

# **ACCORD-CADRE RELATIF A LA FOURNITURE, L'INSTALLATION, LE SUPPORT ET LA MAINTENANCE DE SYSTEMES DE SECURITE INFORMATIQUE DU MUSEE DU QUAI BRANLY - JACQUES CHIRAC**

## **Cahier des clauses techniques particulières (CCTP)**

## Table des matières

<b>1.</b>	<b>GENERALITE</b>	<b>3</b>
1.1	DESCRIPTION DE L'ARCHITECTURE	3
1.2	SCHEMA SIMPLIFIE D'INFRASTRUCTURE	4
<b>2.</b>	<b>DESCRIPTION DES FOURNITURES ET PRESTATIONS</b>	<b>4</b>
2.1	FOURNITURE D'EQUIPEMENT PARE-FEU – CARACTERISTIQUES TECHNIQUES	5
2.2	FOURNITURE D'EQUIPEMENT GESTION D'ACCES A PRIVILEGE – CARACTERISTIQUES TECHNIQUES	5
2.3	FOURNITURE D'EQUIPEMENT DE REPARTITION DE CHARGE ET REVERSE PROXY ET WAF – CARACTERISTIQUES TECHNIQUES	6
2.4	FOURNITURE DES LICENCES	7
2.5	LA GARANTIE, LA MAINTENANCE, LE SUPPORT ET L'ASSISTANCE	7
2.5.1	L'accueil	7
2.5.2	Le diagnostic	8
2.5.3	La maintenance matérielle et le suivi logiciel	8
2.5.4	Niveaux de dysfonctionnement	8
2.5.5	Intervention sur site : maintenance matérielle	8
2.5.6	Niveaux d'erreur ou d'anomalie logiciel	9
2.5.7	Solution de remplacement ou correctif provisoire	9
2.5.8	Suivi logiciel/progiciel correctif	9
2.5.9	Suivi logiciel évolutif	10
2.6	AUTRES PRESTATIONS DE SERVICES	10
2.7	SERVICE D'INVESTIGATION ET DE REPONSE A INCIDENT	12
2.7.1	Investigation	12
2.7.2	Réponse à incident	12
2.7.3	Services complémentaires :	13
<b>3.</b>	<b>POLITIQUE DE SECURITE DU NUMERIQUE</b>	<b>14</b>
<b>4.</b>	<b>RECYCLAGE DE MATERIEL INFORMATIQUE ET GESTION DES DECHETS</b>	<b>17</b>

## 1. GENERALITES

Afin d'assurer la protection de son système d'information, le musée du quai Branly - Jacques Chirac s'est doté de systèmes de protection du réseau de marque CHECKPOINT.

Les pare-feux utilisés masquent les IP des équipements du réseau du musée du quai Branly - Jacques Chirac (NAT) et n'autorisent aucun flux direct vers l'intérieur. Ils permettent la mise en œuvre et la gestion de VPN site à site ainsi que pour des clients nomades au travers d'un module logiciel installé sur les postes clients.

L'Etablissement dispose également de passerelles de connexions de marque WALLIX permettant une gestion des accès à privilèges vers différents équipements effectués par certains mainteneurs tiers ou partenaires.

Des équipements de la marque F5, permettant d'effectuer de la répartition de charges ainsi que du reverse proxy sont également en place. Ils permettent également de sécuriser un certain nombre d'applications web au travers d'un module de sécurité type WAF.

La protection des postes de travail et des serveurs est effectuée au moyen de système EDR/MDR Sophos ainsi que d'un système de proxy basée sur la solution Zscaler.

Ces solutions matériels et logiciels correspondent aux prérequis techniques exprimés par le musée du quai Branly - Jacques Chirac et répondent encore aujourd'hui à ses besoins.

### 1.1 DESCRIPTION DE L'ARCHITECTURE

L'architecture réseau est articulée autour d'une topologie réseau en étoile constituée de plusieurs VLAN. Le cœur de réseau est composé de deux (2) routeurs fibre actif / passif interconnectés en liaison 10Gbe, répartie sur deux (2) salles. Les bâtiments sont interconnectés au cœur de réseaux au travers de commutateurs en configuration « autonome », ou monté en « pile ».

Le musée dispose de plusieurs réseaux isolés par des pare-feu, afin de permettre l'interconnexion de flux spécifiques en fonction des besoins métiers propre à ces réseaux.

L'ensemble des communications entre le réseau Internet et le système d'information du musée du quai Branly - Jacques Chirac est assuré au travers de deux équipements pare-feu CHECKPOINT garantissant un fonctionnement en haute disponibilité, sous la forme d'un cluster. Ce cluster est interconnecté avec un bâtiment distant au travers d'un VPN site à site et permet par ailleurs la connexion pour des utilisateurs nomades via un VPN logiciel à un accès sécurisé sur le site principal du musée du quai Branly - Jacques Chirac.

Un second cluster de deux équipements pare-feu CHECKPOINT permet, en garantissant un fonctionnement en haute disponibilité, d'assurer la protection des autres environnements internes du pouvoir adjudicateur.

Enfin, un dernier pare-feu CHECKPOINT permet de garder cloisonné le réseau de gestion de la sécurité/sûreté du bâtiment.

L'ensemble de ces pare-feux est géré de façon centralisée via une console d'administration redondée, ainsi que d'une console d'analyse des événements et de génération de rapports, le tout est hébergé sur trois (3) boîtiers smart-1 600S

Le premier cluster est composé de deux (2) appliances 9700, le second cluster de deux (2) appliances 9100 et d'un autre boîtier de type 3800.

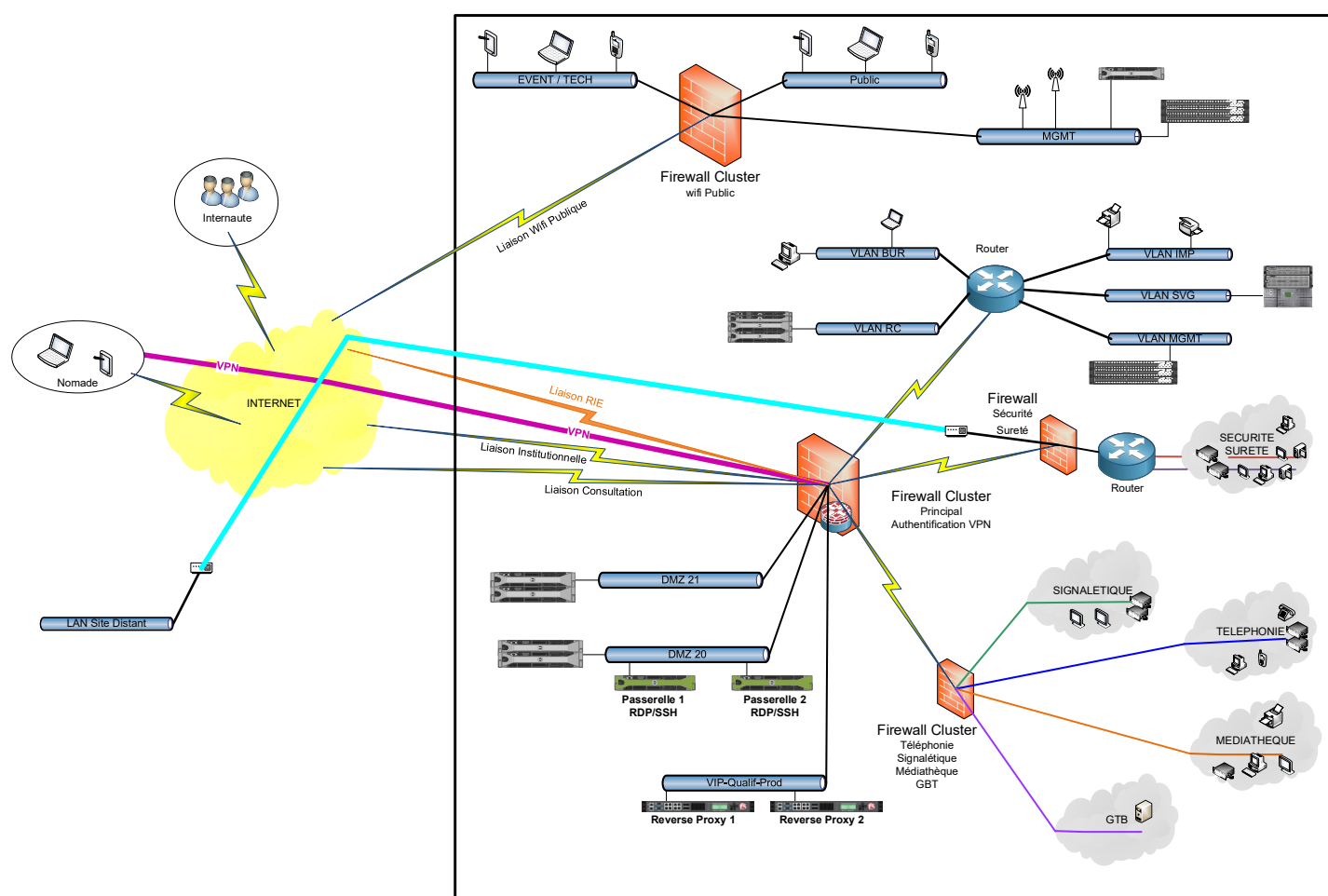
L'Etablissement dispose également d'un réseau wifi public pour ses visiteurs. Ce réseau est physiquement indépendant du reste du système d'information. Un cluster composé de deux (2) équipements pare-feu CHECKPOINT permet également d'assurer sa protection en garantissant là encore de la haute disponibilité. La console d'administration est ici directement intégrée sur les boîtiers.

Ce cluster est composé de deux (2) appliances de type 9100.

Concernant la gestion des accès à privilège, le pouvoir adjudicateur dispose de deux (2) boîtiers WALLIX AdminBastion en haute disponibilité.

La répartition de charge ainsi que le reverse proxy et le WAF sont assurés par deux (2) appliances de type F5 BIG-IP i4600 en haute disponibilité.

## 1.2 SCHEMA SIMPLIFIE D'INFRASTRUCTURE



## 2. DESCRIPTION DES FOURNITURES ET PRESTATIONS

Le présent accord-cadre a pour objet la fourniture, l'installation, le support et la maintenance de systèmes de sécurité informatique de l'établissement public du musée du quai Branly - Jacques Chirac et des prestations associées.

L'accord-cadre permet l'acquisition de solutions de sécurité suivants :

- Pare-feu de marque CHECKPOINT ou équivalent, ainsi que de sa plateforme d'administration ;
- Gestion d'accès à privilège de marque WALLIX ou équivalent ;

- Répartition de charge et reverse Proxy et WAF de marque F5 ou équivalent.
- Protection de type EDR/MDR de marque Sophos ou équivalent.
- Proxy de marque Zscaler ou équivalent.
- Coffre-fort Numérique et de mot de passe de marque LockSelf ou équivalent.
- Authentification multi facteur

Les solutions proposées devront être totalement compatibles avec les solutions existantes.

Dans le cadre du présent accord-cadre, le musée du quai Branly - Jacques Chirac pourra également commander au titulaire des prestations associées de services, de maintenance et de support.

L'accord-cadre permet également l'acquisition de prestations, d'investigation et de réponse à incident en cas notamment de cyberattaque.

## **2.1 FOURNITURE D'EQUIPEMENT PARE-FEU – CARACTERISTIQUES TECHNIQUES**

Le titulaire devra pouvoir, dans le cadre de cet accord-cadre, fournir toute la gamme d'appliances permettant de répondre aux besoins du musée du quai Branly - Jacques Chirac.

Les équipements pare-feu devront permettre la gestion de la politique applicative séparée de la politique de filtrage classique, et une administration via un client lourd.

Ils devront également permettre d'effectuer du filtrage d'URL ainsi que la mise en place de VPN site à site et de VPN SSL pour client nomade.

L'une de ces gammes de matériel doit être évolutive, par la possibilité d'ajout de carte d'extension réseau.

Le titulaire, au travers du bordereau de prix unitaires (BPU) et d'un catalogue, proposera tous types d'extensions, modules, accessoires disponibles pour les gammes de pare-feu proposés.

Le titulaire a la possibilité, au travers du bordereau de prix unitaires (BPU) et d'un catalogue, de proposer toute la gamme de pare-feu CHECKPOINT ou équivalent.

## **2.2 FOURNITURE D'EQUIPEMENT GESTION D'ACCES A PRIVILEGE – CARACTERISTIQUES TECHNIQUES**

Le titulaire doit, dans le cadre de cet accord-cadre, pouvoir fournir toute la gamme d'appliances permettant de répondre aux besoins du musée du quai Branly - Jacques Chirac.

Les équipements devront permettre de tracer et d'enregistrer toutes les actions effectuées sur les équipements auxquels ils permettent une connexion, au travers notamment d'enregistrement permettant un visionnage vidéo des sessions à privilège.

Par ailleurs, ils devront être en capacité d'informer les équipes de gestion du Service du système d'information du pouvoir adjudicateur de toutes connexions effectuées sur son environnement.

Le titulaire a la possibilité, au travers du bordereau de prix unitaires (BPU) et d'un catalogue, de proposer toute la gamme d'AdminBastion WALLIX ou équivalent.

## **2.3 FOURNITURE D'EQUIPEMENT DE REPARTITION DE CHARGE ET REVERSE PROXY ET WAF – CARACTERISTIQUES TECHNIQUES**

Le titulaire doit, dans le cadre de cet accord-cadre, fournir toute la gamme d'appiances permettant de répondre aux besoins du musée du quai Branly - Jacques Chirac.

Les équipements devront permettre d'effectuer, au-delà des fonctionnalités de répartition de charge et de reverse proxy, un rôle de pare-feu pour les applications web (WAF).

Les fonctionnalités attendues sont les suivantes :

- Vérification de la conformité protocolaire
- Protection contre les injections SQL
- Protection contre les attaques de type DDos
- Détection des bots
- Web scraping protection
- Web Site Cloaking
- JSON Protection
- Response Control
- Protection contre le vol de données
- File Upload control
- SSL Offloading
- Web Translations : (URL redirect/Translations, http request/response rewrite)
- Authentification RADIUS des utilisateurs
- Authentification à 2 facteurs : certificats clients, passcode SMS, etc.
- XML Firewall
- Network Firewall
- Antivirus pour les fichiers uploadés
- Client ip reputation
- Apprentissage automatique
- Cache et compression
- Logging, Monitoring and reporting
- Administration centralisée

Le titulaire a la possibilité, au travers du bordereau de prix unitaires (BPU) et d'un catalogue, de proposer toute la gamme BIG-IP F5 ou équivalent.

## 2.4 FOURNITURE DES LICENCES

Le titulaire, au travers du bordereau de prix unitaires (BPU) et d'un catalogue, devra proposer toutes licences des produits permettant au musée du quai Branly - Jacques Chirac de faire l'acquisition de nouvelles fonctionnalités que les équipements peuvent offrir, et le renouvellement de ces licences, pour les solutions suivantes :

- CHECKPOINT ou équivalentes ;
- WALLIX ou équivalent ;
- F5 ou équivalent ;
- Sophos ou équivalent ;
- Zscaler ou équivalent ;
- LockSelf ou équivalent ;

## 2.5 LA GARANTIE, LA MAINTENANCE, LE SUPPORT ET L'ASSISTANCE

Les matériels et logiciels acquis dans le cadre du présent accord-cadre font l'objet d'une maintenance et d'un suivi dont le point de départ est la réception des équipements concernés, ou la reconduction du support et de la maintenance de ces équipements. Les équipements existants pourront également être concernés par des prestations de maintenance et de suivi via cet accord-cadre.

Les prestations de maintenance et de suivi sont indissociables et exécutées par le titulaire ou par les constructeurs et éditeurs, sous la responsabilité du titulaire. Les prestations qui devront être assurées à minima sont celles décrites dans les paragraphes ci-dessous.

Toutes les interventions de maintenance ou de dépannage devront être consignées et décrites dans le détail sur un support réservé à cet effet (type base de suivi, fichier etc.).

Le contenu proposé pour la maintenance et le processus s'y rapportant sont décrits dans le mémoire technique remis par le titulaire à l'appui de son offre. Les délais de livraison sont conformes à ceux décrits dans le mémoire technique remis par le titulaire à l'appui de son offre.

Le titulaire proposera au travers du bordereau de prix unitaires (BPU) et/ou d'un catalogue, l'ensemble des garanties, maintenances support et assistance pour chacun des produits.

### 2.5.1 L'ACCUEIL

L'accueil concerne tout appel pour dysfonctionnement d'un matériel et/ou logiciel associé, dont le titulaire assure la maintenance et le support avec le suivi, directement ou indirectement, via le constructeur ou l'éditeur.

L'accueil est effectué en langue française et doit être possible au minimum par téléphone ou par internet. Il couvre au minimum les aspects suivants :

- Le suivi des dossiers en cours ;
- L'ouverture d'un dossier ;
- La clôture d'un dossier.

Le titulaire proposera un point d'entrée unique pour tous les appels concernant la maintenance et le support des matériels, logiciels, du périmètre en question et ceci dans la plage horaire de 9h à 18h du lundi au samedi, jour fériés exclus.

Le mémoire technique remis par le titulaire à l'appui de son offre détaillera les conditions d'accès au support.

### 2.5.2 LE DIAGNOSTIC

Si le titulaire n'exécute pas lui-même les prestations, il devra router tous les incidents du musée du quai Branly - Jacques Chirac vers les tiers mainteneurs dans un délai inférieur à 30 mn à compter de la demande du musée, dans la plage horaire de la hotline du titulaire. Le titulaire s'engage à suivre l'appel jusqu'à sa clôture, en fournissant au pouvoir adjudicateur un compte rendu d'incident. Un point téléphonique intermédiaire sera établi par le titulaire avec le musée, à H+2 (heures ouvrées) après l'ouverture de l'incident.

A la fin du diagnostic commun, le musée et le titulaire identifient :

- Si le dysfonctionnement est d'origine matérielle ;
- Si le dysfonctionnement a pour origine le système d'exploitation de la configuration ou un logiciel ;
- A défaut, le dysfonctionnement est considéré provenir d'une autre origine et donc n'entre pas dans la prestation du titulaire.

### 2.5.3 LA MAINTENANCE MATERIELLE ET LE SUIVI LOGICIEL

Le titulaire peut, pour tout ou partie du périmètre, se tourner vers le constructeur ou l'éditeur pour exécuter les prestations.

Que ce soit le titulaire ou un constructeur ou un éditeur qui exécute la prestation, le titulaire doit respecter et faire respecter les termes ci-après du présent CCTP.

La réparation de panne matérielle sera effectuée sous la forme d'un échange standard de matériel. Le mémoire technique remis par le titulaire à l'appui de son offre détaille les conditions de cet échange.

### 2.5.4 NIVEAUX DE DYSFONCTIONNEMENT

Deux niveaux de dysfonctionnements matériels sont définis dans le cadre du présent accord-cadre :

- Panne bloquante : une panne est dite bloquante lorsque le dysfonctionnement bloque l'exploitation de la solution technique et qu'aucune solution de contournement n'est connue ;
- Panne non bloquante : une panne est dite non bloquante lorsque le dysfonctionnement permet quand même un traitement en mode dégradé, sans diminution des fonctionnalités.

### 2.5.5 INTERVENTION SUR SITE : MAINTENANCE MATERIELLE

Les interventions de maintenance sur site doivent pouvoir garantir le délai de Garantie de Temps de Rétablissement de quatre (4) heures, à compter de la demande du musée.

Les interventions commencées pendant l'horaire contractuel d'intervention seront poursuivies sans désenclaver, jusqu'au moment où le dysfonctionnement aura disparu, et ceci sans donner lieu à une facturation supplémentaire.

Toutefois, ces interventions nécessitent obligatoirement la présence sur le site d'une personne compétente du musée du quai Branly - Jacques Chirac. À défaut de présence de compétences du musée, le titulaire n'est plus obligé de rester sur site.

Le musée du quai Branly - Jacques Chirac effectuera, après chaque intervention du titulaire, une sauvegarde des paramètres. Une recette commune sera effectuée avec le titulaire pour valider la maintenance.



### 2.5.6 NIVEAUX D'ERREUR OU D'ANOMALIE LOGICIEL

Le suivi correctif des progiciels concerne la correction des dysfonctionnements (erreurs, anomalies et incidents) sur le progiciel dans la limite du périmètre standard que le titulaire aura décrite dans son mémoire technique.

Trois niveaux d'erreur ou anomalie du système d'exploitation ou d'un logiciel, génératrices d'un dysfonctionnement, sont définis dans le cadre du présent accord-cadre et doivent donner lieu à correction par le titulaire :

- Erreur ou anomalie bloquante : une erreur ou une anomalie est dite bloquante lorsqu'après réinitialisation, voir réinstallation, l'exploitation du système d'exploitation ou d'un logiciel est bloquée et qu'il n'existe, pour l'utilisateur du système d'exploitation ou du logiciel, aucune solution de contournement, ni correctif. Une anomalie bloquante entraîne donc l'impossibilité d'exploiter le système d'exploitation ou le logiciel pare-feu ;
- Erreur ou anomalie majeure : une erreur ou anomalie est dite majeure lorsqu'elle a un impact significatif sur le fonctionnement du logiciel, mais il existe au moins une solution de contournement, ou lorsque les conséquences du défaut ne bloquent pas l'utilisation (même dégradée) du produit ;
- Erreur ou anomalie mineure : une erreur ou anomalie est dite mineure lorsqu'elle n'a pas d'impact significatif sur le fonctionnement du système.

### 2.5.7 SOLUTION DE REMPLACEMENT OU CORRECTIF PROVISOIRE

Aucune solution de remplacement ou correctif provisoire, installée par le titulaire, ne devra diminuer les performances et les fonctionnalités du matériel, telles que prévues dans la documentation du constructeur ou du système d'exploitation, ou du logiciel, telles que prévues dans la documentation de l'éditeur.

### 2.5.8 SUIVI LOGICIEL/PROGICIEL CORRECTIF

Le suivi logiciel correctif concerne la correction des dysfonctionnements (erreurs, anomalies et incidents) sur le produit logiciel concerné.

Le suivi progiciel est assuré en langue française.

En cas de dysfonctionnement, d'interruption, de mauvais fonctionnement, etc. d'un niveau de version de produits logiciels et/ou de non-respect des spécifications, le titulaire prendra toutes les mesures appropriées pour rétablir le bon fonctionnement du logiciel.

Le titulaire fournira un support téléphonique, voir sur Internet (ou sur site dans certains cas), avec fourniture de correctif, si nécessaire, pour résoudre les problèmes relatifs aux produits ou documentations techniques, lorsque des erreurs ou anomalies apparaissent à l'exploitation, ou à l'utilisation, ou si la détérioration résulte d'une mauvaise indication de sa part, ou de celle de l'éditeur, ou d'une omission de précaution, ou d'une incompatibilité non mentionnée dans la documentation.

Cette prestation comprend notamment :

- L'analyse de l'erreur ou de l'anomalie constatée sur les logiciels couverts par le suivi correctif ;
- La qualification, par le pouvoir adjudicateur avec l'aide du titulaire, du niveau de criticité de l'erreur ou de l'anomalie ;
- La mise à disposition des correctifs ou de la solution de contournement existant au catalogue de l'éditeur, éventuellement un site WEB du titulaire ou de l'éditeur ;
- L'étude de solutions permettant d'éviter ou de contourner les effets des erreurs ou anomalies, s'il n'y a pas de correctif disponible immédiatement au catalogue de l'éditeur ;

- En cas d'indisponibilité prolongée, supérieure au délai de réparation prévisible, le titulaire fera appel impérativement à l'éditeur, à ses frais, pour résoudre le dysfonctionnement ;
- La fourniture de correctif spécifique à une erreur ou anomalie solutionnée par un correctif développé spécifiquement par l'éditeur ;
- Les tests et contrôles effectués par le titulaire ;
- La mise à disposition de mises à jour, éventuellement sur un site WEB du titulaire ou de l'éditeur, si le correctif ne permet pas la correction.

### 2.5.9 SUIVI LOGICIEL EVOLUTIF

Le suivi évolutif des logiciels assuré par le titulaire consiste à fournir des nouvelles versions, des mises à jour (révisions) et des documentations techniques des logiciels qui :

- Suivent les évolutions de versions des systèmes dans les limites des disponibilités au catalogue de l'éditeur ;
- Comprennent des modifications et extensions fonctionnelles du produit supporté ;
- Contiennent les correctifs établis pour les niveaux de versions antérieures, de changement de plate-forme à seuil concédé équivalent.

Les prestations de suivi progiciel évolutif sont assurées en français.

Les mises à jour logicielles devront être régulièrement communiquées au musée du quai Branly - Jacques Chirac.

Le mémoire technique remis par le titulaire à l'appui de son offre détaille les conditions de cette diffusion.

## 2.6 AUTRES PRESTATIONS DE SERVICES

Au-delà des fournitures et prestations définies ci-avant, le titulaire assurera, dans le cadre du présent accord-cadre, d'autres prestations, notamment :

- De conseil et d'audit ;
- D'étude d'impact ;
- D'installation, de configuration et de paramétrage de tous les matériels ;
- De fourniture de mises à jour (au travers de la maintenance annuelle) ;
- De fourniture des licences connexes aux familles de produits décrites dans le présent CCTP ;
- De remplacement d'équipements existants ou acquis sur la durée de l'accord-cadre ;
- De prestation associée à la mise en place de plateforme ;
- De prestation associée à la mise en place des cas de test ;
- D'opérations de tests, de recettes ;
- De prestation associée de test d'intrusion ;
- De migration des services existants vers de nouvelles plateformes ;
- De transfert de compétence et la formation des administrateurs ;
- De maintenance pendant la période de garantie ;
- D'un contrat de maintenance au-delà de la période de garantie.

Le mémoire remis par le titulaire à l'appui de son offre indique sa méthodologie sur :

- La phase de déploiement, intégrant les coupures de service éventuelles ;
- Les tests unitaires et d'intégration;
- Les audits et les tests d'intrusions.

Ces prestations sont présentées au bordereau de prix unitaires (BPU) sous forme de journée et/ou demi-journée, en heures ouvrées et non ouvrées.

Les prestations de mise à jour et de remplacement d'équipement seront commandées au titulaire par application des prix unitaires « autres prestations de service » du BPU. Pour chaque commande passée sur cette base, le titulaire sera tenu à une obligation de résultat, sans surcoût, quel que soit le nombre d'heures qu'il aura effectivement consacrées à la réalisation de la commande passée.

A ce titre il devra être en mesure de fournir des équipements de prêt équivalents à ceux utilisés par le musée du quai Branly - Jacques Chirac.

Cela doit permettre, si nécessaire, de procéder à un échange de boîtier après réplique de la configuration de production, de façon à minimiser l'indisponibilité, et ainsi palier les problèmes pouvant survenir dans une phase de migration et impactant directement les utilisateurs du musée du quai Branly - Jacques Chirac.

Le mémoire technique remis par le titulaire à l'appui de son offre détaille les conditions de prêts d'équipement.

A l'issue de ces prestations et en fonction de la mission commandée par le pouvoir adjudicateur, le titulaire du présent accord-cadre devra le cas échéant remettre au musée du quai Branly - Jacques Chirac :

- Un dossier technique détaillé décrivant la solution mise en place au musée du quai Branly - Jacques Chirac, mentionnant l'ensemble des paramètres retenus lors de l'installation ;
- L'ensemble des procédures nécessaires à l'exploitation et au bon fonctionnement de la plateforme (procédures complètes et détaillées des opérations périodiques à réaliser) ;
- Un cahier de tests et recette de bon fonctionnement de la configuration complète pour chaque opération ;
- Plus généralement, toutes les documentations techniques et brochures fournies par les constructeurs et les éditeurs des logiciels qui composent la solution ;
- Les procédures d'appel et de maintenance de la solution.

Le titulaire doit être en mesure de réaliser un audit annuel de vérification des plates-formes, afin d'identifier d'éventuelles failles, besoins de mise à jour, ou tout autre problème potentiel sur les plateformes. Cet audit, qui pourra être commandé en tant que de besoin par le musée, sera rémunéré par un prix unitaire qui couvrira tous les frais relatifs à la réalisation de cet audit annuel. Les opérations de corrections mineures seront réalisées dans le cadre de l'audit, sans surcoût.

A l'occasion de l'audit, le titulaire proposera des actions correctives qui pourront faire l'objet de commandes de prestations complémentaires pour les opérations les plus complexes.

## 2.7 SERVICE D'INVESTIGATION ET DE REPONSE A INCIDENT

Le service décrit dans cette section a pour but d'assurer la gestion d'incidents de sécurité sur le système d'information de l'établissement public du musée du quai Branly – Jacques Chirac.

Le titulaire de ce service doit garantir un haut niveau de confidentialité et d'intégrité, et respecter des engagements stricts envers la protection des données et des informations collectées.

Le titulaire proposera un service permettant d'accompagner les équipes de l'établissement, pour la gestion d'un incident de sécurité sur son système d'information, avec une prise en charge rapide après détection d'incident sans bon de commande préalable. Une commande de régularisation sera faite après gestion de la crise en reprenant les prix définis au bordereau de prix unitaires (BPU) sous forme de journée, en heures ouvrées et non ouvrées.

### 2.7.1 INVESTIGATION

L'objectif principal de l'investigation est de comprendre et de documenter l'incident de sécurité. Les actions à mener sont les suivantes :

- **État des lieux après l'incident :**  
Analyser l'ampleur de l'incident.
- **Périmètre impacté :**  
Identifier les systèmes, les données et les services affectés.
- **Causes de l'incident :**  
Dans le cas d'une attaque, il est nécessaire de déterminer :
  - Le *mode opératoire de l'attaquant*.
  - La *séquence des événements* ayant mené à l'incident.
  - Le *vecteur d'intrusion*, les moyens d'élévation de privilèges et de *déplacement latéral*.
- **Archivage sécurisé des preuves :**  
Conserver les traces collectées de manière sécurisée.
- **Chronologie détaillée :**  
Présenter un résumé chronologique complet de l'incident.
- **Recommandations de prévention :**  
Proposer des actions pour prévenir la récurrence de l'incident.

### 2.7.2 REPONSE A INCIDENT

La réponse à un incident de sécurité doit se faire de manière structurée et rapide. Les actions sont les suivantes :

- **Coordination de la gestion de crise :**  
Appliquer une approche méthodologique, telle que le cadre NIST ou SANS.
- **Mesures immédiates :**  
Mettre en place des actions pour limiter l'impact de l'incident, comme :
  - Isolement des systèmes compromis.
  - Coupure des accès affectés.
- **Restauration des systèmes :**

Aider à la reprise d'activité et des services affectés, à la restauration des accès aux données et l'application de correctifs de sécurité.

➤ **Rapports détaillés :**

Rédiger des rapports détaillant les événements, les impacts, les actions entreprises et les mesures prises, à destination des parties prenantes internes et externes, ainsi que des autorités compétentes si nécessaire.

### 2.7.3 SERVICES COMPLEMENTAIRES :

Le titulaire proposera un accompagnement de service proactif et d'expertise forensique et de réponse à incident :

➤ **Rétro-ingénierie de logiciels malveillants :**

Analyser et décortiquer des malwares pour en comprendre le fonctionnement.

➤ **Levée de doutes sur des systèmes ou supports de données :**

Vérification de la conformité et de la sécurité des systèmes et supports de données.

➤ **Rédaction de politiques de sécurité et de procédures opérationnelles :**

Élaboration de stratégies de sécurité et de lignes directrices pour les équipes de l'établissement.

➤ **Recherche proactive de compromissions :**

Détecter des failles de sécurité avant qu'elles ne soient exploitées.

➤ **Évaluation ou proposition de durcissement des systèmes :**

Proposer des actions pour renforcer la sécurité des systèmes existants.

➤ **Localisation et sécurisation des preuves :**

Préparer et sécuriser les preuves pour une exploitation légale.

Le titulaire doit décrire de manière détaillée les niveaux de service, la réactivité attendue et la méthodologie employée. Cela inclut également le processus de déclenchement du service en cas d'incident.

Une qualification PRIS (Prestataire de Réponse à Incident de Sécurité) délivrée par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) serait un atout majeur pour le prestataire.

### 3. POLITIQUE DE SECURITE DU NUMERIQUE

Le cadre de gouvernance de la sécurité numérique de l'État, corédigé avec l'ensemble des ministères, renforce la prise en compte du risque numérique dans la mise en œuvre et l'exploitation des systèmes d'information et de communication de l'État par les ministères et les établissements publics d'État.

Ce cadre vise à :

- Responsabiliser les dirigeants (par exemple les directeurs d'administration centrale ou les responsables d'établissement) à la sécurité numérique ;
- Renforcer la sécurité numérique des établissements publics de l'État ;
- Responsabiliser les acteurs de la transformation numérique ;
- Assurer la cohérence avec les principaux textes réglementaires définissant une gouvernance en matière de numérique ou de sécurité, notamment la nouvelle IGI 1300 et le décret n° 2019-1088 définissant les responsabilités de la direction interministérielle du numérique (DINUM) ;
- Assurer la gouvernance aux différents niveaux de l'État via la mise en place d'une procédure de prise de décision aux niveaux interministériel et ministériel.

Le cadre de gouvernance, à terme, se substituera à la circulaire du Premier ministre n° 5725/SG du 17 juillet 2014 introduisant la politique de sécurité des systèmes d'information de l'État (PSSIE). Actuellement les deux cohabitent et se complètent, surtout en ce qui concerne les règles de sécurité prévues par cette PSSI.

Ce cadre s'articule autour :

- Du décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'État et à la direction interministérielle du numérique modifié par le décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics.
- De l'instruction générale interministérielle n°1337/SGDSN/ANSSI sur l'organisation de la gouvernance de la sécurité numérique de l'État, approuvée par arrêté.
- La circulaire du Premier ministre n° 5725/SG du 17 juillet 2014 introduisant la politique de sécurité des systèmes d'information de l'État (PSSIE).

<https://cyber.gouv.fr/cadre-de-gouvernance-de-la-securite-numerique-de-letat-pssie>

Le titulaire devra respecter la Politique de sécurité du numérique du ministère de la culture (Arrêté du 21 janvier 2022).

En conformité avec les réglementations françaises et européennes, le ministère de la culture a élaboré sa politique en tenant compte de ses enjeux et de ses besoins.

Ainsi, les principes ministériels de gouvernance que la présente politique décrit, doivent être conformes à l'instruction relative à la gouvernance de la sécurité numérique de l'Etat (2021). En outre, les règles de sécurité du numérique appliquées au sein du ministère et des

établissements publics doivent être cohérents avec la politique de sécurité des systèmes d'information de l'Etat (PSSIE)

La Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE) fixe les règles de protection applicables aux systèmes d'information de l'État. Celle-ci est portée par la circulaire du Premier ministre n° 5725/SG du 17 juillet 2014.

La PSSIE s'applique à tous les systèmes d'information des administrations de l'État : ministères, établissements publics sous tutelle d'un ministère, services déconcentrés de l'État et autorités administratives indépendantes.

La PSSIE concerne l'ensemble des personnes physiques ou morales intervenant dans ces systèmes d'information, qu'il s'agisse des administrations de l'État et de leurs agents ou bien de tiers agissant au nom et pour le compte des administrations de l'État (prestataires ou sous-traitants) et de leurs employés.

Par ailleurs, certains périmètres sensibles font l'objet d'exigences particulières :

- les systèmes d'information mis en œuvre par le ministère dans ses relations avec les autres autorités administratives et avec les citoyens doivent respecter le Référentiel Général de Sécurité (RGS) ;
- les services numériques traitant des données à caractère personnel doivent être conformes avec le Règlement Général sur la protection des données (RGPD) ;
- enfin, les transactions électroniques et les systèmes d'authentification électronique doivent respecter le règlement eIDAS portant sur la confiance numérique

Le titulaire doit obligatoirement respecter les dispositions et directives de la PSSIE ainsi que les exigences particulières.

Dans le cadre d'un hébergement de sa solution en mode SaaS il devra obligatoirement respecter le référentiel d'exigences applicables aux prestataires de services cloud défini par l'ANSSI (SecNumCloud). Cette qualification atteste de la qualité et de la robustesse de la prestation, de la compétence du prestataire ainsi que de la confiance pouvant lui être accordée.

<https://cyber.gouv.fr/actualites/lanssi-actualise-le-referentiel-secnumcloud>

Il devra fournir un Plan d'Assurance Sécurité (PAS) dans lequel il décrira l'ensemble des dispositions spécifiques que celui-ci prendra pour garantir le respect des exigences de sécurité de la PSNum et de la PSSIE du donneur d'ordre.

Le PAS pourra être modifié lors de l'exécution du présent accord-cadre pour répondre à des évolutions du système, de son environnement ou du périmètre de l'opération. Cette souplesse garantit que les mesures prises par le titulaire seront toujours adaptées aux exigences de sécurité.

Celui-ci devra plus particulièrement détailler les mesures mises en œuvre pour :

- L'exploitation sécurisée des centres informatiques (solutions en mode SaaS ou éléments constitutifs de la solution) contenant des informations concernant l'Etablissement public du musée du Quai Branly - Jacques Chirac ;
- La prise en compte de la sécurité dans la préconisation et l'installation de solutions de Cybersécurité ;
- Assurer une veille technologique fonctionnelle et de sécurité sur les solutions dont il a la charge ;

- Tout autre document que le titulaire jugera nécessaire de fournir pour justifier les mesures de sécurité qu'il prend dans le cadre de ses prestations.

Il devra également détailler les modalités de participation à la gestion de crises de cybersécurité en appui des équipes internes (mise en place d'un SOC), qu'elles soient mineures ou majeures.

Pour plus d'informations se référer aux chapitres suivants de la PSNum :

- 5.2.13 La gestion des alertes et des incidents
- 5.2.14 La gestion de crise cybersécurité

De plus, devront être décrits clairement les modes d'activations possibles de la prestation de participation à la gestion de crise de cybersécurité, en cas d'impossibilité de passer une commande.

**Important** : Le titulaire doit assurer une veille de sécurité sur tous les composants et logiciels de Cybersécurité dont il a la maintenance et de tous les éléments qu'il serait amené à ajouter dans l'écosystème de Cybersécurité de l'Etablissement public du musée du Quai Branly - Jacques Chirac.

Le titulaire a l'obligation d'informer l'Etablissement public du musée du Quai Branly - Jacques Chirac de tout problème impliquant une des solutions de Cybersécurité dont il a la charge, pouvant menacer la sécurité du Système d'Information de l'Etablissement, et il doit fournir une procédure et la méthodologie à appliquer pour y remédier.



#### 4. RECYCLAGE DE MATERIEL INFORMATIQUE ET GESTION DES DECHETS

Le titulaire peut, à la demande du pouvoir adjudicateur, assurer la reprise des matériels informatique et la destruction des données, avec fourniture d'un certificat de destruction. A ce titre, le titulaire détaille les modalités de reprise, de réemploi et de recyclage des matériels les processus s'y rapportant dans son mémoire technique.

Dans le cadre du décret n° 2014-928 du 19 août 2014 relatif aux déchets d'équipements électriques et électroniques et aux équipements électriques et électroniques usagés, codifié aux articles L.541-10-20 et R.543-172 et suivants du Code de l'environnement, le titulaire indique à quel éco-organisme agréé il adhère pour le traitement des déchets d'équipements électriques et électroniques.