CENTRE DES MONUMENTS NATIONAUX	**Sécurité SI du CMN**

Exigences Cybersécurité CMN

Document applicable au titulaire du marché de maintenance des équipements informatiques billetterie, boutique et contrôle d'accès.

Réf : MSIC-230920262

Confidentialité : Diffusion Restreinte

Version: 1.0

Date : 23/09/26

Nombre de pages : 7

Historique des versions

Date	Version	Auteur	Evolutions
13/09/2026	1.0	Gueddou Smail	Création

1 Objet et périmètre

Ce document définit les exigences minimales de cybersécurité applicables au titulaire du marché de maintenance des équipements informatiques de billetterie, boutique et contrôle d'accès du CMN.
Il couvre l'ensemble des prestations du marché, notamment :

- Le help-desk et la télémaintenance (prise de main à distance, télédistribution),
- Les interventions sur site et en atelier,
- La préparation des matériels et la gestion des masters,
- La logistique, le stockage et la sortie du parc des matériels,
- La maintenance des équipements monétiques et des abonnements associés.

Ces exigences s'appliquent pendant toute la durée du marché, y compris la phase d'implémentation et la réversibilité.
Elles complètent :

- Les obligations légales (notamment RGPD),
- Les obligations contractuelles (CCAP, CCTP, annexe 2 RGPD),
- 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 titulaire, qui doivent respecter un niveau équivalent d'exigences de sécurité.

2 Référentiels

Les exigences définies dans ce document s'appuient sur les normes, réglementations et bonnes pratiques reconnues. Elles constituent un référentiel d'inspiration, sans imposer l'application exhaustive de l'ensemble des standards cités.

Les principaux référentiels applicables sont :

- **Référentiels et guides de l'ANSSI**
  Bonnes pratiques de sécurisation, durcissement, accès à distance, gestion des supports.
- **Normes ISO/IEC 27001 et 27002**
  Management de la sécurité de l'information, mesures organisationnelles et techniques.
- **CIS Benchmarks**
  Durcissement des systèmes d'exploitation et des masters.
- **NIST SP 800-88**
  Effacement sécurisé et destruction des supports de stockage.
- **PCI-DSS et exigences du GIE CB**
  Sécurité des équipements et flux monétiques.
- **RGS et RGPD (UE 2016/679)**
  Sécurisation des traitements, protection des données personnelles.

3 Gouvernance et responsabilité

Le titulaire est responsable de la mise en œuvre et du maintien d'un niveau de sécurité conforme aux exigences du CMN. Conformément au CCTP, il est garant de la sécurité des systèmes inscrits au parc à maintenir.

3.1 Référent sécurité

Le titulaire désigne un point de contact sécurité, disponible en cas d'incident ou de demande urgente du CMN, en charge :

- De la coordination des actions de sécurité,
- Du suivi des incidents,
- De la communication avec le CMN (RSSI, DPO, équipes techniques).

3.2 Plan d'Assurance Sécurité (PAS)

Le titulaire remet un Plan d'Assurance Sécurité dans les 3 mois suivant la notification du marché. Il décrit au minimum :

- L'organisation et les outils de télémaintenance,
- La gestion et la protection des masters,
- Les procédures d'effacement et de destruction des supports,
- Les conditions de stockage et de transport des matériels,
- La gestion des incidents et le processus d'escalade.

Le PAS est mis à jour à chaque évolution significative de l'organisation ou des outils.

3.3 Sous-traitance

Toute sous-traitance impliquant un accès aux matériels, données ou systèmes du CMN (help-desk, interventions sur site, atelier, transport) :

- 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 titulaire.

Tout recours à un service de help-desk ou de télémaintenance opéré hors de l'Union européenne est soumis à l'accord préalable du CMN.

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

3.4 Confidentialité

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

- Une obligation stricte de confidentialité,
- L'interdiction d'utiliser les données ou informations du CMN (données présentes sur les matériels, masters, configurations, documentation) à d'autres fins que celles prévues au marché.

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

4 Gestion des identités et des accès

Le titulaire met en œuvre une gestion rigoureuse des identités et des accès pour l'ensemble des outils et systèmes utilisés dans le cadre du marché : outils de télémaintenance, portails monétiques, portail GLPI du CMN, outil de gestion du parc.

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 accès aux outils de télémaintenance,
  - Les consoles et portails d'administration (monétique, gestion du parc),
  - Tout accès distant aux systèmes du CMN.

4.3 Principe du moindre privilège

- Les droits d'accès sont limités au strict nécessaire, en fonction des missions de chaque intervenant.
- Le titulaire tient à jour la liste nominative des intervenants habilités (help-desk, techniciens, atelier) et la transmet au CMN sur demande.
- Une revue des habilitations est réalisée tous les 6 mois.

4.4 Gestion des départs et des comptes inactifs

- Les accès d'un intervenant quittant le titulaire ou la prestation sont désactivés immédiatement.
- Tout compte inactif depuis 90 jours est désactivé ou supprimé.

4.5 Télémaintenance

- La télémaintenance est réalisée exclusivement avec l'outil en place au CMN ou avec un outil déclaré dans le PAS et validé par le CMN.
- L'installation de tout autre outil de prise de main à distance est interdite.
- Toute prise de main est rattachée à un ticket d'incident ou à une demande du CMN.
- Aucun accès permanent ou non déclaré aux systèmes du CMN n'est autorisé.
- Les sessions sont chiffrées (TLS 1.2 ou supérieur) et tracées : intervenant, date, heure, durée, équipement, numéro de ticket. Ces traces sont conservées au moins 6 mois et transmises au CMN sur demande.
- Les postes des intervenants utilisés pour la télémaintenance sont maintenus à jour et protégés par un antivirus ou EDR actif.

4.6 Télédistribution

- Seuls les logiciels, mises à jour et correctifs fournis par le CMN, par les éditeurs du CMN ou par les constructeurs peuvent être déployés.
- Le titulaire vérifie leur provenance et leur intégrité avant tout déploiement.

5 Sécurité des systèmes du parc

Le titulaire est garant de la sécurité des systèmes inscrits au parc à maintenir (caisses, serveurs, contrôle d'accès, terminaux mobiles, monétique). Les exigences suivantes s'appliquent à la préparation, à la maintenance et à la mise à jour de ces systèmes.

5.1 Masters

- Les masters sont durcis selon les recommandations de l'ANSSI ou les CIS Benchmarks, dans la limite de la compatibilité avec les applications du CMN.
- Les comptes par défaut sont désactivés ou renommés, et leurs mots de passe modifiés.
- Seuls les logiciels validés par le CMN sont intégrés aux masters.
- L'antivirus/EDR retenu par le CMN est intégré et actif sur chaque master.
- Le démarrage sur support externe est désactivé et l'accès au BIOS/UEFI protégé.
- Toute nouvelle version de master est validée par le CMN avant déploiement.

5.2 Protection des masters

- Les masters et leur documentation sont stockés sur des supports chiffrés, dans un lieu sécurisé, avec un accès limité aux intervenants habilités.
- Chaque version est identifiée (numéro de version, date, empreinte SHA-256) et archivée.
- Les masters restent la propriété du CMN et ne peuvent être utilisés pour d'autres clients.

5.3 Comptes d'administration locaux

- Les mots de passe des comptes d'administration locaux sont uniques par équipement lorsque l'environnement le permet (ex. Windows LAPS).
- À défaut, ils sont modifiés à chaque nouveau master et lorsqu'un technicien qui en en avait connaissance quitte la société.
- Ils sont conservés dans un coffre-fort de mots de passe et ne figurent jamais sur les équipements, étiquettes ou comptes rendus d'intervention.

5.4 Antivirus/EDR

- L'agent antivirus/EDR reste actif et relié à la console du CMN en permanence.
- Toute désactivation temporaire nécessaire à une intervention est justifiée, limitée à sa durée et suivie d'une réactivation vérifiée.

5.5 Délais d'application des correctifs

Les correctifs de sécurité (OS, SGBDR, antivirus, firmwares, logiciels monétiques) sont déployés sur le parc selon leur criticité (CVSS) et les recommandations du CERT-FR. Les délais démarrent à la mise à disposition du correctif et, le cas échéant, de la validation de compatibilité par l'éditeur des applications du CMN.

Priorité (CVSS)	**Définition**	**Délai de déploiement sur le parc**
Critique (≥ 9.0)	Vulnérabilité critique, souvent exploitée ou exploitable à distance	7 jours max, ou mesure de contournement validée par le CMN dans l'attente
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 prochain master ou cycle de maintenance

Le titulaire fournit sur demande l'état de déploiement des correctifs par équipement.

5.6 Fin de support

Conformément au CCTP, le titulaire informe le CMN au moins 18 mois avant la fin de support d'un système, d'une version ou d'un agrément, et propose un plan de mise à jour ou de remplacement.

5.7 Monétique

- Tout équipement monétique installé, remplacé ou redéployé dispose d'un agrément GIE CB en cours de validité. Les fins d'agrément sont signalées au CMN dans les conditions prévues au CCTP.
- Aucune donnée de carte bancaire n'est extraite, copiée ou conservée, y compris lors d'une reprise de données ou d'une réparation en atelier.
- Les paramètres monétiques (numéros de commerçant, clés, identifiants de télécollecte) sont traités de manière confidentielle et accessibles aux seuls intervenants habilités

5.8 Bornes wifi

- Les mots de passe d'administration par défaut des bornes sont modifiés à l'installation et conservés dans le coffre-fort désigné par le CMN.
- Le réseau wifi est chiffré (WPA2 minimum, WPA3 lorsque les équipements le permettent) et réservé aux équipements du parc.
- Le firmware des bornes est maintenu à jour dans les délais de l'article 5.5.
- La clé wifi n'est jamais communiquée aux agents ni affichée sur les équipements.
- Les mots de passe sont jamais transmis par mail ou en clair, tout échange se fait pas un canal sécurisé valide pas le CMN.

6 Matériels et supports de stockage

Tout support de stockage d'un matériel du parc (disques durs et SSD des caisses et serveurs, mémoire des terminaux mobiles et des bornes de contrôle d'accès, TPE) est considéré comme contenant des données du CMN, quel que soit son état de fonctionnement.

1.1 Reprise de données

- La reprise de données est limitée aux données nécessaires à la remise en service.
- Les copies temporaires réalisées en atelier sont stockées sur des supports chiffrés et supprimées dès la remise en service validée.
- Les disques préparés à la demande du CMN sont remis en main propre ou expédiés par un moyen tracé.

1.2 Effacement sécurisé

- Un effacement sécurisé est réalisé avant toute sortie définitive du parc (cession, remise aux Domaines, recyclage, retour à un tiers).
- La méthode est adaptée au type de support, conformément au NIST SP 800-88 (niveau « Purge ») : réécriture pour les disques durs, commande d'effacement sécurisé du constructeur ou effacement cryptographique pour les SSD, réinitialisation usine avec chiffrement actif pour les terminaux mobiles, procédure constructeur pour les TPE.
- Un matériel réaffecté à un autre monument est entièrement remasterisé avant réinstallation.

1.3 Garantie constructeur et réparation externe

- Aucun support de stockage n'est envoyé au constructeur ou à un réparateur tiers sans effacement sécurisé préalable.
- Si l'effacement est impossible (support défaillant), le support est conservé par le titulaire et seul le reste du matériel est envoyé.

1.4 Destruction

- Tout support qui ne peut pas être effacé ou dont l'effacement a échoué est détruit physiquement (broyage ou désintégration), par le titulaire ou un prestataire spécialisé.

1.5 Attestation

- Chaque effacement ou destruction fait l'objet d'une attestation indiquant : numéro de série du matériel et du support, méthode, date, résultat, opérateur.
- Les attestations sont transmises au CMN avant toute cession ou remise aux Domaines, et tenues dans un registre consultable sur demande.

1.6 Stockage

- Les matériels du CMN sont stockés dans un lieu sécurisé à accès contrôlé, limité aux intervenants habilités.
- Les stocks du CMN (spare, itinérant, réserve, matériels en attente de sortie) sont physiquement séparés et identifiés, conformément au CCTP.

1.7 Transport

- Chaque expédition et chaque retour sont tracés de bout en bout.
- Toute perte ou vol d'un matériel ou support est traité comme un incident de sécurité et signalé au CMN dans les conditions de l'article 7.

1.8 Interventions sur site

- Les intervenants se présentent au responsable du point de vente et respectent les règles d'accès du monument.
- Aucun équipement ou support non autorisé par le CMN n'est connecté au réseau ou aux matériels du CMN.
- Les supports amovibles utilisés pour les interventions sont dédiés à la prestation et analysés par antivirus avant usage.
- Toute action sur le réseau (brassage, actifs) n'est réalisée que sur demande et sous le contrôle du CMN.

2 Gestion des incidents

2.1 Notification

Tout incident de sécurité ou suspicion d'incident est signalé au CMN dans un délai maximum de 24 heures après sa détection, notamment :

- La compromission ou l'usage anormal d'un compte ou d'un outil de télémaintenance,
- La perte ou le vol d'un matériel, d'un support ou d'un master,
- La détection d'un logiciel malveillant lors d'une intervention,
- Toute anomalie de sécurité constatée sur un équipement monétique.

La notification est envoyée à :

- **rssi@monuments-nationaux.fr**
- **donneespersonnelles@monuments-nationaux.fr**

Elle contient : la description de l'incident, l'impact constaté ou potentiel, les actions engagées et le contact technique pour le suivi.

2.2 Rapport d'incident

Un rapport complet est transmis dans un délai de 72 heures après la notification. Il précise la nature de l'incident, son impact, les mesures correctives et les éléments techniques utiles à l'analyse.

2.3 Collaboration

Le titulaire collabore pleinement avec le CMN lors des investigations : accès aux informations nécessaires, conservation des traces, participation aux actions de remédiation.

3 Audit et contrôle

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

- L'organisation et les outils de télémaintenance,
- La gestion et la protection des masters,
- Les procédures d'effacement et de destruction, y compris par contrôle des attestations et vérification d'échantillons de supports,
- Les conditions de stockage des matériels du CMN, y compris par visite des locaux du titulaire.

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

4 Informations et livrables attendus

Sur demande du CMN, le titulaire fournit :

- Le PAS à jour,
- La liste des intervenants habilités,
- Les traces des sessions de télémaintenance,
- L'état de déploiement des correctifs par équipement,
- Le registre des attestations d'effacement et de destruction.

Ces éléments portent exclusivement sur le périmètre de la prestation fournie au CMN.

5 Fin de marché

Dans le cadre de la réversibilité prévue à l'article 25 du CCAP, le titulaire :

- Remet au CMN ou au nouveau titulaire les masters, leur documentation et les mots de passe d'administration, par un canal sécurisé,
- Restitue l'ensemble des matériels du CMN en stock, avec l'inventaire à jour,
- Supprime les accès, comptes et outils de télémaintenance installés sur les systèmes du CMN, et en fournit la preuve,
- Efface toutes les copies résiduelles détenues (masters, données de reprise, configurations, exports), dans un délai de 30 jours calendaires après la fin du marché,
- Fournit une attestation d'effacement couvrant ces éléments.

Le titulaire ne réutilise aucune donnée, configuration ou master du CMN pour d'autres clients ou à d'autres fins.

6 Sanctions

En cas de non-conformité, le CMN peut, de manière graduelle et proportionnée :

- Demander des actions correctives ou un plan de remédiation,
- Suspendre temporairement les accès de télémaintenance si un risque important pour la sécurité du SI est avéré,
- Signaler les manquements graves ou répétés au CSIRT du ministère de la Culture et, si nécessaire, à l'ANSSI,
- Appliquer les dispositions du CCAP, notamment les pénalités et, en dernier recours, la résiliation du marché.

7 Suivi et révision

Ce document fait l'objet d'une mise à jour annuelle. La révision est réalisée par le RSSI du CMN, en coordination avec la MSIC et le DPO.