**Marché public de services**



**CLAUSES DE SECURITE DES SYSTEMES D’INFORMATION**

**- ANNEXE n°4 du CCTP -**

**OBJET :**

***«*Fourniture de prestations de développement, qualification, diffusion et formation, des applications nationales pour les Missions Nationales de la DSI² de la région académique Occitanie *»***

**Référence : DSI2\_BDMN\_2501**

**Direction des Systèmes d’Information et de l’Innovation (DSI²)**

**Table des matières**

[**Clauses générales de sous-traitance** 3](#_Toc194573626)

[**Exigences générales de sécurité** 4](#_Toc194573627)

[**Ressources humaines** 5](#_Toc194573628)

[**Poste de travail** 6](#_Toc194573629)

[**Hébergement** 7](#_Toc194573630)

[**Maintenance et télémaintenance** 8](#_Toc194573631)

[**Solutions applicatives** 9](#_Toc194573632)

[**Intervention du titulaire dans les locaux du Rectorat** 10](#_Toc194573633)

[**Obligations spécifiques liées aux prestations de développement** 11](#_Toc194573634)

# **Clauses générales de sous-traitance**

Les supports informatiques et documents fournis par le rectorat de la région académique Occitanie au titulaire restent la propriété du rectorat de la région académique Occitanie.

Les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel (article 226-13 du code pénal), il en va de même pour toutes les données dont le titulaire prend connaissance à l’occasion de l’exécution du présent marché.

Conformément à l’article 32 du règlement européen sur la protection des données (UE) 2016/679, le titulaire et le Rectorat de région académique Occitanie mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

Le titulaire s’engage donc à respecter les obligations suivantes et à les faire respecter par son personnel.

* Ne prendre aucune copie des documents et supports d’informations qui lui sont confiés, à l’exception de celles nécessaires à l’exécution de la présente prestation prévue au marché, l’accord préalable du maître du fichier est nécessaire ;
* Ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées au présent marché ;
* Ne pas divulguer ces documents ou informations à d’autres personnes, qu’il s’agisse de personnes privées ou publiques, physiques ou morales ;
* Prendre toutes mesures permettant d’éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d’exécution du marché ;
* Prendre toutes mesures de sécurité, notamment matérielles, pour assurer la conservation et l’intégrité des documents et informations traités pendant la durée du présent marché ;
* Et en fin de marché, à procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations saisies.

À ce titre, le titulaire ne pourra sous-traiter l’exécution des prestations à une autre société, ni procéder à une cession de marché sans l’accord préalable du Rectorat de région académique Occitanie.

Le Rectorat de région académique Occitanie se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées par le titulaire.

# **Exigences générales de sécurité**

|  |  |  |
| --- | --- | --- |
| **Réf.** | **Exigences titulaire** |  |
| SSI\_EX\_GEN\_01 | Le référentiel général de sécurité (RGS) et la PSSI Etat s'appliquent aux marchés du Rectorat, sans qu'il soit besoin que le cahier des charges en fasse mention explicitement. | Oui |
| SSI\_EX\_GEN\_02 | Les composants logiciels doivent fonctionner avec des versions supportées par l'éditeur ou la communauté Open Source qui les produisent. | Oui |
| SSI\_EX\_GEN\_03 | La responsabilité du maintien en condition de sécurité du titulaire comprend les composants et services développés en propre, mais aussi ses composants et dépendances amont (librairies, cadriciels (Framework), environnement d'exploitation, API tierces) ou sous-traités. | Oui |
| SSI\_EX\_GEN\_04 | Le titulaire 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, sauf à démontrer une contrainte supérieure et proposer à ses frais des moyens de cantonner les risques, ou démontrer que les risques sont négligeables dans le contexte d'emploi. | Oui |
| SSI\_EX\_GEN\_05 | Le maintien en condition opérationnelle inclut le maintien en condition de sécurité et donc la mise en œuvre des correctifs de failles de sécurité. | Oui |
| SSI\_EX\_GEN\_07 | La sécurisation des systèmes informatiques dépend de l'évolution des technologies. Il appartient au titulaire du marché de s'aligner sur les standards et référentiels qui concernent les services qu'il propose, utilise ou met à disposition. | Oui |
| SSI\_EX\_GEN\_08 | Les politiques de sécurité convergent pour exiger les mises à jour des composants logiciels vers des versions supportées par l'éditeur ou la communauté Open Source qui les produisent. Dans ces conditions, une vérification d'aptitude au bon fonctionnement ou au service régulier (VABF et VSR) est refusée si des composants ne sont pas à jours des correctifs de failles de sécurité. | Oui |

|  |  |  |
| --- | --- | --- |
| **Réf.** | **Exigences candidat** |  |
| SSI\_EX\_GEN\_04 | Le candidat 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, sauf à démontrer une contrainte supérieure et proposer à ses frais des moyens de cantonner les risques, ou démontrer que les risques sont négligeables dans le contexte d'emploi. | Oui |
| SSI\_EX\_GEN\_06 | Afin de démontrer de manière économique la réalité de leurs efforts pour sécuriser les composants impliqués dans le marché, **candidats** et titulaires sont invités à présenter des labels et certificats qui permettent au Rectorat d'avoir un premier niveau d'assurance au cours de l'évaluation des offres.  Ces qualifications peuvent parfois être globales (ISO27000), partielles (référentiel en Tiers 1 à 4 pour l'hébergement), ou très ponctuelles (rapports de test de l'état de l'art sur des interfaces spécifiques). | Oui |
| SSI\_EX\_GEN\_09 | Durant la préparation ou la réalisation du marché, le Rectorat peut conduire ou mandater des contrôles et audits de sécurité informatique des fournitures, prestations, moyens utilisés et services proposés par le candidat ou titulaire, et leurs sous-traitants. | Oui |

# **Ressources humaines**

|  |  |  |
| --- | --- | --- |
| **Réf.** | **Exigences titulaire** |  |
| SSI\_RH\_01 | Le titulaire s’engage à fournir une liste régulièrement mise à jour, des personnels autorisés à intervenir sur le système d’information du Rectorat, ainsi que leur niveau d’habilitation (types d’accès et ressources concernées du client). | Oui |
| SSI\_RH\_02 | Le titulaire précisera les moyens mis en œuvre, dans le cadre de son processus de recrutement du personnel, pour vérifier les éventuelles condamnations, le cursus et l’expérience professionnelle des futurs employés. | Oui |
| SSI\_RH\_06 | Les personnels du titulaire devront respecter la charte d’usage du système d’information du Rectorat lors de toute intervention à l’installation ou en maintenance. Le titulaire s’engage à en informer ses personnels. | Oui |

|  |  |  |
| --- | --- | --- |
| **Réf.** | **Exigences candidat** |  |
| SSI\_RH\_03 | Si le candidat ou des employés de son entreprise possèdent une habilitation au niveau Confidentiel-Défense, il pourra en faire mention. | Oui |
| SSI\_RH\_04 | Le candidat précisera dans son offre si d’autres clients peuvent accéder aux mêmes locaux que ceux utilisés par le maître d’ouvrage et dans quelle mesure il sera possible de limiter ces accès à la demande de ce dernier. | Sans objet |
| SSI\_RH\_05 | Le candidat indiquera dans sa réponse les qualifications, diplômes ainsi que le niveau d’expérience des personnels retenus pour la réalisation des prestations d’infogérance. | Oui |

# **Poste de travail**

|  |  |  |
| --- | --- | --- |
| **Réf.** | **Exigences titulaire** |  |
| SSI\_PDT\_01 | Les postes de travail du titulaire qui se connecteront au réseau du Rectorat, localement ou à distance, doivent disposer :   * D’un système d’exploitation à jour et maintenu à jour ; * D’un anti-virus ou d’un dispositif de lutte contre les logiciels malveillants à jour et maintenu à jour. * D’un chiffrement pour réduire les risques de fuite de données en cas de vol ou de perte du matériel. | Oui |
| SSI\_PDT-01 | Le rectorat met en œuvre des mesures de sécurité visant à cloisonner les flux de données et les matériels connectés à son réseau. | Oui |

# **Hébergement**

|  |  |  |
| --- | --- | --- |
| **Réf.** | **Exigences titulaire** |  |
| SSI\_HEB\_01 | Le titulaire doit prendre toutes les mesures qui s’imposent en termes de sauvegarde et de restauration pour se conformer au niveau de service exigé.  Les opérations de sauvegardes donnent lieu à un compte-rendu par messagerie avec indicateur de réussite ou d’échec. | Sans objet |
| SSI\_HEB\_02 | Le titulaire doit prendre des mesures permettant de garantir la confidentialité des données relatives aux sauvegardes :   * Confidentialité des flux lors des opérations de sauvegardes ; * Stockage sécurisé des sauvegardes. | Sans objet |
| SSI\_HEB\_03 | En cas de sauvegarde externalisée, le Rectorat doit être informé du nom du prestataire et les sauvegardes doivent être chiffrées avant leur transfert et la clé de chiffrement connue seulement du titulaire et du donneur d’ordres. | Sans objet |
| SSI\_HEB\_05 | En cas de sinistre, le titulaire indiquera les mesures techniques, organisationnelles, procédurales de reprise d’activité. | Sans objet |

|  |  |  |
| --- | --- | --- |
| **Réf.** | **Exigences candidat** |  |
| SSI\_HEB\_04 | Le candidat indiquera les mesures techniques, organisationnelles, procédurales qu’il s’engage à prendre pour assurer la continuité d’activité du système d’information. | Sans objet |
| SSI\_HEB\_06 | Le candidat décrira les moyens mis en œuvre afin d’assurer la continuité des services essentiels (énergie, climatisation, télécommunications) sur le site d’exploitation du système :   * Situation et caractéristiques générales du site d’exploitation ; * Protection et redondance électriques (groupes électrogènes, onduleurs, protection contre les surtensions, etc.) ; * Contrats de service avec les fournisseurs d’accès, caractéristiques des liaisons de secours ; * Systèmes de climatisation ; * Moyens de supervision et remontées d’alarme ; * Les équipements utilisés par le système du donneur d’ordres, en particulier les composants redondants seront décrits (alimentations, disques, cartes contrôleurs, serveurs, équipements réseau, liens réseau) ;   Le candidat précisera les éventuels agréments gouvernementaux ou certificats de conformité qu’il détient. | Sans objet |

# **Maintenance et télémaintenance**

|  |  |  |
| --- | --- | --- |
| **Réf.** | **Exigences titulaire** |  |
| SSI\_MNT\_01 | Le titulaire précisera quelle est sa politique de sécurité vis-à-vis des failles de type 0-day, quel est le délai de correction actuellement appliqué et quel est le mode de diffusion à ses clients. | Sans objet |
| SSI\_MNT\_02 | Le titulaire précisera si sa solution est maintenue en tenant compte des recommandations d'application de correctifs par les éditeurs des briques logicielles utilisées et avec quels délais sont appliquées les mises à jour. | Sans objet |
| SSI\_MNT\_03 | Le titulaire précisera quels sont les moyens mis en œuvre dans l’environnement de production afin de tracer les évènements systèmes (logs de serveurs web, d’authentification etc…). Il précisera si l’architecture de sa solution permet d’avoir une gestion des journaux (logs) centralisée et les logiciels utilisés pour le faire (Rsyslog par exemple). | Sans objet |
| SSI\_MNT\_04 | La connexion de télémaintenance doit se faire à travers la passerelle Internet sécurisée mise à disposition par le Rectorat (VPN IPSEC). | Oui |
| SSI\_MNT\_05 | Les clés permettant l’accès à distance au réseau du Rectorat sont nominatives et personnelles. Il est de la responsabilité du titulaire d’assurer la sécurité physique de ces clés et qu’elles ne soient pas cédées, même temporairement, à des personnes non autorisées. | Oui |
| SSI\_MNT\_06 | Le titulaire doit avoir une politique anti-virus et de mise à jour des correctifs de sécurité appliquée sur les postes de télémaintenance. | Oui |
| SSI\_MNT\_07 | Le titulaire précisera si les postes de télémaintenance sont physiquement isolés du réseau local du titulaire. | Oui |
| SSI\_MNT\_08 | Le titulaire accepte d’utiliser le bastion d’administration du Rectorat pour accéder aux systèmes qu’il devra maintenir (de fait l’accès direct aux serveurs et applications sera interdit). Selon les besoins d’intervention l’accès aux systèmes à maintenir sera ouvert et fermé par la DSI² à la demande du mainteneur ou de la personne habilitée selon le protocole défini dans les conditions de la maintenance. Tout autre mode de fonctionnement devra être validé avec la DSI et le RSSI. | Oui |
| SSI\_MNT\_09 | Le titulaire pourra établir un Plan Assurance Sécurité (PAS) afin de faire connaitre les dispositions de sécurité qu’il met en place pour sa prestation. Le PAS traite :   * Des critères de sécurités utilisés dans la désignation des personnes chargées des interventions. * De la désignation des sites d’exécution de la prestation, protection et accès physiques des locaux utilisés. * Des règles de protections des informations du Système d’Information associées à la prestation de télémaintenance. * De l’architecture générale de la plateforme d’intervention (cloisonnement technique etc.). * Des accès logiques à la plateforme, identification et authentification, mise en veille, déconnexion automatique, gestion des droits, traçabilité… * Des dispositions prises pour assurer la continuité de l’activité après un sinistre ou un incident majeur. * De l’assurance et des contrôles de la sécurité des services de l’intervention fournis. | Oui |

# **Solutions applicatives**

|  |  |  |
| --- | --- | --- |
| **Réf.** | **Exigences titulaire** |  |
| SSI\_APP\_01 | Le titulaire s’engage à fournir une liste exhaustive des logiciels installés, documentée, contenant les informations détaillant chaque logiciel ainsi que les interactions entre eux. | Oui |
| SSI\_APP\_02 | Les interfaces des applications web doivent être utilisables par des navigateurs à l'état de l'art (part de marché cumulée supérieure à 50%), sans générer d'alerte de sécurité et sans module d'extension. | Sans objet |
| SSI\_APP\_03 | Le titulaire attestera que le processus d’authentification des utilisateurs est totalement encrypté par des protocoles à l’état de l’art (Ex : TLS pour le HTTPS). | Sans objet |
| SSI\_APP\_04 | Les communications entre l’application et les navigateurs des utilisateurs doivent être chiffrées. Le titulaire précisera dans sa réponse si c’est le cas pour l’intégralité des pages, dans le cas contraire il précisera celles qui ne le sont pas. | Sans objet |
| SSI\_APP\_05 | La solution du titulaire doit supporter les connexions TLS (https) pour authentifier la source et chiffrer les communications. | Sans objet |
| SSI\_APP\_06 | Le titulaire précisera s’il effectue un contrôle rigoureux des entrées utilisateurs (en particulier afin d’éviter les failles de type XSS (cross side scripting) et de quelle façon ce contrôle est effectué.  Il précisera si une revue de son code a été effectuée dans une optique sécurité. | Sans objet |
| SSI\_APP\_07 | Le titulaire précisera comment sont stockés les mots de passe des utilisateurs et quelles sont les politiques applicables en termes de mots de passe (longueur, présence de caractères alphanumériques obligatoires, possibilité de paramétrages des éléments, etc.) | Sans objet |
| SSI\_APP\_08 | Le titulaire précisera la liste des en-têtes de sécurité mis en œuvre dans l’application afin d’activer les protections des navigateurs. | Sans objet |
| SSI\_APP\_09 | Les cookies ou jetons de session doivent avoir un marquage approprié pour se protéger des vols ou exploitations de sessions déjà ouvertes.  Le titulaire précisera dans sa réponse les cookies nécessaires au fonctionnement de l’application, leur rôle et le marquage associé. | Sans objet |
| SSI\_APP\_10 | Le titulaire précisera si son application fonctionne sans restriction dans le mode navigation « Incognito » proposé par les navigateurs. | Sans objet |
| SSI\_APP\_11 | Dans le cas où des documents peuvent être télé-versés (upload) dans la solution, le titulaire précisera si un interfaçage est possible avec un antivirus. | Sans objet |

|  |  |  |
| --- | --- | --- |
| **Réf.** | **Exigences candidat** |  |
| SSI\_APP\_12 | Un contrôle de non contamination des serveurs Web de production pourra être effectué périodiquement. Le candidat précisera les modalités de mise en œuvre de ce contrôle. | Sans objet |

# **Intervention du titulaire dans les locaux du Rectorat**

|  |  |  |
| --- | --- | --- |
| **Réf.** | **Exigences titulaire** |  |
| SSI\_INT\_01 | Respect des exigences de sécurité du Rectorat : au même titre que les agents du Rectorat, le titulaire doit prendre connaissance et appliquer les règlements internes du Rectorat (PSSI, directive d’utilisation des systèmes d’information, directive d’utilisation de la messagerie, etc.). | Oui |
| SSI\_INT\_02 | Respect des standards et méthodologies du Rectorat : le titulaire doit respecter les standards et les méthodologies préconisés au sein du Rectorat. | Oui |
| SSI\_INT\_03 | Respect du périmètre de la prestation : le titulaire ne tente pas d’accéder à des informations ou des ressources informatiques ne faisant pas partie du périmètre de la prestation. | Oui |
| SSI\_INT\_04 | Connexion d’équipements au réseau du Rectorat : le titulaire doit connecter sur le réseau interne du Rectorat uniquement des équipements autorisés par le Rectorat. Cela comprend tout type de matériel y compris les supports de stockage amovibles (clés ou disques dur USB, etc.) | Oui |
| SSI\_INT\_05 | Recensement des comptes d’accès : le titulaire tient à jour la liste exhaustive des comptes d’accès au SI du Rectorat existants ainsi que des rôles et privilèges qui y sont associés. Il doit être en mesure de fournir cette liste au Rectorat sur demande. | Oui |
| SSI\_INT\_06 | Restitution des informations collectées par le titulaire : à la fin de la prestation, le titulaire doit restituer ou détruire les informations du Rectorat en sa possession. Un procès-verbal de destruction des données doit être signé par le titulaire. | Oui |
| SSI\_INT\_07 | Transfert de connaissances : le titulaire doit préciser la date exacte de départ des intervenants de la prestation et organiser le transfert de connaissances auprès des équipes du Rectorat. | Oui |

# **Obligations spécifiques liées aux prestations de développement**

|  |  |  |
| --- | --- | --- |
| **Réf.** | **Exigences titulaire** |  |
| SSI\_DEV\_01 | Utilisation du cadre standard de développement : le titulaire doit utiliser le cadre commun de développement (méthodes, démarches, etc.) du Rectorat comprenant notamment :   * l’organisation des équipes de développement et de la prestation ; * les configurations matérielles préconisées pour le développement ; * les outils de développement préconisés par le Rectorat (logiciels, versions, etc.) ; * une structure de développement (framework) intégrant les fonctions de sécurité. | Oui |
| SSI\_DEV\_02 | Propriété du code : le Rectorat est propriétaire du code et des droits de propriété intellectuelle des éléments développés dans le cadre de la prestation. | Oui |
| SSI\_DEV\_03 | Ségrégation des environnements : le titulaire doit utiliser différents environnements cloisonnés pour les activités de développement, de recette et de pré-production. | Oui |
| SSI\_DEV\_04 | Documentation du code : le titulaire doit commenter et documenter le code développé dans le cadre de la prestation. La documentation doit être mise à jour régulièrement. | Oui |
| SSI\_DEV\_05 | Traçabilité des actions de développement : toute activité de développement doit être tracée et conservée dans un format facilitant son exploitation ultérieure. | Oui |
| SSI\_DEV\_06 | Sauvegarde des codes sources : le titulaire doit sauvegarder et conserver  chaque version du code source recettée dans le cadre de la prestation. Les accès à ces sauvegardes devront être tracés. | Oui |
| SSI\_DEV\_07 | Dépôt des codes source : le titulaire doit déposer les codes sources dans ses différentes versions et mises à jour selon les recommandations du Rectorat. | Oui |
| SSI\_DEV\_08 | Conduite des tests : lors de la conduite de tests de validation ou du déploiement, le titulaire doit :   * utiliser des données de tests anonymisées ; * ne pas provoquer de perturbations du système d’information du Rectorat lors des séances de test ; * remettre en l’état initial les systèmes testés et réinitialiser le matériel sensible   ne pas introduire de régression vis-à-vis d’un état de sécurité atteint dans une version précédente |  |
| SSI\_DEV\_09 | Contrôle de la qualité et de la sécurité du développement : le Rectorat se réserve le droit de contrôler la qualité et la sécurité du développement fourni par le titulaire, via des audits et/ou des tests d’intrusion par exemple  (audit de code sur les parties les plus sensibles, etc.). |  |