

Annexe sécurité des systèmes d'information

Prérequis pour la mise en œuvre d'un service web externalisé « SaaS »

1. Contexte

Cette annexe de sécurité définit les prérequis de l'université Sorbonne Nouvelle (dénommée « USN » dans la suite du document) devant être mis en œuvre contractuellement et techniquement durant toute la durée de la prestation.

Elle vise à garantir la confidentialité, l'intégrité et la disponibilité du service qui est sous la responsabilité de l'USN.

Les versions devront évoluer durant la durée de la prestation selon leurs obsolescences et mises à jour (ex : version de TLS, complexité des mots de passe).

Il appartient au fournisseur de s'aligner sur les standards et référentiels qui concernent les services qu'il propose, utilise ou met à disposition.

Le principe du Security et Privacy-by design devront être appliqués au développement, au déploiement et à l'exploitation.

Le prestataire reconnaît être tenu à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité et de mise à l'état de l'art.

Les éléments de sécurité mis en œuvre seront détaillés dans un plan d'assurance sécurité (PAS) fourni par le soumissionnaire.

Un cadre de réponse est requis pour servir de repérage des éléments de justification de conformité dans le PAS fourni. Les références de type R.X.Y, renvoient à ce cadre de réponse.

2. Identité numérique de l'USN

L'identité de l'USN sur internet est affirmée au travers du nom de domaine (« DNS ») qui se traduit par des noms spécifiques attribués à chaque service sous la forme nom_service.sorbonne-nouvelle.fr

Le fournisseur du service précisera la nomenclature de nommage selon ce principe ou via une URL propre aux fournisseur (ex : sorbonne-nouvelle.editeur.fr) **(R.2.1)**

3. Compatibilité avec les navigateurs Web

Le service devra être compatible avec les navigateurs courants du marché (ordinateurs et mobiles) dans leur version stable à jour (à minima : <https://gs.statcounter.com/>) . Des conditions particulières du CCTP peuvent s'appliquer en priorité. **(R.3.1)**

4. Gestion des authentifications

L'authentification utilisateur doit reposer prioritairement sur le SSO de l'établissement : son serveur CAS <https://cas.sorbonne-nouvelle.fr/> , l'impossibilité d'utilisation doit être justifiée **(R.4.1)** et est soumise à validation de l'établissement.

En cas d'authentification locale strictement nécessaire :

- Un identifiant et mot de passe unique par utilisateur
- Complexité : au minimum de 12 caractères et comportant obligatoirement au moins un caractère spécial, un chiffre et une majuscule
- L'utilisateur doit pouvoir modifier son mot de passe. La règle de complexité doit rester techniquement obligatoire

À fournir :

- La politique de complexité des mots de passe **(R.4.2)**
- Les mesures de sécurité des jetons de session d'authentification, dont la durée de vie et le mécanisme relatif aux cookies (ex : « Secure » flag, Http-Only, Same-site, etc.) **(R.4.3)**
- Les mesures de protections contre les attaques de type force brute sur les comptes utilisateurs locaux **(R.4.4)**
- Les éventuelles règles d'obligations de changement régulier des mots de passe par les utilisateurs pour les comptes locaux **(R.4.5)**
- Eventuellement (ce n'est pas un prérequis strict sauf disposition réglementaire particulière) les solutions de renforcement de l'authentification disponibles (ex : MFA) pour les comptes locaux **(R.4.6)**

5. Gestion des privilèges

Un système de contrôle d'accès basé sur des rôles permettant de différencier les privilèges des utilisateurs doit être détaillé **(R.5.1)**. Le service doit permettre que tout utilisateur puisse se voir attribuer un niveau de privilèges personnalisable (ex : administrateur global, administrateur secondaire, utilisateur simple, etc.)

6. Intégration avec le SI interne de l'USN et d'autres API tierces

Au cas où le service aurait nécessité d'être interconnecté avec le système d'information de l'établissement, fournir :

- La liste et les détails des interactions réseau avec le système d'information interne de l'USN (ex : accès interne à des API ou nécessité de connexion depuis des éléments du SI de l'USN vers le service). **(R.6.1)**
- Les dispositifs de sécurisation d'accès aux API USN et aux API tierces **(R.6.2)**. L'ouverture des API de l'USN sera soumise à validation préalable par la DNUM et sera notamment en fonctions des possibilités de sécurisations présentées.

7. Envoi de courriels

Dans le cas d'envois de courriels par le service avec comme émetteur des adresses @sorbonne-nouvelle.fr, l'architecture cible proposée **(R.7.1)** devra être validée au préalable par l'USN pour conformité avec sa politique (serveurs d'envois, SPF/DKIM, etc).

Aucune demande d'ajout d'enregistrement au DNS de l'USN ne sera acceptée par défaut sans cela.

8. Sécurité des données en transit

Les données échangées entre l'utilisateur et le service doit être chiffré en HTTPS. Le certificat délivré est reconnu par une autorité de certification reconnue.

Le niveau minimum du chiffrement est TLS v 1.2 avec activation de la politique HSTS. La configuration du HTTPS devra correspondre au minimum au niveau « Intermediate » de <https://ssl-config.mozilla.org/> **(R.8.1)**

Dans le cas de l'utilisation du protocole ACME, la préconisation de l'ANSSI <https://cyber.gouv.fr/publications/automatisation-de-la-gestion-des-certificats-avec-acme> devra être appliquée.

Dans le respect du bon fonctionnement du service, l'USN sera susceptible d'exiger, à son appréciation, le renforcement de la configuration en cas de score de sécurité jugé trop bas selon des outils de diagnostic de type <https://www.ssllabs.com/ssltest> ou équivalent.

9. Sécurité des données au repos

Les mots de passe utilisateur ne doivent pas figurer en clair, y compris dans une base de données ou le code en ligne.

À fournir :

- Les méthodes de protection de la sécurité des données utilisateurs et sensibles au repos des mises en œuvre (ex : méthode de hashage AES-256 des mots de passe et des données à caractère personnelles en base de données, pseudonymisation), y compris concernant les sauvegardes **(R.9.1)**

10. Hébergement

L'hébergement du service doit être effectué dans un datacenter au minimum « Tiers 3 », dont le niveau de service comprend (y compris pour les sauvegardes) :

Les mesures de protection contre les incidents environnementaux : incendies, inondations, coupures et surcharges électriques, et la régulation thermique, la climatisation et la gestion de l'humidité ainsi que celles contre les intrusions physiques de tiers extérieurs,

En cas d'hébergement chez un sous-traitant. Les niveaux de service contractuels applicables doivent être fournis.

À fournir :

- Les certifications (ex : ISO 27001) et labellisations (ex : Tiers 3) de l'hébergeur **(R.10.1)**
- Les mesures protections contre les incidents environnementaux (cf. plus haut) **(R.10.2)**
- Les mesures de protection des accès physiques aux serveurs (ex : habilitation par badges restreignant l'accès aux locaux) **(R.10.3)**
- Les éventuelles autres méthodes de résilience de l'infrastructure déployée chez l'hébergeur (ex : Infrastructure-as-a-code) **(R.10.4)**
- La méthode d'hébergement du service, y compris son cloisonnement logiques (ex : Machine virtuelle dédiée ou partagée) **(R.10.5)**

L'hébergement par un sous-traitant dont le siège social est soumis à une juridiction en dehors de l'Union européenne n'est pas autorisé

Fournir :

- La localisation de la juridiction légale de cet hébergeur **(R.10.6)**

11. Sauvegardes, plan de continuité/reprise d'activité

Des sauvegardes doivent prévenir une perte de donnée en cas de problèmes d'intégrité.

La durée de rétention des sauvegardes doit être au minimum de 2 semaines.

La durée maximum de perte d'enregistrement des données acceptable : 24 heures

Au moins un jeu de sauvegarde doit être stocké hors du site de production.

À détailler :

- La fréquence des sauvegardes (RPO) **(R.11.1)**, à minima quotidienne
- Les paliers de durées de rétention (ex : hebdomadaires un mois, mensuelles un an), à minima de deux semaines pour les quotidiennes **(R.11.2)**
- L'organisation des sauvegardes hors-site (ex : 3-2-1) **(R.11.3)**
- L'utilisation, le cas échéant éventuelle d'un dispositif d'immuabilité de protection contre les rançongiciels **(R.11.4)**

Le plan de continuité ou de reprise d'activité du service éventuel pour garantir la résistance aux sinistres graves doit être détaillé. **(R.11.5)**

12. Sécurité du réseau

L'accès réseau au serveur depuis Internet et au sein de l'hébergeur doit être sécurisé par :

- Des éléments de sécurité réseau (ex : Pare-feu, segmentation de réseau, sondes de détections d'intrusion, protection DDoS, etc.) **(R.12.1)**
- La supervision active du service contre les événements anormaux **(R.12.2)**
- Les moyens d'accès à distance pour la télémaintenance (ex : VPN) **(R.12.3)**

13. Disponibilité

Contractuellement l'application doit à minima avoir pour garantie un taux disponibilité contractuel de 99,9% annuel en jour et heure ouvrées **(R.13.1)**

- Le support doit être disponible par téléphone, mail ou système de ticket **(R.13.2)**
- Les garanties contractuelles de taux d'intervention (GTI) et de rétablissement (GTR) sont à fournir, selon le niveau d'incident (mineur, majeur critique) **(R.13.3)**

Un système de pénalités en cas de dépassement doit être mis en œuvre **(R.13.4)**

Des dispositions particulières peuvent figurer dans le CCAP.

14. Architecture de l'application

Les composants du service devront être à l'état de l'art et utilisant de composants reconnus sur le marché.

À fournir **(R.14.1)** :

- L'architecture applicative globale, les systèmes d'exploitation, les composants logiciels employés (ex : PHP, MySQL) et leurs versions

15. Protection contre les attaques Web

Le développement de l'application devra prendre en compte les référentiels de bonnes pratiques de développement sécurisé, notamment le référentiel OWASP contre les attaques Web usuelles (ex : injections SQL, XSS, etc.) **(R.15.1)**

Il mettra en place les protections d'en-tête http usuelles (ex : CSP, X-Frame Policy, etc.) avec un niveau au minimum B selon <https://developer.mozilla.org/en-US/observatory> **(R.15.2)**

L'utilisation de mots de passe dans le code est interdite.

Dans le respect du bon fonctionnement du service, l'USN sera susceptible d'exiger, à son appréciation, le renforcement de la configuration en cas de score de sécurité jugé trop bas selon des outils de diagnostic de type <https://developer.mozilla.org/en-US/observatory> ou équivalent.

16. Développements et gestion de projet

Le prestataire est tenu d'assurer la sécurité des développements conformément à l'état de l'art dans chacune des technologies mises en œuvre.

À fournir :

- La gestion de sécurité du projet (ex : validation RSSI, PSSI dédiée, analyses de risques et mesures de sécurité associées, homologation, etc.), moyens de sécurité RH (ex, (formations SSI, clauses de confidentialité, gestion des accès logiques et physiques) **(R.16.1)**
- Les méthodes de sécurisation du processus de développement du projet, la séparation des environnements de développement et de production, le versionnage (ex : CI/CD, Git) **(R.16.2)**
- La méthodologie de revue de sécurité du code (peer-reviewing, audits statiques, audits via le réseau, etc.) et la mise en œuvre éventuelles d'audits de sécurité **(R.16.3)**

17. Maintien en conditions de sécurité

Les serveurs, système d'exploitation, composants logiciels employés, applications et tout composant technique doivent être dans des versions de sécurité à jour et maintenues par leurs développeurs, éditeurs ou mainteneurs.

Le fournisseur ne peut conditionner ses garanties de bon fonctionnement de fournitures ou prestations qu'il fournit à l'emploi de composants dans une version non supportée.

Dans le cas d'une maintenance applicative ou systèmes incluse dans le service, l'application des correctifs de sécurité d'un niveau de sévérité élevé (Score CVSS v3 supérieur à 7) doit-être au maximum de 72 heures après publication. **(R.17.1)**

Le délai comprend les tests de non régression.

Les correctifs d'un niveau inférieur doivent être appliqués sous un délai inférieur à trente jours.
(R.17.2)

En cas d'interruption de service pour maintenance, le chef de projet USN doit être prévenu au moins 48 heures préalablement. **(R.17.3)**

18. Journaux d'événements

La politique de gestion des journaux d'événements (Logs) doit être en accord avec la législation.

A fournir :

- La nature des informations journalisées (ex : horodatage, IP, action spécifique) **(R.18.1)**
- La durée de rétention **(R.18.2)** à minima de six mois pour les événements de sécurité

19. Gestion d'incidents et contacts sécurité

Sera fournie :

- La politique de gestion d'incident **(R.19.1)**

Le circuit d'alerte en cas d'incident de disponibilité, d'intégrité ou de confidentialité devra comprendre **(R.19.2)** :

- Le responsable de projet fonctionnel désigné par l'USN
- Les Responsables de la sécurité des systèmes d'information, à l'adresse rssi@sorbonne-nouvelle.fr
- En cas d'incident concernant aussi les données à caractère personnel, le Délégué à la protection des données à caractère personnelles à l'adresse dpd@sorbonne-nouvelle.fr

20. Accompagnement à l'usage sécurisé pour les administrateurs fonctionnels

Si l'usage du service le nécessite par les administrateurs fonctionnels de l'USN en conditions de sécurité nécessite des précautions, les modalités de cet accompagnement sera précisé **(R.20.1)**

21. Audit de sécurité

L'établissement se réserve de pouvoir, à tout moment, contrôler que les exigences de sécurité sont satisfaites par les dispositions prises par le prestataire.

Le périmètre et la périodicité des audits de sécurité sont définis précisément par les points de contact sécurité de l'établissement comme défini dans l'article « Contacts sécurité ».

Les audits peuvent être réalisés par l'établissement, ou délégués à un tiers.

Le contrôle s'effectuera selon des modalités contractuelles définies (visite des locaux du prestataire avec interviews individuelles des membres des équipes du prestataire, accès aux machines mises à la disposition du prestataire) par les points de contacts sécurité.

Cette visite sera notifiée au prestataire selon un délai de 15 jours.

La pratique de tests intrusifs par le prestataire est interdite sur tout ou partie du système d'informations de l'établissement.

Le client doit se réserver le droit de requérir l'expertise d'un organisme ou d'une société tierce présentant des compétences en matière de sécurité.

De plus, l'USN se réserve le droit de procéder à des audits de sécurité, dont par le biais :

- D'outils de sécurité réseau de type Tenable, ZAP, Nikto ou équivalent
- De services externes automatisés comme, par exemple Scan'er de Renater ou Silene du CERT-FR
- Des outils d'audits de code statiques

Dans le respect du bon fonctionnement du service, l'USN sera susceptible d'exiger, à son appréciation, le renforcement de la configuration en cas de score de performances jugé trop bas selon des outils de diagnostic de type <https://www.webpagetest.org/>, <https://pagespeed.web.dev/>, <https://gtmetrix.com/> ou équivalent.

22. Réversibilité

A l'issue de la prestation, les données doivent être retournées à l'USN dans un format ouvert et exploitable.

À fournir :

- La méthode de mise en œuvre de la réversibilité, dont le format des données retournées et le délai. Les données seront fournies dans un format ouvert (ouverts (SQL, XML, format plat type MD...) **(R.21.1)**
- Le justificatif de destruction des données à l'issue du contrat **(R.21.2)**

23. Transactions financières

Au cas où le service mette en œuvre des transactions bancaire ou financières (ex : paiement en ligne, virement de financements, etc.), seront fournis les justificatifs de certification applicables du prestataire sous-traitant (ex : PCI-DSS, DSP2, etc.) **(R.23.1)**