
ANNEXE CYBERSECURITE

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES

**CHAMBRE DE COMMERCE ET D'INDUSTRIE
DE CORSE**

Sommaire

1	PRESENTATION GENERALE	3
2	OBJET DU DOCUMENT	3
3	PERIMETRE	3
4	EXIGENCES GENERALES	3
4.1	ORGANISATION ET CONTRAT	3
4.2	ETHIQUE	4
4.3	PROPRIETE INTELLECTUELLE	4
5	EXIGENCES PARTICULIERES LIEES AUX ACTIVITES DU PRESTATAIRE	4
5.1	COMPETENCES DES INTERVENANTS	4
5.2	DOCUMENTATION	5
5.3	METHODES ET OUTILS	5
5.4	ACCES	6
5.5	DEVELOPPEMENT / INTEGRATION	6
5.6	TRAÇABILITE ET LIVRAISON	7
5.7	VEILLE	7
6	PROTECTION DU SYSTEME D'INFORMATION DU PRESTATAIRE	7
6.1	EXIGENCES GENERALES	7
6.2	EXIGENCES RELATIVES AUX OUTILS ET A L'ENVIRONNEMENT DE DEVELOPPEMENT	7
6.3	EXIGENCES RELATIVES AUX PLATEFORMES DE TESTS ET D'INTEGRATION	8
6.4	EXIGENCES RELATIVES AUX OUTILS DE MAINTENANCE	8
6.5	EXIGENCES RELATIVES AUX OUTILS DE TELEMANTENANCE	8
6.6	USAGE DE PLATEFORMES DE TRAVAIL COLLABORATIF	9
7	EXIGENCES RELATIVES AUX INTERVENTIONS D'INTEGRATION ET DE MAINTENANCE CHEZ LE COMMANDITAIRE	9
7.1	PROTOCOLE D'INTERVENTION	9
7.2	BONS COMPORTEMENTS	9
7.3	MOYENS UTILISES LORS DE L'INTERVENTION	10
7.4	RAPPORT D'INTERVENTION	10
8	EXIGENCES RELATIVES AUX OPERATIONS D'EXPLOITATION ET ADMINISTRATION DES SYSTEMES	10
8.1	EXIGENCES RELATIVES A L'EXPLOITATION	10
8.2	EXIGENCES RELATIVES A L'ADMINISTRATION	11
8.3	EXIGENCES RELATIVES A LA SECURITE DES MATERIELS ET LOGICIELS	11
8.4	EXIGENCES RELATIVES A LA CONTINUITE D'ACTIVITE	11
9	ANNEXES	11
9.1	ANNEXE 3 REFERENCES DOCUMENTAIRES	11
9.2	ANNEXE 4 ECHELLE DE CONFIDENTIALITE DU COMMANDITAIRE	13
10	GLOSSAIRE	13
10.1	ACRONYMES	13

1 Présentation générale

Dans le cadre des opérations quotidiennes mises en œuvre sur les systèmes d'information de la CCI de Corse, certaines tâches sont confiées à des prestataires qui s'engagent à respecter des exigences techniques et organisationnelles relative à la sécurité.

2 Objet du document

Le document a pour objet de définir une liste d'exigences de sécurité applicables à un prestataire en fonction du périmètre et de la nature de la prestation.

3 Périmètre

Les exigences génériques applicables à l'ensemble des prestataires sont formalisées au chapitre 4. Les exigences décrites ci-dessous sont applicables en fonction de la nature de la prestation :

- Mise en œuvre d'un système d'informations
- Traitement de données appartenant au commanditaire
- Intégration de systèmes d'information
- Maintenance
- Support de proximité
- Exploitation et administration de systèmes d'information

« Commanditaire » désigne la Chambre de Commerce et d'Industrie de Corse.

« Prestataire » désigne le titulaire.

4 Exigences générales

Les exigences listées dans ce chapitre portent sur les aspects suivants : juridique, organisationnel, responsabilité et impartialité du prestataire d'intégration et de maintenance. Elles doivent être précisées dans le cadre du contrat établi entre le commanditaire et le prestataire.

4.1 Organisation et contrat

a) Le prestataire doit être une entité ou une partie d'une entité dotée de la personnalité morale de façon à pouvoir être tenu juridiquement responsable de sa prestation.

b) Le prestataire a, en sa qualité de professionnel, un devoir de conseil vis-à-vis du commanditaire.

c) Le prestataire d'intégration et de maintenance réalise ses prestations dans le cadre d'une convention (ou d'un contrat) préalablement approuvée par le commanditaire.

- La loi applicable à la convention est la loi française.
- La convention doit préciser les exigences en matière de cybersécurité comme par exemple le niveau de cybersécurité visé pour le système objet de la prestation.
- Il est recommandé que le commanditaire identifie dans la convention de service les éventuelles exigences légales et réglementaires spécifiques auxquelles il est soumis et notamment celles liées à son secteur d'activité.

d) Le prestataire doit décrire l'organisation de son activité d'intégration et de maintenance en termes de cybersécurité au bénéfice de chaque commanditaire.

e) Le prestataire doit mettre en place une chaîne de responsabilité de la cybersécurité pour les besoins de ses prestations. En particulier, il doit définir un point de contact pour la cybersécurité lors de la prestation, qui sera en charge : de la liaison avec la chaîne de responsabilité du commanditaire, de la garantie du respect de la politique de cybersécurité, de la communication sur les divergences par rapport aux exigences et des éventuelles non-conformités.

f) Le prestataire doit accepter les audits demandés par son commanditaire ayant pour objectif de vérifier que l'ensemble des mesures de cybersécurité demandées contractuellement sont bien appliquées. Ces audits seront limités aux moyens techniques et organisationnels relatifs à la prestation et respecteront la déontologie des audits. Il est conseillé de suivre le référentiel d'exigences définies pour les prestataires d'audits à la sécurité des systèmes d'information [PASSI].

g) Le prestataire doit fournir au commanditaire un Plan d'Assurance Sécurité (PAS) pour les prestations qu'il effectue, détaillant la prise en compte des aspects liés à la cybersécurité lors des différents types de prestations d'intégration et de maintenance qu'il effectue, répondant aux exigences de cybersécurité demandées par ce dernier.

4.2 Ethique

a) Le prestataire doit disposer d'une charte d'éthique que l'ensemble de ses intervenants doit signer.

b) Dans le cas où le prestataire intervient comme expert technique pour le compte d'un autre prestataire, il devra respecter les règles de déontologie et en particulier garantir son impartialité. Sauf cas exceptionnel où le prestataire est le seul compétent dans un domaine, il ne pourra pas être expert pour un système qu'il a lui-même intégré ou pour lequel il dispose d'un contrat (contrat de maintenance par exemple).

4.3 Propriété intellectuelle

La propriété intellectuelle, et en particulier celle des codes sources développés ou intégrés par le prestataire pour le système du commanditaire doit être précisée dans la convention ou le contrat passé entre le prestataire et le commanditaire.

De manière générale, le prestataire s'engage à fournir à la demande, et à l'issue de la prestation, l'intégralité des données dont le commanditaire est propriétaire, et ce dans un format exploitable.

5 Exigences particulières liées aux activités du prestataire

L'objectif n'est pas de détailler des exigences pour chaque activité mais d'insister sur des points spécifiques.

5.1 Compétences des intervenants

a) Le prestataire doit s'assurer, pour chaque prestation, que les intervenants désignés pour réaliser la prestation ont les qualités et les compétences requises en matière de cybersécurité. De ce fait, les intervenants :

- Doivent avoir suivi une formation en cybersécurité des systèmes ;
- Devraient être habilités à la cybersécurité par le prestataire. (L'habilitation est un acte formel par lequel le prestataire déclare qu'un intervenant est compétent sur son domaine d'habilitation)
- Doivent justifier d'une expérience suffisante (supérieure à deux ans).

b) Le prestataire doit fournir les procédures d'installation et d'exploitation et les consignes de sécurité liées aux systèmes déployés.

5.2 Documentation

- a) Le prestataire doit s'assurer que les informations relatives à ses activités avec le commanditaire sont traitées avec un niveau de confidentialité suffisant. En l'absence d'exigences particulières du commanditaire, l'ensemble des documents relatifs à la conception, à la configuration ou au fonctionnement du système doivent être considérés de niveau «TLP:AMBER» (cf §9.2).
- b) Si le prestataire est en mesure de traiter des informations et documents sensibles et/ou utiliser des systèmes d'information critiques soumis aux normes et réglementations de cybersécurité en vigueur dans le secteur, ces informations, devront être considérées de niveau « Diffusion Restreinte » ou d'un niveau de confidentialité adapté compte tenu du contexte. Les exigences spécifiques sont disponibles dans l'instruction interministérielle relative à la protection des systèmes d'information sensibles [II_901].
- c) Le prestataire ne doit pas accéder aux données de production contenues sur les systèmes déployés. Le traitement de ces données est limité au commanditaire.
- d) Le prestataire doit être en mesure de détruire tout ou partie des informations relatives au projet sur simple demande écrite du commanditaire. Le prestataire doit être en mesure d'apporter la preuve de la destruction de ces informations. Pour les informations sensibles le prestataire doit se référer aux instructions figurant dans [II_901].

5.3 Méthodes et outils

- a) Le prestataire est responsable des méthodes et outils (logiciels ou matériels) utilisés par ses intervenants et de leur bonne utilisation (précautions d'usage, maîtrise de la configuration, etc.). Pour cela, il doit mettre en œuvre un processus de formation des intervenants à ses outils et assurer une veille technologique sur les mises à jour, la pertinence de ces outils ainsi que les risques éventuels liés à leur utilisation.
- b) Le prestataire susceptible de stocker des données du commanditaire doit utiliser un équipement maîtrisé chiffré, sécurisé à l'état de l'art, validé par le commanditaire.
- b) Le prestataire doit disposer des licences valides des outils (logiciels ou matériels) utilisés pour la réalisation de la prestation. Il ne doit utiliser que des outils que l'éditeur s'engage à maintenir.
- c) Les intervenants ne recourent qu'aux méthodes et outils validés par le commanditaire.

Remarque : cela signifie de prendre en compte les outils et méthodes nécessaires pour les situations d'intervention lors de réponse aux incidents et autres modes d'urgence.

- d) Le prestataire fournit ou utilise des outils, dans le cadre de l'exécution des prestations, conformes à la réglementation en vigueur, quel que soit le secteur d'activité concerné.
- e) Le prestataire réalise un suivi de l'activité sécurité et une revue régulière des journaux d'événements conformément aux directives du commanditaire.
- f) Le prestataire rend compte, pendant la durée d'exécution des prestations, du respect des exigences de sécurité décrites dans ce document et applicables à la prestation, au commanditaire. Des jalons sécurité peuvent être définis entre le commanditaire et le prestataire.
- g) Un audit de sécurité sera réalisé sur les systèmes déployés (logiciels ou matériels) avant la livraison au commanditaire afin de vérifier leur conformité par rapport aux règles de sécurité du

commanditaire applicables à la prestation. Sur demande du commanditaire, des audits (organisationnels et techniques) réguliers pourront être planifiés après installation des systèmes déployés.

5.4 Accès

- a) Les accès aux ressources informatiques utilisées dans le cadre de la prestation sont affectés nominativement à chaque personne concernée. En présence de compte générique, il doit être possible de faire le lien entre le compte et la personne physique ayant réalisée les opérations de traitement.
- b) Le prestataire dispose d'une procédure de gestion des comptes et des droits d'accès. Celle-ci stipule des mesures de revue des comptes conformément aux directives du commanditaire.
- c) Le prestataire doit respecter le principe du besoin d'en connaître. Les profils, rôles, et privilèges des intervenants du prestataire sont limités au strict nécessaire à la réalisation de la mission ou prestation.
- d) Le prestataire désactive les comptes d'accès de ses intervenants dans les circonstances suivantes : fin de la mission de l'intervenant chez le commanditaire, compromission ou suspicion de compromission de comptes du prestataire, incident ou suspicion d'incident sur les systèmes du prestataire.

5.5 Développement / intégration

- a) Le prestataire doit démontrer que ses processus de développement emploient des méthodes d'ingénierie à l'état de l'art, des processus de contrôle qualité et des techniques de validation afin de réduire les défaillances logicielles et les vulnérabilités. Dans le cadre de cette exigence, le terme logiciel s'applique aux logiciels développés par le prestataire : développement d'applications spécifiques ou développement des programmes utilisateurs PLC sur la base de composants logiciels (progiciels par exemple) fournis par un équipementier ou un éditeur logiciel.
- b) Les caractéristiques de cybersécurité des équipements ainsi que leurs certifications doivent être un critère de choix dans le processus d'achat du prestataire lorsque les équipements ne sont pas imposés par le commanditaire. Il pourra s'appuyer sur les profils de protection publiés sur le site de l'ANSSI (<http://www.ssi.gouv.fr>). Le prestataire doit soumettre à validation par le commanditaire la liste et caractéristiques de l'ensemble des équipements qui seront intégrés chez le commanditaire.

Remarque : lorsque les équipements sont imposés par le commanditaire, le prestataire doit être en mesure d'apporter un conseil au commanditaire pour lui signaler que le niveau de cybersécurité des équipements n'est pas en adéquation avec le niveau de cybersécurité visé pour le système final.

- c) Le prestataire doit vérifier la mise en œuvre des règles de bonnes pratiques. Pour cela, il pourra par exemple utiliser les options avancées de certains compilateurs (y compris pour le développement d'application automates) ou des outils dédiés à la vérification des bonnes pratiques de programmation.
- d) Le prestataire doit utiliser, lorsque des solutions existent, des outils d'analyse statique et des tests de robustesse pour les développements qu'il réalise. L'objectif est de vérifier la qualité des développements et l'absence de bugs « élémentaires » régulièrement utilisés lors d'attaques informatique (débordement de pile « buffer overflow », par exemple).

e) Le prestataire doit être en mesure d'accepter, sur demande explicite du commanditaire, un audit des codes sources développés par ses soins.

f) Le prestataire doit être en mesure de réaliser des tests unitaires et d'ensemble pour vérifier que les exigences de cybersécurité sont bien implémentées.

5.6 Traçabilité et livraison

a) Le prestataire doit être en mesure de tracer les mises à jour et modifications qu'il a apporté aux systèmes déployés et de fournir ces traces aux commanditaires.

b) Le prestataire doit garantir, dans son processus de livraison, l'intégrité et l'authenticité de l'ensemble des logiciels, programmes, éléments de configuration et documentation. Les éléments concernés sont en particulier : les micro-logiciels, les systèmes d'exploitation et autres logiciels utilisés, les fichiers de configuration des équipements réseau, les mises à jour, etc.

c) Le prestataire doit être en mesure de garantir la confidentialité des éléments précédents si le commanditaire en fait la demande. En particulier, il est recommandé que la confidentialité des éléments de configuration soit systématiquement assurée.

d) Le prestataire doit être force de proposition pour rehausser le niveau de sécurité des architectures. Toute évolution de l'architecture doit faire l'objet d'une validation formelle du service de sécurité du commanditaire.

e) En cas de modification de la prestation, l'impact sur la sécurité des systèmes déployés ou sur les données du commanditaire doit être évalué et toute modification de la prestation doit faire l'objet d'une validation formelle du service de sécurité du commanditaire.

5.7 Veille

a) Le prestataire doit déployer un processus de veille sur les menaces et vulnérabilités sur les produits et technologies mises en œuvre sur les systèmes qu'il a déployés. Il pourra s'appuyer sur les informations publiées par les CSIRT étatiques ou privés ainsi que les sites web des équipementiers.

b) Le prestataire doit mettre en œuvre un processus de veille sur l'évolution des moyens techniques pour renforcer le niveau de cybersécurité des systèmes.

c) Le prestataire s'engage à informer dans les meilleurs délais le commanditaire de tout évènement ou incident de cybersécurité présumé et/ou avéré impactant les données et systèmes du commanditaire.

6 Protection du système d'information du prestataire

6.1 Exigences générales

a) Le prestataire doit être en mesure de mettre en œuvre des mesures pour protéger le système d'information qu'il utilise pour ses prestations avec le commanditaire et en particulier s'assurer que son système d'information est en mesure d'accueillir des informations de niveau «TLP:AMBER».

6.2 Exigences relatives aux outils et à l'environnement de développement

a) Le prestataire doit utiliser un environnement de développement sécurisé afin que celui-ci ne soit pas le point d'entrée pour atteindre les systèmes chez les commanditaires (par l'insertion de codes malveillants par exemple). Il est conseillé de dédier des locaux physiques pour le développement. Le mécanisme de contrôle d'accès doit permettre de tracer l'identité des personnes y pénétrant et l'heure d'accès.

b) Le prestataire doit également veiller à la protection des documents au format papier utilisés dans le cadre de sa prestation.

c) L'environnement de développement doit être dédié et séparé des autres environnements informatiques – de tests et d'exploitation- du prestataire. En particulier, cet environnement ne doit pas être connecté à internet ni directement (sans filtrage et mesures de sécurité) au réseau bureautique du prestataire.

d) Les outils de gestion des configurations (« versioning ») devront garantir l'intégrité, l'authenticité et la traçabilité des éléments qu'ils contiennent et suivant les besoins, la confidentialité.

e) Les outils permettant d'assurer les exigences précédentes doivent être mis en œuvre suivant les règles de l'art. Il est recommandé d'utiliser des produits qualifiés par l'ANSSI lorsqu'ils existent.

f) Le niveau de sécurité de l'environnement de développement doit être vérifié par des audits (organisationnels et techniques) réguliers. Il est conseillé que l'environnement de développement soit homologué en s'appuyant pour cela sur le guide d'homologation et les guides de bonnes pratiques comme le guide d'hygiène par exemple.

6.3 Exigences relatives aux plateformes de tests et d'intégration

a) Lorsque les plateformes de tests et d'intégration appartiennent au prestataire, celui-ci doit appliquer les mêmes exigences que pour les environnements de développement.

b) Lorsque les plateformes de tests et d'intégration appartiennent au commanditaire mais sont hébergées chez le prestataire, les mesures de sécurité doivent être précisées par le commanditaire. A défaut, les mesures de l'alinéa précédent seront appliquées.

6.4 Exigences relatives aux outils de maintenance

a) Le prestataire doit mettre en place une procédure de gestion des outils de maintenance afin de vérifier qu'ils sont conformes aux exigences de sécurité du système pour lequel ils seront utilisés chez le commanditaire.

b) Le prestataire doit s'assurer que les outils de maintenance ne contiennent pas de données sensibles du commanditaire ou alors que les outils pour en assurer la confidentialité sont bien mis en œuvre.

c) Le prestataire doit mettre en œuvre des éléments pour renforcer la sécurité des outils de maintenance. Il pourra pour cela, s'appuyer sur les guides et notes techniques publiés sur le site de l'ANSSI.

6.5 Exigences relatives aux outils de télémaintenance

a) Lorsque la télémaintenance est autorisée sur le système du commanditaire, le prestataire doit être en mesure de dédier un poste pour la télémaintenance du système du commanditaire à la demande de ce dernier.

- b) Le prestataire doit être en mesure de mettre en œuvre les recommandations et directives selon les exigences de la CCIC.
- c) Les solutions de télémaintenance devront être auditées régulièrement afin de vérifier la bonne mise en œuvre des mesures de vérifier le niveau réel de sécurité.
- d) Le prestataire doit être en mesure d'effectuer les opérations de télémaintenance depuis des locaux maîtrisés disposant du même niveau de sécurité que le système du commanditaire si celui-ci le demande.

6.6 Usage de plateformes de travail collaboratif

- a) Dans le cas où le prestataire mettrait à disposition du commanditaire une plateforme de travail collaboratif pour échanger des données (pour les études par exemple), le niveau de sécurité de celle-ci doit être clairement indiquée et portée à la connaissance du commanditaire.
- b) Le niveau réel de sécurité doit être vérifié régulièrement par des audits réalisés conformément au référentiel d'exigences [PASSI].

7 Exigences relatives aux interventions d'intégration et de maintenance chez le commanditaire

Les exigences ci-dessous portent sur les interventions réalisées sur les systèmes chez les commanditaires. Cela concerne en premier lieu les intervenants réalisant des activités de maintenance mais cela peut également concerner les intervenants réalisant des activités de mise en service par exemple. Certaines mesures peuvent être redondantes avec celles décrites précédemment.

7.1 Protocole d'intervention

- a) Les intervenants devant intervenir sur les systèmes du commanditaire doivent être individuellement clairement identifiés et leurs rôles précisés. En particulier, un référent cyber (assuré par le chef d'équipe par exemple) doit être identifié.
- b) L'accès aux installations doit être validé par le commanditaire.
- c) Les intervenants doivent respecter les règles de cybersécurité du commanditaire et s'être assuré qu'un protocole d'intervention, identifié dans un permis ou bon de travail par exemple, a bien été validé par les deux parties.
- d) En cas d'intervention du prestataire sur les systèmes ou en cas d'évolution logicielle, il doit être possible de revenir à la version antérieure du système ou de revenir à l'état précédant l'intervention.
- f) Le prestataire doit réaliser systématiquement des tests de non-régression.

7.2 Bons comportements

- a) Les intervenants appliquent les bonnes pratiques lors de leurs interventions chez le commanditaire sans que celles-ci ne soient systématiquement rappelées par ce dernier.
- b) Les intervenants se conforment aux règles en vigueur chez le commanditaire.

c) Les intervenants doivent être capables de signaler au commanditaire, des situations anormales qu'il aurait constatées, présentant des risques en termes de cybersécurité.

7.3 Moyens utilisés lors de l'intervention

a) Les interventions sur l'installation du commanditaire doivent être réalisées avec des outils validés, c'est-à-dire qui respectent les exigences détaillées au chapitre relatif aux outils de maintenance et aux outils de télémaintenance.

b) L'ensemble des équipements matériels et logiciels utilisés pour les interventions sur les systèmes (comme les consoles de programmation et de maintenance) doit être recensé dans la gestion du parc afin d'être bien identifié pour faciliter leur maintien en condition de sécurité.

c) Les équipements utilisés doivent être exclusivement dédiés aux systèmes (pas de bureautique). Les équipements utilisés devraient être exclusivement dédiés aux systèmes du commanditaire.

d) En cas de besoin particulier, suite à un incident (de cybersécurité ou autres) par exemple nécessitant l'utilisation d'outils spécifiques non identifiés parmi les outils habituels, l'intervenant doit être en mesure d'analyser, avec le commanditaire, les risques liés à leur utilisation et de mettre en œuvre les mesures pour traiter ces risques.

7.4 Rapport d'intervention

a) La fourniture d'un rapport ou compte-rendu d'intervention doit être systématique.

b) Le rapport doit contenir une liste de contrôle (check-list) des actions à réaliser après l'intervention, et en particulier vérifier que les sauvegardes des données (données de configuration, modifications de programmes, etc.) ont été réalisées.

c) Le rapport doit lister les anomalies constatées et assurer une traçabilité des actions réalisées et des modifications apportées sur le système du commanditaire.

d) Le rapport d'intervention doit permettre au commanditaire de gérer le cycle de vie de son système et d'en assurer le MCS.

Remarque : le format du rapport d'intervention est à la discrétion du commanditaire. Le rapport d'intervention peut être saisi dans une base de données de maintenance (GMAO) ou des outils de gestion du parc du commanditaire par exemple. L'objectif n'est pas d'alourdir les processus déjà en place chez le commanditaire mais de s'appuyer sur ces derniers.

8 Exigences relatives aux opérations d'exploitation et administration des systèmes

8.1 Exigences relatives à l'exploitation

a) Le prestataire doit documenter les procédures d'exploitation et les mettre à disposition du personnel intervenant auprès du commanditaire.

b) Le prestataire doit appliquer un processus de gestion des changements aux systèmes, à l'organisation, aux processus et moyens de traitement de l'information. Tout changement ayant potentiellement une incidence sur la sécurité appliquée à la prestation doit être contrôlé.

c) Le prestataire doit ajuster et surveiller les dimensionnements des ressources afin de garantir la performance exigée du système.

- d) Le prestataire doit sauvegarder l'information, les logiciels, les images systèmes et doit tester ces sauvegardes conformément à une politique de sauvegarde convenue.
- e) Le prestataire doit journaliser les activités de l'utilisateur et tout évènement lié à la sécurité de l'information. Ces journaux sont vérifiés régulièrement.
- f) Les activités de l'opérateur et de l'administrateur système doivent être journalisées et vérifiées.
- g) L'intégrité des journaux est garantie par des mesures de protection contre la falsification et les accès non autorisés.
- h) Les horloges de l'ensemble des systèmes doivent être synchronisées sur une source de référence temporelle unique.
- i) Des informations sur les vulnérabilités techniques des systèmes d'information en exploitation doivent être obtenues en temps opportun, l'exposition de l'organisation à ces vulnérabilités doit être évaluée et les mesures appropriées doivent être prises pour traiter le risque associé.
- j) Le prestataire s'engage à la fin de la prestation, sur demande du commanditaire, à restituer les données appartenant au commanditaire dans un format exploitable conformément à une procédure de réversibilité convenue.

8.2 Exigences relatives à l'administration

- a) Le prestataire s'engage à respecter les préconisations de l'ANSSI relatives à l'administration sécurisée des systèmes d'information conformément aux directives du commanditaire.

8.3 Exigences relatives à la sécurité des matériels et logiciels

- a) Le prestataire doit fournir à ses intervenants des postes de travail qui disposent d'un antivirus et d'un anti-malware.
- b) Le prestataire doit mettre en œuvre des mesures de détection, prévention, récupération, sensibilisation pour se protéger contre les logiciels malveillants.

8.4 Exigences relatives à la continuité d'activité

- a) Le prestataire doit mettre en place un plan de secours informatique pour les systèmes qu'il exploite et administre conformément aux directives du commanditaire (exigences de niveau de service, RPO, RTO, etc.). Le prestataire doit notamment tester et actualiser le PSI annuellement, communiquer les comptes rendus des tests et informer le commanditaire des axes d'amélioration.

9 Annexes

9.1 Annexe 3 Références documentaires

Codes, textes législatifs et réglementaires	Document
---	----------

[LPM]	Loi de programmation militaire n°2013-1168 du 18 décembre 2013.
[LOI_IL]	Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés définissant le cadre juridique pour le traitement des données à caractère personnel.
[II_901]	Instruction interministérielle relative à la protection des systèmes d'information sensibles, n°901/SGDSN/ANSSI, 28 janvier 2015. Disponible sur http://www.legifrance.gouv.fr .
Normes et documents Renvoi	Document
[CSI_MESURES_PRINCIPALES]	Cybersécurité des systèmes industriels, Méthode de classification et mesures principales, disponible sur http://www.ssi.gouv.fr/systemesindustriels
[CSI_MESURES_DETAILLEES]	Cybersécurité des systèmes industriels, Mesures Détaillées, disponible sur http://www.ssi.gouv.fr/systemesindustriels
[CSI_MAITRISER_LA_SSI]	Cybersécurité des systèmes industriels, Maitriser la SSI pour les systèmes industriels, disponible sur http://www.ssi.gouv.fr/systemesindustriels
[CSI_CAS_PRATIQUE]	Cybersécurité des systèmes industriels, Cas pratique, disponible sur http://www.ssi.gouv.fr/systemesindustriels
[HOMOLOGATION]	L'homologation de sécurité en neuf étapes simples, ANSSI, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[HYGIENE]	Guide d'Hygiène Informatique, ANSSI, version en vigueur. disponible sur http://www.ssi.gouv.fr
[PASSI]	Référentiel d'exigences pour les prestataires d'audit à la sécurité des systèmes d'information. Disponible sur http://www.ssi.gouv.fr
[GUIDE_ACHAT]	Guide d'achat de produits de sécurité et de services de confiance qualifiés, version en vigueur.
[CSI_GUIDE_FORMATION]	Cahier des charges portant sur la formation à la cybersécurité pour les systèmes industriels, disponible sur http://www.ssi.gouv.fr/systemesindustriels

9.2 Annexe 4 Echelle de confidentialité du commanditaire

Confidentialité	
1	Niv1 : « TLP:CLEAR » Informations publiques pouvant être distribuées librement en dehors de la CCI de Corse. Les destinataires peuvent diffuser cette information au monde entier, il n'y a pas de limite à la divulgation. Par exemple, les informations susceptibles d'être publiées sur Internet.
2	Niv2 : « TLP:GREEN » Divulgation limitée. Les destinataires peuvent partager les informations TLP:GREEN avec leurs pairs et les organisations partenaires au sein de leur Communauté , mais pas via des canaux accessibles au public.
3	Niv3 : «TLP:AMBER» Divulgation limitée. Informations circulant sur la base du besoin d'en connaître au sein de la CCI de Corse et de ses clients. « TLP:AMBER » est utilisée lorsque l'information nécessite un soutien pour être traitée efficacement, mais qu'elle présente un risque pour la vie privée, la réputation ou les opérations si elle est partagée en dehors des organisations concernées. Si l'information ne peut circuler qu'au sein de la CCI de Corse seulement, la classification à utiliser est « TLP:AMBER+STRICT ».
4	Niv4 « TLP:RED » : Informations destinées aux personnes habilitées dans l'interdiction de les partager avec qui que ce soit. L'information est classifiée « TLP:RED » lorsque les informations ne peuvent pas être traitées efficacement sans risque significatif pour la vie privée, la réputation ou les opérations des organisations concernées.

10 Glossaire

10.1 Acronymes

- ❖ **ANSSI** : Agence nationale de la sécurité des systèmes d'information
- ❖ **AMOA** : Assistance à Maitrise d'Ouvrage (parfois désignée AMO) AMOE Assistance à Maitrise d'Oeuvre (parfois désignée AME) AMOAD Assistance à Maitrise d'Ouvrage Déléguée
- ❖ **AO** : Analyse Organique
- ❖ **AF** : Analyse Fonctionnement
- ❖ **BMS** : Building Management System
- ❖ **CCTP** : Cahier des Clauses Techniques Particulières
- ❖ **CdC** : Cahier des Charges
- ❖ **CSI** : Cybersécurité des Systèmes Industriels
- ❖ **CSIRT** : Computer Security Incident Response Team
- ❖ **FAT** : Factory Acceptance Test (recette usine)
- ❖ **GTB** : Gestion Technique de Bâtiment
- ❖ **ICS** : Industrial Control System
- ❖ **LPM** : Loi de Programmation Militaire
- ❖ **MCO** : Maintien en Conditions Opérationnelles
- ❖ **MCS** Maintien en Conditions de Sécurité

- ❖ **MOA** : Maitrise d’Ouvrage
- ❖ **MOE** : Maitrise d’OEuvre
- ❖ **PCA** : Plan de Continuité d’Activité
- ❖ **PAS** : Plan d'Assurance Sécurité
- ❖ **PLC** : Programmable Logic Contrôler
- ❖ **RPO** : Quantité maximale de données qu’il est acceptable de perdre
- ❖ **RTO** : Durée maximale d’interruption admissible
- ❖ **SAT** : Site Acceptance Test (recette site)
- ❖ **SFD** : Spécifications Fonctionnelles Détaillées SFG Spécifications Fonctionnelles Générales
- ❖ **VPN** : Virtual Private Network