe techniques, certificats, clés de chiffrement, credentials de service).

- Les secrets doivent être stockés dans un coffre-fort de secrets dédié (ex. : HashiCorp Vault, AWS Secrets Manager, Azure Key Vault ou équivalent), et non dans des fichiers de configuration, variables d'environnement non protégées ou dépôts de code.
- Aucun secret ne doit apparaître en clair dans le code source, les scripts, les logs ou les systèmes de gestion de version.
- Les secrets doivent faire l'objet d'une rotation régulière, selon une fréquence adaptée à leur criticité et au minimum annuellement.
- Les accès aux secrets doivent être nominatifs, journalisés et limités au strict nécessaire.
- En cas de suspicion de compromission d'un secret, celui-ci doit être révoqué immédiatement et l'Établissement notifié sans délai.
- À la fin du contrat, l'ensemble des secrets liés à l'Établissement doit être révoqué et supprimé.

5. Sécurité des systèmes et du réseau

Le prestataire doit garantir un niveau de sécurité élevé sur l'ensemble des infrastructures, systèmes et composants réseaux utilisés pour fournir ou opérer le service. Les exigences suivantes s'appliquent à tous les environnements (on-premise, cloud, hybride, SaaS).

5.1 Segmentation des environnements

- Les environnements production, test/recette et administration doivent être strictement séparés.
- Aucun accès transversal non justifié ne doit être autorisé entre ces environnements.
- Les jeux de données utilisés en test/recette doivent être anonymisés.

5.2 Filtrage et exposition Internet

- Tout accès direct Internet vers les serveurs de l'Établissement est strictement interdit.
- Les flux entrants et sortants doivent être filtrés, tracés et maîtrisés.
- Toute exposition publique (API, services web) doit être déclarée et validée par l'Établissement.

5.3 Chiffrement des communications et des données

- Toutes les communications doivent être sécurisées par TLS 1.2 ou supérieur.
- Les données au repos doivent être protégées par un chiffrement AES-256 ou équivalent.
- Les clés de chiffrement doivent être gérées de manière sécurisée (accès restreint, rotation, stockage protégé).

5.4 Accès administratifs

Les accès d'administration doivent obligatoirement passer par :

- un VPN sécurisé, ou
- une solution ZTNA validée par l'Établissement.

Les accès administrateurs doivent être nominatifs, tracés et protégés par MFA.

5.5 Journalisation, horodatage et synchronisation

Tous les systèmes doivent être configurés pour journaliser les événements critiques :

- connexions, actions administratives, accès sensibles, erreurs système.

Les journaux doivent être horodatés via une source NTP synchronisée et conservés pour une durée minimale de 6 mois.

6. Supervision et détection

Le prestataire doit mettre en place des mécanismes de supervision et de détection permettant d'identifier rapidement toute activité suspecte ou tout incident de sécurité.

6.1 Protection des postes et serveurs

Chaque système (serveur, VM, instance cloud, poste technique, conteneur critique) doit être équipé :

- d'un EDR et d'un antivirus à jour,
- avec une configuration conforme à l'état de l'art.

Les incidents détectés doivent être analysés et traités sans délai.

6.2 Alertes de sécurité

Toute alerte critique émise par l'EDR, le SIEM, l'IDS/IPS ou tout autre outil de supervision doit être :

- transmise immédiatement à l'Établissement,
- accompagnée des éléments nécessaires à l'analyse (horodatage, source, impact, mesures prises).

6.3 Journalisation et conservation des logs

Les journaux doivent couvrir au minimum :

- connexions utilisateurs,
- actions administratives,
- tentatives d'accès non autorisées,
- modifications sur les systèmes.

Les logs doivent être horodatés (NTP), protégés contre toute modification et conservés au moins 6 mois.

7. Gestion des vulnérabilités et mises à jour

Le prestataire doit mettre en place un processus formalisé de gestion des vulnérabilités permettant d'identifier, d'évaluer et de corriger rapidement les failles de sécurité.

7.1 Délais d'application des correctifs

Les correctifs doivent être appliqués selon la criticité (CVSS) et conformément aux recommandations du CERT-FR. Les délais démarrent à compter de la mise à disposition du patch par l'éditeur.

Priorité (CVSS)	Définition	Délai d'application
Critique (≥ 9.0)	Vulnérabilité critique, souvent exploitée ou exploitable à distance	48 h à 7 jours max.
Haute (7.0–8.9)	Risque important nécessitant une action rapide	30 jours max
Moyenne (4.0–6.9)	Vulnérabilité modérée	60 jours max
Faible (0–3.9)	Risque faible, impact limité	Cycle normal de maintenance

7.2 Exigences complémentaires

7.2.1 Rapports de correctifs

Le prestataire doit fournir sur demande un rapport contenant la liste des correctifs appliqués, leur date d'installation, les vulnérabilités corrigées et leur criticité, ainsi que le périmètre concerné.

7.2.2 Scans de vulnérabilités

Le prestataire réalise des scans réguliers de vulnérabilités (infrastructure, applicatif, API) ainsi qu'après chaque mise à jour majeure. Un rapport de scan peut être transmis à l'Établissement sur demande.

8. Sécurité applicative et développement sécurisé

Le prestataire réalisant des développements logiciels pour l'Établissement doit intégrer la sécurité à chaque étape du cycle de développement.

8.1 Cycle de développement sécurisé (Secure SDLC)

Le prestataire doit appliquer les bonnes pratiques de développement sécurisé, notamment celles définies par l'OWASP et les guides de l'ANSSI.

- Les exigences de sécurité doivent être définies dès la phase de conception.
- Une revue de sécurité doit être réalisée avant toute mise en production.
- Les développeurs doivent être sensibilisés aux vulnérabilités applicatives courantes.

8.2 Analyse du code et tests de sécurité

- **Analyse statique (SAST)** : analyse automatisée du code source pour détecter les vulnérabilités avant compilation ou déploiement.
- **Analyse dynamique (DAST)** : tests de sécurité sur l'application en cours d'exécution.
- **Revue de code** : tout composant sensible ou exposé doit faire l'objet d'une revue par un pair ou un référent sécurité.

Ces analyses doivent être réalisées à chaque version majeure et sur demande de l'Établissement.

8.3 Gestion des dépendances tierces

- Le prestataire doit maintenir à jour l'inventaire des bibliothèques et composants tiers utilisés.
- Les dépendances présentant des vulnérabilités connues (CVE) doivent être mises à jour selon les délais définis à la section 7.

- Le prestataire doit être en mesure de fournir une liste des composants logiciels (SBOM) sur demande.

8.4 Sécurisation de la chaîne CI/CD

- Les pipelines CI/CD doivent être sécurisés et accessibles uniquement aux personnes autorisées.
- Les accès aux outils de build, dépôts de code et registres d'artefacts doivent être contrôlés et journalisés.
- Aucun secret, credential ou clé API ne doit être intégré en clair dans le code source ou les scripts de déploiement.

9. Sauvegardes et continuité

Le prestataire doit garantir la protection, la disponibilité et la capacité de restauration des données et services de l'Établissement, y compris en situation d'incident majeur.

9.1 Exigences de sauvegarde

Le prestataire doit mettre en œuvre des mécanismes de sauvegarde permettant de se prémunir contre les risques de compromission, notamment en cas d'attaque de type ransomware.

- Les sauvegardes doivent inclure au moins une sauvegarde **hors ligne ou isolée**, déconnectée du système principal, protégée de toute altération ou suppression.
- Les accès aux systèmes de sauvegarde doivent être strictement contrôlés (authentification forte, journalisation).
- Les mécanismes de sauvegarde doivent être protégés contre toute suppression ou modification malveillante.

9.2 Tests de restauration

La mise en œuvre de sauvegardes ne suffit pas à garantir la capacité de reprise. Le prestataire doit s'assurer régulièrement que les données sauvegardées sont effectivement restaurables et intègres.

- Un test de restauration complet doit être réalisé au minimum une fois par an, portant sur l'ensemble des données et systèmes critiques.
- Des tests partiels doivent être réalisés au minimum tous les 6 mois.
- Chaque test doit faire l'objet d'un rapport documenté précisant la date, le périmètre, le résultat et les actions correctives éventuelles.
- Ces rapports doivent être transmis à l'Établissement sur demande ou lors du bilan semestriel.
- En cas d'échec d'un test, l'Établissement doit en être informé sans délai et un plan de remédiation fourni.

9.3 Exigences de continuité d'activité

Le prestataire doit disposer d'un PRA/PCA intégrant explicitement les scénarios de cyberattaque (ex. : ransomware, compromission, perte d'intégrité). Les mécanismes de reprise doivent garantir l'intégrité des données restaurées et l'absence de compromission persistante. Les plans doivent être testés régulièrement.

10. Gestion des incidents

Le prestataire doit disposer d'un dispositif permettant de détecter, analyser et traiter rapidement tout incident de sécurité susceptible d'impacter les systèmes, services ou données de l'Établissement.

10.1 Notification des incidents

Tout incident de sécurité, suspicion d'incident ou tentative d'accès illicite doit être signalé à l'Établissement dans un délai maximum de 24 heures après sa détection.

La notification doit être adressée au RSSI et au DPO de l'Établissement, selon les coordonnées communiquées en début de prestation.

La notification doit contenir :

- une description de l'incident,
- l'impact constaté ou potentiel,
- les actions correctives engagées ou prévues,
- le contact technique pour le suivi.

10.2 Rapport d'incident

Un rapport complet doit être transmis dans un délai de 72 heures après la notification, incluant :

- la nature de l'incident,
- l'impact réel ou potentiel,
- les mesures correctives mises en œuvre ou planifiées,
- les éléments techniques utiles à l'analyse.

10.3 Collaboration

Le prestataire doit collaborer pleinement avec l'Établissement lors des investigations. Il doit fournir l'accès aux informations nécessaires, faciliter les analyses et participer aux actions de remédiation.

11. Audit et contrôle

L'Établissement se réserve le droit de procéder à des audits de sécurité visant à vérifier la conformité du prestataire aux exigences techniques, organisationnelles et réglementaires applicables.

11.1 Audits programmés

L'Établissement peut réaliser, ou faire réaliser par un tiers mandaté, des audits techniques (infrastructures, configurations, sécurité applicative), organisationnels (processus, gouvernance, gestion des accès) ou réglementaires (RGPD, sécurité des données). Ces audits sont programmés avec un préavis raisonnable et en coordination avec le prestataire.

11.2 Contrôles et tests d'intrusion

L'Établissement peut faire réaliser des contrôles de conformité ou des tests d'intrusion, incluant des tests portant sur la posture externe du prestataire ou des contrôles destinés à vérifier l'efficacité des mécanismes de détection. La portée, les modalités et les limites des tests sont définies dans le cadre contractuel.

11.3 Livrables attendus du prestataire

Le prestataire fournit à l'Établissement les éléments nécessaires au suivi de la sécurité du service :

- **Annuellement :** Un rapport de conformité et les preuves de certifications (ex. : ISO 27001, SecNumCloud).
- **Semestriellement (ou sur demande) :** Un bilan détaillant les incidents de sécurité, les correctifs appliqués, l'état des sauvegardes/restaurations et l'évolution des accès.

12. Fin de contrat

À la fin du marché ou contrat ou sur demande de l'Établissement, le prestataire doit garantir une réversibilité complète et sécurisée des données et des accès liés au service fourni.

12.1 Restitution et destruction des données

Les données de l'Établissement doivent être restituées intégralement dans un format standard et exploitable. Toutes les copies résiduelles doivent être supprimées, y compris les environnements de test, préproduction, exports techniques et jeux d'essai. Les journaux contenant des données de l'Établissement doivent également être supprimés.

12.2 Délai maximal d'effacement

L'ensemble des données, sauvegardes, journaux, secrets et copies techniques appartenant à l'Établissement doit être supprimé dans un « délai maximal de 30 jours calendaires » à compter de la date de fin effective du contrat ou marché ou de la demande formelle de l'Établissement.

- À l'issue de ce délai, le prestataire fournit une attestation d'effacement confirmant la suppression complète.
- Si des contraintes techniques ou légales imposent une conservation temporaire au-delà de ce délai, le prestataire doit en informer l'Établissement par écrit en justifiant la durée résiduelle et les mesures de protection associées.
- Passé le délai de 30 jours, aucune donnée de l'Établissement ne peut être conservée sous quelque forme que ce soit.

12.3 Attestation d'effacement

Le prestataire fournit une attestation d'effacement confirmant la suppression des données de l'Établissement. Cet effacement doit couvrir les données, sauvegardes, journaux et copies techniques. L'Établissement peut demander un contrôle ou un audit afin de vérifier l'effacement complet.

12.4 Suppression des accès

- Tous les comptes, accès, droits et identifiants créés pour l'Établissement doivent être supprimés.
- La suppression doit être tracée : le prestataire doit fournir une preuve de suppression des accès (journal d'audit ou équivalent).
- Toutes les clés API, tokens, certificats et secrets utilisés pour l'Établissement doivent être révoqués.

12.5 Interdiction de réutilisation

Le prestataire ne doit pas réutiliser les données de l'Établissement pour d'autres clients, des environnements internes, des jeux d'essai ou des environnements de développement.

13. Sanctions et clauses

En cohérence avec les bonnes pratiques de gestion des risques, les mesures suivantes peuvent être mises en œuvre en cas de non-conformité de sécurité.

13.1 Mesures graduelles et proportionnées

En cas de non-conformité, l'Établissement peut demander au prestataire de mettre en place des actions correctives, de fournir un plan de remédiation ou d'appliquer des mesures temporaires de réduction du risque. L'objectif est d'encourager un retour à la conformité dans les meilleurs délais, dans un esprit de coopération.

13.2 Suspension temporaire des accès

Si un risque important pour la sécurité du SI est avéré, et conformément au principe de réduction immédiate de la surface d'attaque (ANSSI), l'Établissement peut suspendre temporairement certains accès techniques le temps d'éliminer le risque.

13.3 Notification aux autorités compétentes

En cas d'écarts significatifs ou répétés, l'Établissement peut saisir les autorités compétentes (CERT ministériel, ANSSI) conformément aux bonnes pratiques nationales de gestion des risques fournisseurs. Cette étape peut être déclenchée lorsque le prestataire ne répond pas aux sollicitations de sécurité, que les actions correctives ne sont pas mises en œuvre, ou qu'un risque important demeure malgré les alertes de l'Établissement.

13.4 Application des dispositions contractuelles

Si les actions correctives ne sont pas mises en œuvre ou si les manquements se répètent, les dispositions prévues au contrat peuvent être appliquées, notamment les pénalités ou, en dernier recours, la résiliation du marché ou contrat pour non-conformité de sécurité.

14. Suivi et révision

Ce document fait l'objet de mises à jour régulières afin de garantir son alignement avec les évolutions réglementaires, techniques et organisationnelles.