



## Sécurité SI du CMN

### Annexe 4 AE-CCAP - Cybersécurité

Document applicable dans le cadre du marché Installation d'une solution de comptage de la fréquentation et services associés pour les monuments du Centre des Monuments Nationaux

Réf : MSIC-2511070956

|                                |                                                        |      |         |      |
|--------------------------------|--------------------------------------------------------|------|---------|------|
| CENTRE DES MONUMENTS NATIONAUX | Annexe 4 AE-CCAP - Cybersécurité<br>Sécurité SI du CMN | Réf. | Version | Page |
|                                |                                                        |      | 1.0.    | 2/11 |

## 1 Objet et périmètre

Ce document définit les exigences minimales de cybersécurité applicables à tout prestataire intervenant sur le système d'information du CMN ou traitant des données appartenant au CMN, quels que soient :

- Le type de prestation (hébergement, développement, maintenance, infogérance, support, audit, etc.),
- Le mode de mise en œuvre (API, SaaS, plateforme web, billetterie, 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 du CMN,
- Et s'inscrivent dans le cadre de la Politique de Sécurité des Systèmes d'Information (PSSI) du CMN.

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 au CMN 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 :

### 2.1.1 Règlement européen NIS2 (UE 2022/2555)

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

### 2.1.2 Référentiels et guides de l'ANSSI

PGSSI-S, guides techniques, bonnes pratiques de sécurisation, durcissement et supervision.

### 2.1.3 Normes ISO/IEC 27001 et 27002

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

### 2.1.4 OWASP Top 10

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

### 2.1.5 CIS Benchmarks

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

### 2.1.6 RGS et RGPD (UE 2016/679)

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

|                                |                                                        |      |         |      |
|--------------------------------|--------------------------------------------------------|------|---------|------|
| CENTRE DES MONUMENTS NATIONAUX | Annexe 4 AE-CCAP - Cybersécurité<br>Sécurité SI du CMN | Réf. | Version | Page |
|                                |                                                        |      | 1.0.    | 3/11 |

Ces référentiels constituent la base de contrôle à utiliser par le CMN pour évaluer la conformité des prestataires.

## 3 Gouvernance et responsabilité

Le prestataire est responsable de la mise en œuvre et du maintien d'un niveau de sécurité conforme aux exigences du CMN. 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 du CMN.

- De la coordination des actions de sécurité,
- Du suivi des incidents,
- De la communication avec le CMN (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 du CMN 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 du CMN :

- Doit être notifiée avant mise en œuvre,
- Doit être soumise à validation écrite du CMN,
- 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 Confidentialité

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

- Une obligation stricte de confidentialité,
- Un engagement de non-divulgateion,
- L'interdiction d'utiliser les données ou informations du CMN à d'autres fins que celles prévues au contrat.

Cette obligation s'applique pendant toute la durée du marché et au-delà de sa résiliation.

|                                |                                                        |      |         |      |
|--------------------------------|--------------------------------------------------------|------|---------|------|
| CENTRE DES MONUMENTS NATIONAUX | Annexe 4 AE-CCAP - Cybersécurité<br>Sécurité SI du CMN | Réf. | Version | Page |
|                                |                                                        |      | 1.0.    | 4/11 |

### 3.5 Schéma d'escalade en cas d'incident

Le prestataire doit disposer d'un processus d'escalade clair en cas d'incident de sécurité. Ce processus doit permettre d'identifier rapidement les interlocuteurs responsables et d'assurer une coordination efficace avec le CMN.

Il doit préciser :

- 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 CMN (MSIC, RSSI, DPO),
- Les délais attendus pour les premières actions.

L'objectif est d'assurer une réaction rapide et structurée, en garantissant la continuité des échanges entre le CMN et le prestataire.

## 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 du CMN. 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 le CMN.
- 

### 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 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.

Revue périodique des droits

- Une revue complète des droits d'accès doit être réalisée tous les 6 mois, incluant :
  - Comptes utilisateurs,
  - Comptes administrateurs,
  - Accès API,
  - Accès aux environnements techniques.
- Le prestataire doit fournir les résultats de cette revue sur demande du CMN.

### 4.4 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.

|                                |                                                        |      |         |      |
|--------------------------------|--------------------------------------------------------|------|---------|------|
| CENTRE DES MONUMENTS NATIONAUX | Annexe 4 AE-CCAP - Cybersécurité<br>Sécurité SI du CMN | Réf. | Version | Page |
|                                |                                                        |      | 1.0.    | 5/11 |

## 5 Sécurité des systèmes et du réseau

Le prestataire doit garantir un niveau de sécurité élevé sur l'ensemble des infrastructures, systèmes, environnements et composants réseaux utilisés pour fournir ou opérer le service du CMN. 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 du CMN 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 le CMN.

### 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 le CMN.
- Les accès administrateurs doivent être :
  - Nominatifs,
  - Tracés,
  - 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.
- Ils doivent être conservés pour une durée conforme aux exigences du CMN (minimum 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 pouvant affecter les systèmes ou les données du CMN.

## 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 au CMN,
  - 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 (Network Time Protocol)),
  - Protégés contre toute modification,
  - 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 susceptibles d'affecter les systèmes ou données du CMN.

## 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 d'application des correctifs démarrent à compter de la mise à disposition du patch par l'éditeur ou du correctif de sécurité publié.

| Priorité (CVSS)   | Définition                                                          | Délai d'application                                                           |
|-------------------|---------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Critique (≥ 9.0)  | Vulnérabilité critique, souvent exploitée ou exploitable à distance | 48 h à 7 jours max. Application « dans les plus brefs délais » selon CERT-FR. |
| 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                                        | Intégrée au cycle normal de maintenance                                       |

Les systèmes exposés à Internet, les applications critiques et les composants utilisés pour l'authentification doivent être corrigés en priorité.

Le prestataire doit assurer un suivi continu des vulnérabilités et garantir l'application des mises à jour de sécurité dans des délais adaptés à leur criticité, sur l'ensemble des composants du

|                                |                                                        |      |         |      |
|--------------------------------|--------------------------------------------------------|------|---------|------|
| CENTRE DES MONUMENTS NATIONAUX | Annexe 4 AE-CCAP - Cybersécurité<br>Sécurité SI du CMN | Réf. | Version | Page |
|                                |                                                        |      | 1.0.    | 7/11 |

système d'information, y compris les équipements matériels, objets connectés et capteurs déployés.

## 7.2 Exigences complémentaires

### Rapports de correctifs

Le prestataire doit être en mesure de fournir, sur demande du CMN, un rapport contenant :

- La liste des correctifs appliqués,
- La date d'installation,
- Les vulnérabilités corrigées et leur criticité,
- Le périmètre concerné.

### Scans de vulnérabilités

Le prestataire réalise :

- Des scans réguliers de vulnérabilités (infrastructure, applicatif, API),
- Des scans après chaque mise à jour majeure,
- L'analyse des résultats et le traitement des vulnérabilités détectées.

Un rapport de scan peut être transmis au CMN sur demande.

## 8 Sauvegardes et continuité

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

Les exigences détaillées liées aux modalités opérationnelles de sauvegarde, de rétention et de continuité sont définies dans le cahier des charges (CCTP / CCP).

Le présent document précise uniquement les exigences complémentaires de sécurité.

### 8.1 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.

À ce titre :

- Les sauvegardes doivent inclure au moins une sauvegarde immuable, non modifiable et protégée contre toute altération ou suppression.
- Les sauvegardes doivent inclure au moins une sauvegarde hors ligne ou isolée, déconnectée du système principal.
- 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.

### 8.2 Exigences de continuité d'activité

Les paramètres opérationnels de continuité (RPO, RTO, modalités de reprise) sont définis dans le cahier des charges (CCTP / CCP).

D'un point de vue cybersécurité, le prestataire doit garantir la résilience du service face aux incidents de sécurité.

À ce titre :

- 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 :

|                                |                                                        |      |         |      |
|--------------------------------|--------------------------------------------------------|------|---------|------|
| CENTRE DES MONUMENTS NATIONAUX | Annexe 4 AE-CCAP - Cybersécurité<br>Sécurité SI du CMN | Réf. | Version | Page |
|                                |                                                        |      | 1.0.    | 8/11 |

- L'intégrité des données restaurées
- L'absence de compromission persistante
- Les plans doivent être testés régulièrement (tests techniques ou exercices).
- Les procédures doivent inclure la gestion de crise et la communication avec le CMN.

## 9 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 du CMN.

### 9.1 Notification des incidents

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

La notification doit être envoyée à :

- [rssi@monuments-nationaux.fr](mailto:rssi@monuments-nationaux.fr)
- [donneespersonnelles@monuments-nationaux.fr](mailto:donneespersonnelles@monuments-nationaux.fr)

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.

### 9.2 Rapport d'incident

Un rapport complet doit être transmis dans un délai de 72 heures après la notification.

Il doit inclure :

- 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.

### 9.3 Collaboration

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

## 10 Audit et contrôle

Le CMN 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.

### 10.1 Audits programmés

Le CMN peut réaliser, ou faire réaliser par un tiers mandaté, des audits :

- Techniques (infrastructures, configurations, sécurité applicative),
- Organisationnels (processus, gouvernance, gestion des accès, gestion des incidents),
- Ou réglementaires (RGPD, sécurité des données).

|                                |                                                        |      |         |      |
|--------------------------------|--------------------------------------------------------|------|---------|------|
| CENTRE DES MONUMENTS NATIONAUX | Annexe 4 AE-CCAP - Cybersécurité<br>Sécurité SI du CMN | Réf. | Version | Page |
|                                |                                                        |      | 1.0.    | 9/11 |

Ces audits sont programmés selon un préavis raisonnable et en coordination avec le prestataire.

## 10.2 Contrôles inopinés et tests d'intrusion

Le CMN peut faire réaliser des contrôles de conformité ou des tests d'intrusion dans le cadre de l'évaluation du niveau de sécurité fourni par le prestataire.

Ces actions peuvent inclure :

- Des tests techniques portant sur la posture externe du prestataire (tests de type « boîte noire »),
- Des contrôles destinés à vérifier l'efficacité des mécanismes de détection et de réponse (supervision, alerting, SOC).

Lorsque ces tests peuvent avoir un impact opérationnel, le prestataire en est informé dans des conditions adaptées, permettant d'assurer la coordination nécessaire. La portée, les modalités et les limites des tests sont définies dans le cadre contractuel afin de garantir la sécurité, la légalité et la continuité de service.

## 10.3 Informations et livrables attendus du prestataire

Le prestataire fournit au CMN les éléments nécessaires au suivi de la sécurité du service. Ces rapports portent exclusivement sur le périmètre de la prestation et incluent :

- **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.

La fourniture de ces documents n'implique pas l'accès aux informations internes propriétaires du prestataire.

## 11 Fin de contrat

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

Ces exigences portent exclusivement sur la protection, la suppression et la traçabilité des données du CMN sous l'angle cybersécurité.

### 11.1 Restitution et destruction des données

Les données du CMN doivent être restituées intégralement dans un format standard et exploitable.

Toutes les **copies résiduelles** doivent être supprimées, y compris :

- Environnements de test
- Préproduction,
- Exports techniques,
- Jeux d'essai.

**Les journaux contenant des données du CMN** doivent également être supprimés : même si la donnée principale est effacée, elle peut rester visible dans les logs, ce qui crée un risque de fuite.

|                                |                                                        |      |         |       |
|--------------------------------|--------------------------------------------------------|------|---------|-------|
| CENTRE DES MONUMENTS NATIONAUX | Annexe 4 AE-CCAP - Cybersécurité<br>Sécurité SI du CMN | Réf. | Version | Page  |
|                                |                                                        |      | 1.0.    | 10/11 |

## 11.2 Attestation d'effacement

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

## 11.3 Suppression des accès

- Tous les comptes, accès, droits et identifiants créés pour le CMN 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 le CMN doivent être révoqués.

## 11.4 Délai maximal d'effacement

- Un délai maximal d'effacement doit être défini.

## 11.5 Interdiction de réutilisation

Le prestataire ne doit pas réutiliser les données du CMN pour :

D'autres clients, des environnements internes, des jeux d'essai, des environnements de développement.

# 12 Sanctions et clauses

En cohérence avec les bonnes pratiques de gestion des risques précisées exclusivement dans le présent document, les mesures suivantes peuvent être mises en œuvre en cas de non-conformité de sécurité :

## 12.1 Mesures graduelles et proportionnées

En cas de non-conformité, le CMN 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.

## 12.2 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), le CMN peut suspendre temporairement certains accès techniques le temps d'éliminer le risque.

|                                |                                                        |      |         |       |
|--------------------------------|--------------------------------------------------------|------|---------|-------|
| CENTRE DES MONUMENTS NATIONAUX | Annexe 4 AE-CCAP - Cybersécurité<br>Sécurité SI du CMN | Réf. | Version | Page  |
|                                |                                                        |      | 1.0.    | 11/11 |

## 12.3 Notification aux autorités compétentes

En cas d'écarts significatifs ou répétés aux règles de sécurité, et conformément aux obligations internes du CMN :

- Le CMN peut saisir le CERT du Ministère de la Culture, qui suit les incidents de sécurité impliquant les prestataires et leurs niveaux de conformité.
- Si la situation le justifie, certains manquements graves peuvent également être signalés à l'ANSSI, conformément aux bonnes pratiques nationales de gestion des risques fournisseurs.

Cette étape n'est pas systématique, mais elle peut être déclenchée lorsque :

- le prestataire ne répond pas aux sollicitations de sécurité,
  - les actions correctives ne sont pas mises en œuvre,
  - un risque important demeure malgré les alertes du CMN.
- L'objectif est d'assurer un niveau de sécurité conforme aux exigences de l'État et de garantir que le fournisseur traite les sujets de sécurité avec la réactivité nécessaire.

## 12.4 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 contractuelles du CCP,

Ou, en dernier recours, la résiliation du marché pour non-conformité de sécurité.

## 13 Suivi et révision

Ce document fait l'objet d'une mise à jour annuelle afin de garantir l'alignement avec les évolutions réglementaires, techniques et organisationnelles.

La révision est réalisée par le RSSI du CMN, en coordination avec la Direction des Systèmes D'Information (MSIC) et le DPO.