



ESID de Bordeaux - Juin 2020

EXIGENCES D'HYGIENE CYBER DES S2I

(systèmes industriels d'infrastructure)

Socle minimum relatif aux marchés de maintenance

	Exigences
1	<p>Le titulaire devra désigner en son sein un point de contact Cyber (POC cyber) pour les besoins de ses prestations ; celui-ci sera garant des obligations contractuelles de cybersécurité de l'entreprise et de ses sous-traitants. Son niveau minimal requis correspond à la formation en ligne de l'ANSSI dite MOOC ("massive on line open course" = cours en ligne), gratuite.</p> <p>Une attestation de désignation du POC cyber devra être fournie dans l'offre par le titulaire ou, au plus tard, avant la notification du marché. En cas de changement de ce POC en cours d'opération, une nouvelle attestation devra être fournie.</p>
2	<p>Toute documentation relative au dossier cybersécurité du système industriel fera l'objet d'une mention de protection au minimum de type "Diffusion restreinte", exigeant un poste de travail isolé dans l'entreprise (aucune connexion à internet). Les exigences de l'instruction interministérielle 901 (II 901) devront être appliquées.</p> <p>Le chiffrement de fichiers sera utilisé pour tous les échanges sensibles sur des réseaux non protégés (Internet...). Le logiciel de chiffrement, à la charge de l'entreprise, devra être autorisé par l'ANSSI (ZED par exemple, ou ACID)</p> <p><i>Nota : le chiffrement de fichiers avec Zed! Free n'est pas autorisé; seule une version de Zed! qualifiée par l'ANSSI doit être utilisée.</i></p>
3	<p>Toute personne intervenant sur les systèmes industriels, pour leur modification de configuration ou maintenance, devra être formée à la cybersécurité. L'entreprise devra pouvoir attester que ces personnes ont toutes suivi une formation ou une sensibilisation aux risques cyber.</p> <p>Le titulaire peut se baser sur les supports et présentations de l'ANSSI pour établir sa formation de sensibilisation ; celle-ci sera à communiquer à l'ESID pour validation.</p>
4	<p>Tout personnel devant intervenir sur les systèmes devra y avoir été formellement autorisé préalablement par l'ESID, sur un document écrit. A cette fin, le titulaire devra établir la liste des personnes qu'il estime devoir travailler sur les systèmes.</p>
5	<p>Pour toute intervention sur un système industriel, une procédure de gestion des interventions devra être mise en place au préalable, qui identifiera :</p> <ul style="list-style-type: none">- la(les) personne(s) qui exécute(nt) le travail ;- la date et l'heure de l'intervention ;- le périmètre sur lequel le travail est exécuté ;- les actions réalisées ;- la liste des équipements retirés ou remplacés;- les modifications apportées et leur impact. <p>A l'issue de la prestation, un PV sera obligatoirement établi par le titulaire, et inséré dans le registre de l'USID.</p>
6	<p>Le prestataire devra vérifier, et mettre à jour si nécessaire :</p> <ul style="list-style-type: none">- la cartographie physique du système industriel qui correspond à la répartition physique des équipements ;- la cartographie des applications (programmes automates, applications de supervision, ...). <p><i>Nota : le titulaire se basera sur les documents de l'ANSSI : "Cartographie du système d'informations" et l'annexe A des "Mesures détaillées".</i></p>
7	<p>Les postes de travail, les serveurs... devront être installés dans des locaux à accès limité (fermés à clé, ou digicode, ou mobiliers sécurisés ...).</p> <p>L'accès aux équipements du système devra être protégé physiquement : armoires fermées à clé, mise en place de scellés...</p>

8	<p>Les postes de supervision et des équipements de terrain (automates) ne doivent pas avoir d'accès possible à Internet. L'accès aux ports Ethernet et USB du système ainsi que les connexions sans fil (Wi-Fi, Bluetooth, NFC, etc.) seront bloqués si ces derniers ne sont pas utilisés.</p> <p>Les équipements autorisés à se connecter aux installations dans le cadre des interventions devront être clairement identifiés et validés (PC dédiés validés par le bureau SSI de l'ESID) ; ils devront être marqués par le bureau SSI de l'ESID. Une attestation de contrôle cyber de l'équipement devra être en permanence présentable à l'Administration et présente avec l'équipement.</p>
9	<p>Seuls les médias amovibles (clef USB, disques durs, carte SD...) dédiés au système industriel (c'est-à-dire étiquetés comme tels) pourront se connecter sur le système. L'utilisation de ces médias pour tout autre usage est interdite. Réciproquement, l'utilisation de tout autre média est interdite.</p> <p>Les clefs USB seront fournies par l'Administration.</p> <p>Ces médias amovibles devront passer par un sas antiviral (ordinateur de l'USID dit "station blanche") avant d'être connecté au système. Si l'accès à un sas antiviral n'est pas possible, le titulaire s'engagera auprès de l'administration à ce que les médias utilisés ont été vérifiés et sont sains.</p>
10	<p>Lors d'un remplacement de matériel, les mots de passe par défaut de sortie d'usine devront être modifiables et modifiés. Les mots de passe seront transmis à l'Administration (RSSI-A) sous enveloppe scellée et datée/signée par le POC Cyber. Chaque modification du mot de passe sera tracée dans un registre tenu par l'Administration</p>
11	<p>Les équipements d'administration et les stations de maintenance ou d'ingénierie du système industriel, que ces équipements soient fixes ou nomades, devront être dédiés à ce seul usage et respecter des règles de durcissement de leur configuration. La mise à jour de ces moyens et leur éventuelle connexion à des réseaux tiers ne devra pas remettre en cause leur intégrité ni celle du système industriel.</p> <p>Pour les cas particuliers où l'intervenant apporte ses propres outils (outils de diagnostic propres à l'équipementier par exemple), une procédure sera mise en place pour vérifier que les équipements de l'intervenant ont un niveau de sécurité satisfaisant. Une telle situation ne doit arriver qu'en cas d'absolue nécessité et doit rester exceptionnelle.</p>
12	<p>Le processus de sauvegarde des données et configurations du système industriel initialement défini sera respecté, et régulièrement testé afin de permettre une restauration en cas d'incident. Les données concernées sont toutes les données nécessaires à la reconstruction de l'installation après un sinistre : programmes, fichiers de configuration, firmwares, paramètres de procédé (réglages d'asservissement par exemple), etc. Cela peut également concerner des données ayant un aspect réglementaire comme des exigences de traçabilité</p> <p>Les configurations devront être sauvegardées avant et après toute modification, y compris si celle-ci est apportée "à chaud". Les sauvegardes seront fournies dans un support amovible (clé USB) sain (contrôlé avant la livraison sur une station antivirale).</p> <p>Si le titulaire souhaite modifier le processus de restauration des sauvegardes sur les équipements, il devra le faire valider préalablement par l'USID.</p>
13	<p>Dans le cadre du MCS, le titulaire a l'obligation:</p> <ul style="list-style-type: none"> - de tenir systématiquement l'administration informée de la sortie des mises à jour logicielles et matérielles sur les produits objet du contrat en précisant les améliorations apportées ou les éventuels défauts corrigés ; - d'informer systématiquement l'administration de l'ensemble des failles de sécurité qu'il pourrait découvrir ou avoir connaissance sur tous les systèmes industriels d'infrastructure couverts par le contrat. Pour ces failles de sécurité, en complément de l'information sur leur criticité et leurs impacts, le titulaire précisera également si leur correction est envisagée et à quelle échéance ; - de prendre en compte les mises à jour et/ou les corrections de failles de sécurité sans régression de service. <p>Le titulaire précisera la date d'obsolescence des équipements ou de l'un de leurs composants, si celle-ci est disponible.</p>
