

Dossier de Consultation des Entreprises

Marché de maintenance des réseaux de transmission des PC de la DIR Centre-Est

CCTP Annexe 2 – Clauses de sécurité informatique



Historique des versions du document :

Version	Date	Commentaire
0	15/09/25	Version initiale
1	30/01/26	Version modifiée

Affaire suivie par :

Béatrice BOUILLER - SES / PES
<i>Tél. : 04 72 47 16 25</i>
Courriel : beatrice.bouiller@developpement-durable.gouv.fr

Rédacteurs :

- SES / PES : Béatrice BOUILLER

Relecteur :

Table des matières

1 - PRÉAMBULE.....	5
2 - DOCUMENTS DE RÉFÉRENCE.....	5
3 - OBLIGATIONS GÉNÉRALES DE SÉCURITÉ.....	5
3.1 - Responsabilité.....	5
3.1.1 - Obligations du maître d'ouvrage.....	5
3.1.2 - Obligations du titulaire.....	6
3.1.3 - Obligations du titulaire relatives à la télémaintenance.....	6
3.2 - Comité de suivi.....	7
3.3 - Confidentialité.....	7
3.4 - Localisation des données.....	7
3.5 - Audit de sécurité.....	8
3.6 - Réversibilité.....	8
4 - EXIGENCES DE SÉCURITÉ.....	9
4.1 - Gestion de la sécurité.....	9
4.2 - Traitement des incidents.....	9
4.3 - Exigences relatives aux achats de matériel.....	9
4.3.1 - Vulnérabilités matérielles.....	9
4.3.2 - Fournisseurs tiers.....	10
4.3.3 - Logiciels embarqués.....	10
4.3.4 - Compatibilité avec les systèmes existants.....	10
4.4 - Connaître le Système d'Information.....	10
4.4.1 - Etat de l'art Connaître le Système d'Information.....	10
4.4.2 - Cartographie des systèmes.....	11
4.5 - Gestion des identités et des accès.....	11
4.5.1 - Authentification.....	11
4.5.2 - Contrôle des authentifications.....	12
4.5.3 - Inventorier les comptes utilisateurs et leur niveau de privilège.....	12
4.5.4 - Stockage sécurisé des mots de passe.....	12
4.6 - Gestion des flux.....	13
4.6.1 - Confidentialité et intégrité des flux.....	13
4.6.2 - Contrôle et filtrage des flux.....	13
4.6.3 - Protéger les expositions directes sur Internet.....	14
4.7 - Protection antivirale.....	14
4.8 - Gestion des mises à jour.....	15

4.8.1 - Mise à jour des correctifs de sécurité.....	15
4.8.2 - Cas particulier d'utilisation de systèmes obsolètes.....	15
4.9 - Continuité de l'activité.....	16
4.10 - Sécurisation des réseaux.....	16
4.10.1 - Réseaux Wifi.....	16
4.10.2 - Création ou extension de réseaux.....	17
4.11 - Sécuriser l'administration.....	17
4.11.1 - Utiliser les protocoles d'administration sécurisés.....	17
4.12 - Choix des composants du système.....	18
4.12.1 - Privilégier l'usage de produits qualifiés par l'ANSSI.....	18
4.13 - Journalisation.....	18
4.14 - Contrôle de la prise en compte de ces mesures avant le déploiement en production.....	19
4.15 - Personnels en charge des prestations.....	19
4.15.1 - Liste de personnels intervenant sur le SI.....	19
4.15.2 - Qualification et formation dans le domaine de la SSI.....	20
4.15.3 - Exigences de sécurité pour les personnels extérieurs.....	20
5 - CLAUSES DE CONFIDENTIALITÉ TYPE EN CAS DE SOUS-TRAITANCE.....	21

1 - Préambule

Ce document présente les exigences de sécurité à respecter par l'ensemble des projets s'intégrant dans le Système d'Information de la DIRCE.

Ces exigences de sécurité sont inspirées du Guide d'hygiène informatique [DR01], et permettent de fixer les règles de protection minimales applicables à tout SI et donc également aux SI et réseaux de l'État, par application de la Politique de Sécurité des SI de l'État (PSSIE) [DR02].

Dans la suite du document, les systèmes, applications ou matériels concernés par l'objet du marché pourront être regroupés sous la dénomination de système.

2 - Documents de référence

Exemple de documents de référence établis par l'ANSSI :

Réf.	Intitulé
DR01	Guide d'hygiène informatique
DR02	Politique de Sécurité des Systèmes d'Information de l'État (PSSIE)
DR03	Référentiel Général de Sécurité (RGS)
DR04	Exigences de cybersécurité pour les prestataires d'intégration et de maintenance des systèmes industriels
DR05	Recommandations de configuration des commutateurs et pare-feux Hirschmann
DR06	Recommandations de sécurité relatives aux réseaux WiFi
DR07	Sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection
DR08	Recommandations de sécurité relatives à TLS
DR09	Recommandation pour l'administration sécurisée d'un SI

3 - Obligations générales de sécurité

3.1 - Responsabilité

3.1.1 - Obligations du maître d'ouvrage

Le Maître d'Ouvrage s'engage à faire connaître au titulaire les anomalies qu'il est amené à constater, et ce, dans les meilleurs délais.

Il assure que toutes les interventions de maintenance n'étant pas du ressort du titulaire

seront effectuées dans les règles de l'art, de telle façon que cela ne provoque pas de pannes intempestives sur les matériels ou équipements faisant l'objet du présent marché. Il permet au personnel du titulaire d'avoir accès aux installations, aux schémas, aux réglages... et lui communiquera toutes modifications quant à l'installation/suppression des matériels et équipements.

3.1.2 - Obligations du titulaire

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. En particulier il s'engage à informer la DIRCE des risques d'une opération envisagée, des incidents éventuels ou potentiels, et de la mise en œuvre éventuelle d'actions correctives ou de prévention.

Outre le respect de ses obligations au titre de la convention de service, le prestataire informera préalablement la DIRCE de toute opération susceptible de provoquer l'indisponibilité (ou une dégradation des performances) du système.

Le prestataire est responsable du maintien en condition de sécurité du système pendant toute la durée des prestations.

Les mécanismes de sécurité mis en œuvre doivent évoluer conformément à l'état de l'art : la découverte de failles dans un algorithme, un protocole, une implémentation logicielle ou matérielle, ou encore l'évolution des techniques de cryptanalyse et des capacités d'attaque par force brute doivent être pris en compte.

3.1.3 - Obligations du titulaire relatives à la télémaintenance

- Sécurisation des flux de télémaintenance : le titulaire utilisera uniquement le tunnel sécurisé avec chiffrement des communications (VPN^o) mise à disposition de la DIRCE pour la connexion à distance, en astreinte ou en situation de télémaintenance, aux réseaux utilisés dans le cadre de la Prestation (que ce soient ceux du titulaire, ceux de l'acheteur ou les deux éventuellement). Le personnel du titulaire devra explicitement utiliser les services d'accès distants mis à disposition par la DIRCE.
- Chiffrement des postes de télémaintenance : le titulaire met en œuvre le chiffrement intégral du poste de travail utilisé en astreinte ou pour les opérations de télémaintenance.
- Connexion distante : le titulaire restreint la connexion distante aux personnels en situation de télémaintenance, aux horaires définis (ex. connexion non autorisée en horaires ouvrés), et aux ressources nécessaires en télémaintenance uniquement.

3.2 - Comité de suivi

Un comité de suivi permettra de gérer la mise en place et l'évolution du volet sécurité de la prestation : respect du calendrier, conformité des prestations, respect de l'obligation de collaboration, validation des améliorations pour accroître la sécurité. Il traitera également des questions techniques touchant à la sécurité : collaboration dans la gestion des incidents, détection des anomalies et préconisation d'améliorations, exploitation des résultats des audits de contrôle des prestations sécurité.

Ce comité traitera également, si les prestations du marché le nécessitent, des obligations liées à la loi du 6 janvier 1978 relative à l'Informatique, aux fichiers et aux libertés : déclaration par la DIRCE auprès de la CNIL, communication des déclarations au prestataire, informations par le prestataire des modalités de gestion ou d'exploitation des applications et des modifications de celles-ci.

Le comité de suivi se réunira selon la périodicité est définie au CCTP.

3.3 - Confidentialité

Le prestataire a une obligation de discrétion, de sécurité et de secret (conformément à l'article 5 du CCAG).

L'ensemble des intervenants du prestataire s'engage à assurer la confidentialité de l'intégralité des informations traitées dans le cadre de la prestation.

La divulgation des informations ne devra se faire qu'aux seules personnes ayant le besoin d'en connaître. La méthodologie, la documentation, les informations ou le savoir-faire provenant de la DIRCE sont considérés comme confidentiels, et le titulaire ne peut les utiliser que pour l'accomplissement de la prestation. Les informations sensibles ou confidentielles et le système d'information utilisés par le prestataire doivent respecter l'ensemble des règles de l'instruction interministérielle n° 9011 relative aux mesures de protection des systèmes d'information traitant d'informations sensibles non-classifiées de défense de niveau Diffusion Restreinte (DR). En cas de manipulation d'informations sensibles classifiées, le prestataire s'engage à respecter l'instruction générale interministérielle n° 13002 sur la protection du secret de la défense. En cas de sous-traitance, toutes ces obligations s'appliquent également aux sous-traitants.

Le PAS identifie les données sensibles et les règles qui s'y appliquent.

3.4 - Localisation des données

Les lieux d'hébergement des données doivent satisfaire aux exigences de sécurité du donneur d'ordres et aux dispositions de la loi du 6 janvier 1978 modifiée, relative à la protection des données personnelles.

Le prestataire s'engage, sur le périmètre de la prestation, à spécifier préalablement et précisément les lieux géographiques dans lesquels les données informatiques liées à la prestation seront hébergées ;

De même, le prestataire précise si ses infrastructures (techniques ou organisationnelles) sont gérées par une entité juridique appartenant à un pays disposant de lois autorisant l'État à accéder aux données (ex. « Patriot Act » aux États-Unis).

L'hébergement sur le territoire national des données sensibles de la DIRCE est obligatoire sauf accord explicite de la DIRCE et dérogation dûment motivée.

Enfin, en cas de changement de localisation des données ou services, le prestataire s'engage à informer préalablement la DIRCE.

3.5 - Audit de sécurité

Conformément à l'article 17 du CCAG FCS , la DIRCE peut réaliser ou faire réaliser, à tout moment, un audit de sécurité pour vérifier que les exigences de sécurité sont satisfaites par les dispositions prises par le prestataire.

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).

Dans le cas où des écarts entre le niveau de sécurité effectif et les exigences de sécurité exprimées dans le présent CCTP seraient constatés et ne feraient l'objet d'aucune contestation de la part du prestataire, la DIRCE se réserve le droit d'appliquer les pénalités de retard liées au délai de non mise en conformité, ce délai court à partir de la mise en demeure notifiée par la DIRCE jusqu'à la mise en conformité. (pénalités de retard décrites à l'article 4 du CCAP).

3.6 - Réversibilité

A la fin du présent marché, quelle qu'en soit sa cause, le titulaire s'engage, dans les 3 mois précédant la fin de la prestation, à assurer la réversibilité du service.

Il s'agira de transmettre l'ensemble des ressources et des compétences requises pour la poursuite du service. Au cours de la période de réversibilité, le titulaire continue à assurer les activités qui lui sont attribuées, sauf contrordre du commanditaire.

Durant la période de réversibilité, le titulaire doit permettre au commanditaire de prendre le relais, ou de le faire prendre par un tiers. Cette transition doit être effectuée dans les meilleures conditions et sans interruption du service en cours.

Les modalités détaillées seront proposées par le candidat, elles seront affinées et planifiées avec le commanditaire le moment venu.

Le prestataire s'engage à apporter l'assistance nécessaire durant la période de migration pour faciliter le transfert des moyens de sécurité matériels et logiciels, et la reprise de leur exploitation par la DIRCE, ou par un autre prestataire de service.

Le prestataire s'engage à garantir, lors du transfert, la sécurité des données et des applications qui lui ont été confiées, conformément à ses obligations.

En outre, la phase de réversibilité ne doit pas, en principe, modifier la qualité, les termes et les conditions des services fournis durant le contrat et définis dans le Service Level Agreement (SLA).

En cas d'arrêt des prestations confiées au titulaire par le donneur d'ordres, l'ensemble des matériels, logiciels et documentations confiés au titulaire doivent être restitués. Le déménagement de cet ensemble des locaux du titulaire sera assuré aux frais du titulaire dans un délai maximum d'un mois après l'arrêt des prestations confiées au titulaire

4 - Exigences de sécurité

Les exigences de sécurité s'appliquent aux systèmes, applications et matériels couverts par le périmètre du marché.

4.1 - Gestion de la sécurité

Le candidat précisera les moyens mis en œuvre dans le cadre du processus d'amélioration continu de la sécurité de ses infrastructures et de formation de son personnel.

4.2 - Traitement des incidents

Traitement des incidents de sécurité : le titulaire contacte les interlocuteurs sécurité de l'acheteur désignés pour signaler tout incident de sécurité susceptible d'affecter les données ou le SI de l'acheteur. De plus :

- si cet incident a lieu sur le SI de la DIRCE, le titulaire participera à la demande de l'acheteur au traitement de l'incident ;
- si cet incident a lieu sur le SI du titulaire, le titulaire autorisera la DIRCE ou un tiers désigné à participer au traitement de l'incident (si l'acheteur le souhaite).

4.3 - Exigences relatives aux achats de matériel

Lors de l'achat de matériel, plusieurs risques cyber doivent être pris en compte pour garantir un bon niveau de sécurité de la DIRCE. Voici les principaux risques à considérer :

4.3.1 - Vulnérabilités matérielles

Le titulaire doit s'assurer que le matériel proposé et fourni ne contient pas de vulnérabilités connues et exploitables par des cyberattaquants. Il devra vérifier

que le matériel acheté est à jour avec les derniers correctifs de sécurité, qu'il respecte les niveaux d'exigences du présent CCTP et qu'il est compatible avec les systèmes de sécurité existants à la DIRCE.

4.3.2 - Fournisseurs tiers

Les fournisseurs de matériel et de prestations de maintenance peuvent être des vecteurs de risques cyber. Le titulaire doit respecter les normes et bonnes pratiques de cybersécurité. La DIRCE se réserve le droit d'évaluer la sécurité du titulaire et des sous-traitants et s'assurera qu'ils respectent les normes et bonnes pratiques de cybersécurité.

4.3.3 - Logiciels embarqués

Le matériel peut inclure des logiciels embarqués qui présentent des risques de sécurité. Le titulaire doit vérifier que ces logiciels sont sécurisés et qu'ils peuvent être mis à jour régulièrement pour corriger les vulnérabilités éventuelles.

4.3.4 - Compatibilité avec les systèmes existants

Le nouveau matériel doit être compatible avec les systèmes de sécurité existants de la DIRCE. Une incompatibilité peut créer des failles de sécurité exploitables par des attaquants. La DIRCE pourra refuser un matériel proposé si son niveau de sécurité n'est pas suffisant ou incompatible avec les matériels et mesures déjà en place.

4.4 - Connaître le Système d'Information

4.4.1 - Etat de l'art Connaître le Système d'Information

Afin d'anticiper les obsolescences logicielles, il est demandé, lors du remplacement d'un système ou équipement existant ou lors de la rénovation de ce dernier, d'**établir un inventaire des systèmes, applications et matériels** qui seront déployés au sein du système d'information et des réseaux de la DIRCE.

Pour chacun des composants du système qui seront déployés, il est demandé :

- d'identifier le type de l'équipement,
- d'identifier la localisation dans l'équipement,
- de fournir la version applicative déployée, et celle préconisée par l'éditeur,
- de fournir la configuration du matériel livré ou déployé (sauf en cas de configuration usine)
- de fournir la date de fin de support des logiciels si annoncée par l'éditeur ou le constructeur,
- d'indiquer la date d'application des derniers correctifs de sécurité,

- de lister les dépendances avec d'autres composants du SI.

Le titulaire fournit la preuve de conformité pour chaque nouveau matériel proposé.

4.4.2 - Cartographie des systèmes

Le titulaire dispose d'un inventaire et d'une cartographie des systèmes d'information dont il à la charge et doit les maintenir, selon les préconisations de l'ANSSI issues du guide « cartographie des systèmes d'information », dans l'outil mis à sa disposition par l'acheteur. L'inventaire et la cartographie comprennent également la liste des « briques » matérielles et logicielles utilisées, ainsi que leurs versions exactes avec leur configuration. Ils comportent une base de données de configuration. La cartographie est livrée à la demande de l'acheteur et au minimum à chaque mise à jour majeure du système.

4.5 - Gestion des identités et des accès

4.5.1 - Authentification

Les identifiants des comptes d'accès sont nominatifs. L'utilisation d'un même compte par plusieurs personnes n'est pas autorisée sauf si une contrainte le justifiant est acceptée par le donneur d'ordres. Dans ce cas, le candidat présentera les mesures techniques et/ou organisationnelles pour garantir l'imputabilité.

L'utilisation de mots de passe constructeur ou par défaut est **interdite**. Il est impératif de partir du principe que les configurations par défaut des systèmes d'information sont systématiquement connues des potentiels attaquants.

Les éléments d'authentification par défaut des composants du système installé doivent donc être modifiés dès leur installation et, s'agissant des mots de passe, ils devront être conformes à la politique de gestion des mots de passe suivante :

- Les mots de passe pour les profils utilisateurs doivent contenir 12 caractères ou plus, et être composés d'au moins un caractère de chacun des types suivants:
 - majuscules,
 - minuscules,
 - chiffres,
 - caractères spéciaux.
- Les mots de passe pour les profils administrateurs doivent contenir 16 caractères ou plus, et être composés d'au moins un caractère de chacun des types suivants:
 - majuscules,
 - minuscules,
 - chiffres,
 - caractères spéciaux.

- Les mots de passe ne doivent pas être vulnérables aux attaques par dictionnaire..

L'utilisation de protocoles dont l'authentification est en clair est **interdite**.

L'utilisation de certificats clients et serveurs pour l'authentification est une alternative préférable aux mots de passe à condition que la clef privée soit protégée dans un matériel adéquat.

Lorsque cela est nécessaire l'authentification à double facteurs sera mise en œuvre.

4.5.2 - Contrôle des authentifications

Afin de rendre plus difficiles les attaques sur les authentifications (attaque par brute force ou par dictionnaire), il est **imposé une augmentation du délai entre deux tentatives de connexions**.

Il est également demandé de vérifier que le stockage des mots de passe dans les configurations des équipements soit réalisé à l'aide d'un chiffrement conforme au Référentiel Général de Sécurité.

4.5.3 - Inventorier les comptes utilisateurs et leur niveau de privilège

Des **comptes nominatifs** doivent être mis en place.

Il est demandé de lister les utilisateurs et leur rôle au sein du système qui sera déployé.

En complément, il est demandé de fournir la liste :

- des comptes de services (hiérarchisés),
- des comptes d'administration.

Le **principe du moindre privilège** est appliqué à tous les types de compte. Le principe du moindre privilège est le principe selon lequel chaque intervenant doit disposer d'un compte ayant exactement les droits nécessaires à l'accomplissement de ses tâches.

4.5.4 - Stockage sécurisé des mots de passe

Le stockage des mots de passe doit se faire dans un outil de coffre-fort numérique chiffré. La solution logicielle recommandée sur le parc de la DIRCE pour le stockage sécurisé des mots de passe est la solution KeePass disponible sur Windows (ou son alternative qui est la solution KeePassX pour les environnements sous Linux) ou la solution Bitwarden pour certains cas de coffres forts partagés.

4.6 - Gestion des flux

4.6.1 - Confidentialité et intégrité des flux

Tous les flux d'administration doivent être chiffrés par des procédés fiables (SSH, SSL, Ipsec, etc.), garantissant la confidentialité et l'intégrité des données.

De façon générale, tous les flux contenant des informations sensibles et circulant sur un réseau public doivent être chiffrés par des procédés apportant ces mêmes garanties.

Le choix et le dimensionnement des algorithmes cryptographiques doivent être effectués conformément aux règles et recommandations du RGS en la matière.

Le candidat indiquera l'ensemble des mécanismes et mesures mis en oeuvre pour garantir la confidentialité et l'intégrité des flux d'administration.

Les protocoles réseaux suivants sont considérés comme non sécurisés et sont proscrits du réseau technique de la DIRCE :

- telnet,
- HTTP,
- IMAP,
- SMTP,
- POP3,
- FTP,
- rlogin,
- rcp,
- rsh,
- LDAP,
- VNC.

Bien qu'il soit difficile d'en dresser une liste exhaustive, les protocoles les plus courants reposent sur l'utilisation de TLS [DR8] et sont souvent identifiables par l'ajout de la lettre « S » (pour secure en anglais) à l'acronyme du protocole.

4.6.2 - Contrôle et filtrage des flux

De manière générale, le filtrage des flux ne fait pas partie du périmètre du marché et est assuré par les équipes sécurité de la DIRCE.

Néanmoins, dans le cadre du déploiement d'une nouvelle infrastructure ou de l'évolution d'une infrastructure existante, le titulaire devra respecter les principes énoncés dans ce paragraphe.

Au titre de la défense en profondeur, trois zones seront mises en place, chacune étant

protégée par un dispositif de filtrage :

- une zone publique regroupant les machines qui hébergent des services ayant vocation à communiquer avec l'extérieur (Reverse Proxy, Serveur Web, FTP, Serveur de mail, DNS ,etc.) ;
- une zone privée regroupant les machines n'ayant pas vocation à communiquer avec l'extérieur ;
- un réseau dédié à l'administration des machines et des équipements à partir de postes de travail situés à la DIRCE.

Le trafic réseau en provenance et à destination du système doit faire l'objet d'un contrôle permanent afin de n'autoriser que les flux légitimes. **Une matrice de flux (inventaire des flux légitimes) sera fournie par le prestataire.**

La politique de filtrage est définie à partir de la matrice des flux. Les dispositifs de filtrage sont bloquants par défaut, tout ce qui n'est pas explicitement autorisé étant interdit.

Le service global doit être protégé contre les attaques classiques sur IP et les protocoles associés (filtrage sanitaire) notamment :

- attaque en déni de service (TCP SYN Flood, Ping Flooding, SMURF, Ping of Death, large packet attacks, etc.) ;
- IP options (source routing, etc.).

Le candidat décrira dans sa réponse les différents mécanismes de protection prévus au niveau des équipements pour contrer les attaques classiques sur IP et les protocoles associés.

Les interfaces d'administration des machines ou des équipements du système ne doivent pas être accessibles depuis l'extérieur. Les services correspondants seront donc configurés pour ne pas accepter de connexions sur les interfaces publiques.

L'accès à distance pour la télémaintenance ne peut se faire que par la solution de télémaintenance mise à disposition du titulaire par la DIRCE ou par le Ministère.

Seuls les services utiles au bon fonctionnement de l'application doivent être activés. **Les autres services doivent être désactivés et si possible désinstallés.**

4.6.3 - Protéger les expositions directes sur Internet

Dans les cas particuliers d'exposition d'un équipement ou d'un composant du SI sur Internet, il est demandé de se rapprocher de l'équipe réseau de la DIRCE afin d'étudier la conformité. Un équipement raccordé au réseau de la DIRCE ne doit en aucun cas être connecté à internet via une connexion externe de type partage de connexion 4G ou autre.

4.7 - Protection antivirale

La système, l'application ou le matériel livré par le titulaire devra supporter une protection antivirale fournie par la DIRCE.

Les restrictions liées à l'utilisation d'un antivirus devront être listées et argumentées par le titulaire.

4.8 - Gestion des mises à jour

4.8.1 - Mise à jour des correctifs de sécurité

Le titulaire informe la DIRCE dès la parution d'une alerte de sécurité portant sur un des composants du système couvert par le présent marché.

Le titulaire applique les correctifs recommandés par les fournisseurs de solutions matérielles ou logicielles (logiciels système ou applicatifs, logiciels embarqués) sur tous les matériels dont il a la charge.

En cas d'alerte grave (attaque virale, faille critique) annoncée par le CERT (Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques), le titulaire doit alerter la DIRCE dans un délai de 4 heures ouvrées. Le correctif ou une solution palliative doit être appliqué dans un délai de 48 heures sur les infrastructures hébergeant le système du donneur d'ordres (serveurs, pare-feux, routeurs ouverts vers l'extérieur).

Les passages de correctifs doivent être précédés d'une sauvegarde spécifique du système et des données qu'il contient, ainsi que de tests sur un environnement de préproduction.

La validation du bon fonctionnement du système se fera conjointement avec les équipes techniques du titulaire et le chef de projet responsable de l'application.

En cas d'alerte donnée par les équipes d'experts du titulaire, par l'administration ou le CERT, le maître d'ouvrage sera notifié par téléphone et courrier électronique avant toutes opérations. La décision de l'action ne pourra être prise que par des personnels de la maîtrise d'ouvrage désignés par écrit. En particulier, le responsable sécurité de la maîtrise d'ouvrage sera le correspondant privilégié pour le suivi des opérations.

Le titulaire s'engage à fournir une adresse mail, un numéro de téléphone et les périodes correspondantes d'opération (H24, heures ouvrables, ...) permettant au maître d'ouvrage de suivre le traitement d'une alerte.

4.8.2 - Cas particulier d'utilisation de systèmes obsolètes

Si des **systèmes obsolètes** (qui ne sont plus supportés par leurs fabricants) devaient être déployés provisoirement, il conviendra de les **identifier** pour les **soumettre à validation de l'équipe cybersécurité de la DIRCE afin de les isoler** au maximum du reste du SI de la DIRCE.

Cette mesure s'applique aussi au niveau du réseau par un filtrage strict des flux, tout comme elle s'applique au niveau des secrets d'authentification qui doivent être dédiés à ces systèmes obsolètes.

4.9 - Continuité de l'activité

Le titulaire doit prendre toutes les mesures nécessaires pour assurer la continuité des services couverts par le marché de maintenance des réseaux de transmission des PC de la DIR Centre-Est.

4.10 - Sécurisation des réseaux

4.10.1 - Réseaux Wifi

Il est demandé de suivre les recommandations de l'ANSSI qui s'appliquent aux réseaux Wifi sur des périmètres industriels.

Il est demandé de **privilégier les installations filaires**, et sur obtention d'une dérogation de l'équipe cybersécurité, de respecter à minima l'ensemble des directives suivantes :

- Lorsqu'il s'agit de configurer un point d'accès Wifi, il est demandé de configurer le point d'accès pour utiliser un chiffrement robuste. Le mode WPA2 avec l'algorithme de chiffrement AES-CCMP est fortement recommandé,
- Il est demandé de s'interfacer avec une infrastructure d'authentification centralisée en s'appuyant sur WPA-Entreprise (standard 802.1x et protocole EAP), et d'utiliser une des méthodes d'authentification suivantes :
 - EAP-TLS, qui exige toutefois une Infrastructure de Gestion de Clés (IGC), avec clé privée et certificat à déployer auprès de chaque utilisateur. Lorsqu'EAP est utilisé, il convient par ailleurs que les clients vérifient l'authenticité du serveur d'authentification ;
 - EAP-TTLS, qui ne nécessite que le déploiement de certificats X509 serveurs et peut donc s'avérer plus pratique lorsqu'il est difficile de déployer des certificats clients. Ceux-ci s'authentifient alors généralement par couple utilisateur/mot de passe. Le support EAP-TTLS n'étant pas natif sous Windows, il convient de s'assurer qu'il est pris en charge par les clients Wi-Fi potentiels ;
 - PEAP, similaire à EAP-TTLS mais nativement pris en charge par Windows.
- Lorsque que le point d'accès Wi-Fi prend en charge la fonctionnalité de private Vlan invité et afin d'améliorer la protection en confidentialité des flux entre terminaux connectés à un même réseau Wi-Fi, il est demandé de le configurer en mode isolated.
- Il est demandé de désactiver systématiquement la fonction WPS (Wi-Fi Protected Setup)

des points d'accès.

- Sécuriser l'administration du point d'accès Wi-Fi, en:
 - utilisant des protocoles d'administration sécurisés (par exemple, HTTPS),
 - connectant l'interface d'administration à un réseau filaire d'administration sécurisé, a minima en y empêchant l'accès aux utilisateurs Wi-Fi,
 - utilisant des mots de passe d'administration robustes (respectant la politique de gestion des mots de passe présentée au chapitre Changer les éléments d'authentification par défaut sur les équipements et services), d'une longueur supérieure à 20 caractères.
- Il est demandé de remonter les événements de sécurité vers l'équipe réseau de la DIRCE.
- Lorsque des données sensibles (au sens RGPD), doivent être véhiculées via le réseau Wi-Fi, l'utilisation d'un protocole de sécurité spécifique, tel que TLS [DR8] ou IPsec, doit être mise en oeuvre.
- N'activer l'interface Wi-Fi que lorsqu'elle celle-ci doit être utilisée.
- Désactiver systématiquement l'association automatique aux points d'accès Wi-Fi configurés sur les terminaux.
- Maintenir le système d'exploitation et les pilotes Wi-Fi des terminaux à jour des correctifs de sécurité.

4.10.2 - Création ou extension de réseaux

En cas d'ajout ou de modification d'équipements réseaux du parc de la DIRCE, il est nécessaire de respecter les préconisations suivantes :

Faire valider par l'équipe de maintenance et le Pôle Equipements et Systèmes :

- l'architecture réseau proposée,
- la compatibilité des équipements réseaux déployés avec le reste du parc d'équipements en production,

La configuration d'équipements réseaux déployés au sein du parc de la DIRCE sera réalisée sous contrôle d'un technicien de la DIRCE.

4.11 - Sécuriser l'administration

4.11.1 - Utiliser les protocoles d'administration sécurisés

Il est imposé de **n'utiliser que des protocoles d'administration sécurisés** [DR09] sur

les systèmes et équipements, il est donc demandé en particulier :

- d'abandonner HTTP au profit de HTTPS, avec TLS en version TLS1.3 minimum,
- d'abandonner Telnet au profit de SSH, en version SSHv2 minimum.

4.12 - Choix des composants du système

4.12.1 - Privilégier l'usage de produits qualifiés par l'ANSSI

La qualification est prononcée par l'ANSSI et permet d'attester d'un niveau de sécurité et de confiance dans les produits et les prestataires de service listés dans les catalogues que publie l'agence.

La qualification offre donc des garanties de sécurité et de confiance sur les produits ou les prestations de service.

Cette qualification fait suite à une étude approfondie du fonctionnement technique de la solution et de son écosystème. **Il est demandé de privilégier l'usage de produits qualifiés par l'ANSSI lorsqu'ils sont définis.**

A titre d'exemple, la solution de « coffre-fort » de mots de passe KeePass2 a obtenu, pour sa version 2.10 portable, une Certification de Sécurité de Premier Niveau (CSPN) par l'ANSSI.

4.13 - Journalisation

Il est imposé la journalisation des accès aux données et des opérations effectuées suivants (horodatés et conservés pendant au moins un an) :

- pare-feu :
 - paquets bloqués,
- systèmes et applications :
 - authentification :
 - réussites et échecs d'authentifications,
 - gestion des comptes et des droits :
 - modification des données d'authentification (ajout ou suppression de compte / rôle et affectation de droits)
 - Modification des stratégies de sécurité :
 - édition / application / réinitialisation de configuration,
 - activité des systèmes et des processus :
 - démarrages / arrêts,
 - dysfonctionnements / surcharges du système,
 - chargements / déchargements de modules,
 - activité matérielle (défaillances, connexions / déconnexions physiques)
 - services :
 - erreurs de protocoles (par exemples les erreurs 403, 404 et 500 pour les services HTTP),

- traçabilité des flux applicatifs aux interconnexions (URL sur un relai HTTP, en-têtes des messages sur un relai SMTP, etc.).
- antivirus :
 - détections d'éléments suspects par l'antivirus.

Afin de pouvoir corréler ces événements entre différents composants, leur source de synchronisation de temps (grâce au protocole NTP) doit être identique.

4.14 - Contrôle de la prise en compte de ces mesures avant le déploiement en production

Il s'agit de **passer en revue la prise en compte par les projets de l'ensemble des mesures de cybersécurité listées** dans le présent document.

A cette fin, il est demandé d'envoyer à l'équipe cybersécurité de la DIRCE tous les éléments lui permettant d'apprécier la prise en compte des différentes mesures.

Si l'équipe cybersécurité de la DIRCE le juge nécessaire, des tests plus approfondis pourront être exigés avant la mise en production, par exemple via la mise à disposition d'une plateforme de tests ou de préproduction. À défaut, la vérification de l'application des mesures de sécurité pourra être vérifiée une fois le déploiement en production réalisé.

4.15 - Personnels en charge des prestations

4.15.1 - Liste de personnels intervenant sur le SI

Le titulaire s'engage à fournir une liste, régulièrement mise à jour, des personnels autorisés à intervenir sur le système d'information du maître d'ouvrage ainsi que leur niveau d'habilitation (types d'accès et ressources concernées de la DIRCE).

Le candidat précisera les moyens mis en oeuvre, dans le cadre de son processus de recrutement du personnel, pour vérifier les éventuelles condamnations, le cursus et l'expérience professionnelle des futurs employés.

Si le candidat ou des employés de son entreprise possèdent une habilitation au niveau Confidentiel-Défense, il pourra en faire mention.

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.

Dans le cadre de plans de sécurité gouvernementaux, le donneur d'ordres pourra imposer un renforcement des contrôles d'accès physiques et logiques à ces équipements.

4.15.2 - Qualification et formation dans le domaine de la SSI

Le titulaire sensibilise son personnel, intervenant dans le cadre des prestations, à la sécurité des systèmes d'information et aux règles de la DIRCE.

Le titulaire veille notamment à ce que son personnel intervenant dans le cadre des prestations respecte les dispositions concernant la sécurité du présent marché.

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 ;
- la fréquence et le contenu des actions de formation et de sensibilisation des personnels de l'hébergeur aux enjeux de sécurité.

4.15.3 - Exigences de sécurité pour les personnels extérieurs

Le candidat précisera les moyens de contrôle mis en œuvre pour s'assurer du respect des exigences de sécurité du donneur d'ordres par ses sous-traitants éventuels, ainsi que des consultants ou techniciens amenés à intervenir dans le cadre du support et de la maintenance sur le système de la DIRCE. Cette exigence peut être étendue à tous les types de soutiens (ménage, chauffage, climatisation, etc) si la sensibilité du système le justifie.

5 - Clauses de confidentialité type en cas de sous-traitance

Les supports informatiques et documents fournis par la société [identité du responsable de traitement] à la société [identité du prestataire] restent la propriété de la société [identité du responsable de traitement].

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 la société [identité du prestataire] prend connaissance à l'occasion de l'exécution du présent contrat.

Conformément à l'article 34 de la loi informatique et libertés modifiée, la société [identité du prestataire] s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

La société [identité du prestataire] 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 contrat, 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 contrat ;
- 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 contrat ;
- prendre toutes mesures de sécurité, notamment matérielles, pour assurer la conservation et l'intégrité des documents et informations traités pendant la durée du présent contrat ;
- et en fin de contrat, à procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations saisies.
-

À ce titre, la société [identité du prestataire] ne pourra sous-traiter l'exécution des prestations à une autre société, ni procéder à une cession de marché sans l'accord préalable de la société [identité du responsable de traitement].

La société [identité du responsable de traitement] se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées par la société [identité du prestataire].



MINISTÈRE CHARGÉ DES TRANSPORTS

*Liberté
Égalité
Fraternité*

**Direction interdépartementale
des routes Centre-Est**
228 rue Garibaldi
69446 Lyon Cedex 03
Tél : 04 69 16 62 00

www.developpement-durable.gouv.fr