Installation de Agora



|  |
| --- |
| **Identification du document** |
| Référence | Clauses AO |
| Date de dernière mise à jour | 17/10/2024 |
| Rédaction et vérification | 17/10/2024 |
| Version |  |
| Classification |  |
| Nombre de pages |  |

**CYCLE DE VIE DU DOCUMENT**

**AUTEUR(S)**

| Fonction | Nom | Date |
| --- | --- | --- |
| Assistant aux utilisateurs | Anne-Marie Galland | 09/03/2020 |
|  |  |  |
|  |  |  |

**RELECTEUR(S)**

| Fonction | Nom | Date |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**VALIDATION**

| Fonction | Nom | Date |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**HISTORIQUE DU DOCUMENT**

| Version | Date | Description | Détails |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Sommaire

[Installation de Agora 1](#_Toc180070861)

[1 Règles minimales de confidentialité de l’information 4](#_Toc180070862)

[2 Gestion des accès et gestion des droits 4](#_Toc180070863)

[3 Cycle de vie des ressources 5](#_Toc180070864)

[4 Durcissement des composants 5](#_Toc180070865)

[5 Reversibilité 5](#_Toc180070866)

[6 Sécurité liée à l’exploitation 6](#_Toc180070867)

[6.1 Procédures et responsabilités liées à l’exploitation 6](#_Toc180070868)

[6.2 Déploiement 6](#_Toc180070869)

[6.3 Protection contre les logiciels malveillants 7](#_Toc180070870)

[6.4 Ségrégation entre front-OFFICE et back-office 7](#_Toc180070871)

[7 Journalisation 7](#_Toc180070872)

[7.1 système de journalisation 7](#_Toc180070873)

[7.2 Traçabilité des utilisateurs du back-office 8](#_Toc180070874)

[8 Gestion des vulnérabilités techniques 8](#_Toc180070875)

[8.1 Veille, analyse, maitrise des risques liés aux vulnérabilités 8](#_Toc180070876)

[8.2 Communication avec Le musée du Louvre 9](#_Toc180070877)

[8.3 Délais de traitement des vulnérabilités 9](#_Toc180070878)

[9 Audit du Service 9](#_Toc180070879)

# Règles minimales de confidentialité de l’information

* Le titulaire ne partage aucune information liée au Contrat à des personnes tierces sans accord explicite et formalisé d’un responsable du musée du Louvre de la prestation ;
* Le titulaire ne stocke, publie, fait transiter aucune information liée au Contrat vers des environnements tiers (boite mail externe, personnelle ou professionnelle ; périphérique de stockage externe ; serveur ; service en ligne ; etc.) sans accord explicite et formalisé d’un responsable du Louvre de la prestation ;
* Si le transfert d’information vers des personnes ou des environnements tiers est autorisé par un responsable du musée du Louvre de la prestation, alors le titulaire met en œuvre des mesures pour assurer un niveau de confidentialité adapté aux enjeux (outils, sensibilisation du tiers impliqué, etc.) ;
* Le titulaire utilise des moyens sécurisés pour l’échange et le stockage des informations confidentielles. Il s’informe donc du niveau de confidentialité des informations manipulées auprès d’un responsable du musée du Louvre de la prestation, et valide avec lui les moyens à utiliser pour ces échanges. LE MUSÉE DU LOUVRE met à disposition les outils adaptés : poste de travail sécurisé, espace disque et support externe chiffré, services en ligne sécurisés. Le titulaire met à disposition de ses employés des moyens similaires pour la gestion des données sensibles.
* A l’issue de la prestation, le titulaire détruit toutes les informations liées à la prestation, y compris celles des personnes tierces qui auraient éventuellement été impliquées au cours de l’exécution du Contrat. Une preuve de destruction est fournie au responsable du musée du Louvre de la prestation (a minima, un certificat de destruction).

|  |
| --- |
| **Réponse du soumissionnaire :** |

# Gestion des accès et gestion des droits

Le titulaire détaille dans son offre des mécanismes d’authentification et de gestion des droits d’accès suffisamment robustes pour garantir l’authenticité des accès.

Le titulaire réalise une revue régulière des accès et des privilèges sur les parties du Service et les outils dont il a la responsabilité, et met à jour les droits si besoin.

Les comptes d’administration (ceux qui permettent de modifier le fonctionnement du service en lui-même, par opposition à ceux qui en permettent simplement l’usage) sont particulièrement surveillés.

|  |
| --- |
| **Réponse du soumissionnaire :** |

# Cycle de vie des ressources

Le titulaire liste les ressources traitant des informations du musée du Louvre sous sa responsabilité dans le cadre du Contrat, et définit leur cycle de vie, en particulier celui des informations et systèmes. Cet inventaire est maintenu à jour tout au long de la durée du Contrat.

Le titulaire informe systématiquement Le musée du Louvre de toute modification devant survenir sur ces ressources. Cette information est réalisée suffisamment tôt, pour permettre au musée du Louvre d’analyser les impacts de la modification, et de prendre les mesures éventuellement nécessaires.

Lors de la mise au rebut de ressources, le titulaire applique des mesures de sécurité permettant d’assurer la confidentialité des informations.

|  |
| --- |
| **Réponse du soumissionnaire :** |

# Durcissement des composants

Le titulaire :

* Est responsable du choix des composants et bibliothèques impliqués dans l’architecture technique de la solution
* Identifie, applique puis communique au musée du Louvre les mesures de durcissement sur tous les composants techniques impliqués dans l’architecture de la solution
* Applique les mesures de durcissement communiquées par Le musée du Louvre
* Prend en compte les exigences liées au durcissement de certains des socles déjà mis en place par Le musée du Louvre, avec lesquels les codes développés et les composants intégrés dans le cadre du Contrat doivent s’intégrer

Pour information ces mesures de durcissement appliquées ou à appliquer sont communément basées sur les guides publiquement disponibles de l’ANSSI (<https://www.ssi.gouv.fr/administration/bonnes-pratiques/>) bien que cette liste ne soit ni limitative ni exhaustive.

|  |
| --- |
| **Réponse du soumissionnaire :** |

# Réversibilité

Le titulaire met en œuvre des mesures techniques et organisationnelles pour garantir la sécurité des données et des applications qui lui sont confiées, lors du transfert des prestations de la part du précédent titulaire en conformité avec les réglementations applicables. Durant la phase de transfert, l’assurance de la sécurité réside notamment dans :

* La gestion des accès, habilitations ;
* Le transfert de responsabilités ;
* Le transfert de toute la documentation sécurité ;
* La fourniture d’informations nécessitant des mesures de protection adaptées ;
* La gestion de la continuité de l’activité

Les mesures listées ci-dessus sont à réaliser par le titulaire, même en l’absence de phase de réversibilité contractualisée.

|  |
| --- |
| **Réponse du soumissionnaire :** |

# Sécurité liée à l’exploitation

## Procédures et responsabilités liées à l’exploitation

Toute action en production se fait au travers d’un bastion (du titulaire si le service est entièrement sous sa responsabilité, directe ou indirecte ; ou du musée du Louvre si le Service est hébergé par Le musée du Louvre ou l’un de ses sous-traitants). Ce bastion garantit l’authentification des intervenants, le masquage des identifiants réellement utilisés sur le système administré, et la traçabilité des connexions et des actions.

Seules les personnes dûment habilitées sont autorisées à intervenir dans chaque environnement : une revue des personnes intervenant aura lieu avant chaque intervention en production.

|  |
| --- |
| **Réponse du soumissionnaire :** |

## Déploiement

Le titulaire s’assure que :

* Toutes les opérations de déploiement et de retour arrière ont été testées en environnement d’intégration, hors production ;
  + Toutes les conditions de déploiement sont réunies, en particulier :
  + Qu’il ne subsiste pas de défaut de sécurité critique ou majeur ni trop de défauts mineurs ;
* Que la procédure de retour arrière testée est disponible ;
* Qu’une autorisation de déploiement a été formalisée par Le musée du Louvre ;
* L’intégrité des informations déployées (code, configuration, etc.) est vérifiée, si possible par une personne tierce, avant et après le déploiement ;
* Des tests validés par Le musée du Louvre sont réalisés post déploiement pour vérifier la réussite de l’opération.

|  |
| --- |
| **Réponse du soumissionnaire :** |

## Protection contre les logiciels malveillants

Le titulaire met en place des mesures de détection, de prévention et de récupération, conjuguées à une sensibilisation de ses utilisateurs pour se protéger contre les logiciels malveillants.

Idéalement, le titulaire déploie une démarche ISO27001

|  |
| --- |
| **Réponse du soumissionnaire :** |

## Ségrégation entre front-OFFICE et back-office

Si le Service doit être exposé sur Internet, alors le titulaire sépare, fonctionnellement et techniquement, le *front office* du *back office.*

Le back-office n’est pas exposé sur Internet, et un filtrage IP est mis en place pour n’autoriser que les adresses IP source et les ports strictement nécessaires à accéder à cette interface. Sauf justification validée par Le musée du Louvre, seule l’adresse IP de sortie du musée du Louvre est autorisée.

Sauf justification validée par Le musée du Louvre, tous les accès en administration se font au travers du bastion d’administration du musée du Louvre.

|  |
| --- |
| **Réponse du soumissionnaire :** |

# Journalisation

## Système de journalisation

Le titulaire met en place un système de journalisation permettant d’analyser tous les accès au Service et les actions réalisées sur ce dernier. Les journaux doivent être disponibles sur une période minimum de six (6) mois et comporter au minimum :

* L’adresse IP ;
* L’horodatage précis, reposant sur une horloge synchronisée avec un serveur de temps reconnu ;
* Le login utilisé s’il s’agit d’un accès authentifié ;
* Les commandes utilisées ;
* Les données sensibles ou personnelles qui ont été accédées si c’est le cas (que ce soit en lecture, création, modification ou suppression).

Ce système respecte les recommandations de sécurité de l’ANSSI[[1]](#footnote-1). En particulier, les journaux sont :

* déportés sur un serveur distant,
* protégés de toute modification ou suppression,
* accessibles pour exploités, en lecture seule, par le musée du Louvre.

|  |
| --- |
| **Réponse du soumissionnaire :** |

## Traçabilité des utilisateurs du back-office

Le *back-office* du Service n’est accessible que par les utilisateurs légitimes, depuis le SI du musée du Louvre, de manière transparente en termes d’authentification.

Le titulaire met en place des moyens de journalisation sur l’ensemble des éléments qui participent aux traitements sur le *back-office*, pour permettre le suivi détaillé des opérations et d’en identifier l’origine ainsi que l’instant précis.

Dans le cas d’un Service hébergé par Le musée du Louvre, sur demande du musée du Louvre, le titulaire propose une solution pour que ces journaux puissent être transmis au fil de l’eau et de manière sécurisée au SOC du musée du Louvre.

|  |
| --- |
| **Réponse du soumissionnaire :** |

# Gestion des vulnérabilités techniques

## Veille, analyse, maitrise des risques liés aux vulnérabilités

Une vulnérabilité technique est une faille dans l’un des composants du service ou dans l’un des processus (de conception, de développement, de recette ou d’exploitation) qui permettrait potentiellement de porter atteinte, de manière malveillante ou non, sur l’un des critères de sécurité (disponibilité, intégrité, confidentialité et traçabilité), à une donnée ou une fonction essentielle du Service.

Le titulaire s’assure que le Service n’expose pas de vulnérabilité connue pendant toute la durée de vie du Contrat, et maintient donc à jour tous les composants du Service.

Pour cela, le titulaire :

* Met en place les moyens et procédures nécessaires pour identifier et évaluer les vulnérabilités affectant le Service ; et pour identifier puis valider techniquement (analyse, recette, tests de non nocivité) les mesures compensatoires associées (correctifs ou solutions de contournement).
* Maintient à jour la liste des composants du Service sous sa responsabilité avec, pour chacun d’eux, sa version actuelle, sa dernière version disponible et les vulnérabilités corrigées par les éventuelles versions intermédiaires ;
* Se tient informé de toute alerte de sécurité et des mises à jour recommandées, en suivant des bulletin de veille, par exemple et à commencer par celui du CERT-FR[[2]](#footnote-2) ;
* Détermine l’urgence et l’importance des actions qui en découlent.
* Suit et respecte le cycle de vie des OS et composants utilisés par le Service sous sa responsabilité en appliquant les patchs nécessaires.

|  |
| --- |
| **Réponse du soumissionnaire :** |

## Communication avec Le musée du Louvre

Le titulaire communique au musée du Louvre, dans les plus brefs délais et au maximum sous 24h après leur découverte la survenance de toute faille de sécurité pouvant avoir des conséquences directes ou indirectes sur la sécurité du Service ;

## Délais de traitement des vulnérabilités

Le titulaire est garant du maintien en conditions de sécurité du Service et des outils en lignes manipulant des informations du musée du Louvre utilisés pour réaliser les prestations, à ses frais sauf cas particuliers (par exemple, si le maintien en conditions de sécurité est compromis par un changement intervenu hors du périmètre de responsabilité du titulaire et de ses sous-traitants).

Le titulaire précisera les délais d’intervention et de mise à jour en cas de découverte d’une vulnérabilité sur les composants du service ou l’OS selon la criticité de la vulnérabilité et notation CVSS.

Le titulaire pourra proposer une solution de contournement qui sera étudiée par le musée du Louvre

# Audit du Service

Le titulaire autorise Le musée du Louvre à mandater une société d’audit de sécurité afin de réaliser une évaluation d’architecture, de configuration, de code, et réaliser des tests d’intrusion et de conformité.

Ces audits seront réalisés dans un cadre formalisé convenu entre les Parties, et ne concerneront que les briques rentrant dans le fonctionnement du Service, sous la responsabilité du titulaire et de ses sous-traitants.

|  |
| --- |
| **Réponse du soumissionnaire :** |

1. <https://www.ssi.gouv.fr/guide/recommandations-de-securite-pour-la-mise-en-oeuvre-dun-systeme-de-journalisation/> [↑](#footnote-ref-1)
2. [↑](#footnote-ref-2)