



ESID de Bordeaux - Avril 2020

EXIGENCES D'HYGIENE CYBER DES SII

(systèmes industriels d'information)

Dix règles générales relatives aux marchés de travaux

	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 clauses ci-après pour l'entreprise et ses sous-traitants. Une attestation 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> <p>Ce POC pourra utilement suivre le MOOC ("massive on line open course" = cours en ligne) gratuit de l'ANSSI afin de disposer du niveau minimal de sensibilisation.</p>
2	<p>Toute documentation relative au dossier cybersécurité du système industriel, s'il est requis dans le cadre du marché, 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 conception, mise en place, configuration et maintenance, devra être formée à la cybersécurité. L'entreprise devra pouvoir attester que ces personnes ont suivi une formation ou une sensibilisation aux risques cyber. 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, en conception, mise en place, configuration ou maintenance.</p>
5	<p>Le prestataire devra établir :</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>Une cartographie "Projet" sera soumise au stade VISA avant réalisation, et la cartographie finale sera fournie au stade des OPR (opérations préalables à la réception).</p> <p><i>Nota : pour les établir, le titulaire se basera sur les documents de l'ANSSI : "Cartographie du système d'informations" et l'annexe A des "Mesures détaillées".</i></p>
6	<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>
7	<p>Les postes de supervision et des équipements de terrain (automates) ne devront 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>

8	<p>Seuls les médias amovibles (clefs USB, disques durs, cartes 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 ou de la division Investissement dit "station blanche") avant d'être connectés 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>
9	<p>Lors de la mise en place, les mots de passe par défaut de sortie d'usine devront être modifiables et modifiés.</p> <p>Les mots de passe devront être transmis à l'Administration (RSSI-A) sous enveloppe scellée et datée/signée par le POC Cyber. Elle sera stockée dans un lieu sûr. Chaque modification du mot de passe devra être tracée dans un registre tenu par l'Administration.</p>
10	<p>Un processus de sauvegarde des données et configurations du système industriel devra être défini, mis en œuvre et testé afin de permettre leur restauration en cas d'incident. Les données concernées sont toutes les données nécessaires à la reconstruction de l'installation après un sinistre : les programmes, les fichiers de configuration, les firmwares, les 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 toutes modifications, y compris lorsque celles-ci ont été apportées "à chaud". Les sauvegardes seront fournies dans un support amovible (clé USB) sain (c'est-à-dire contrôlé préalablement sur une station antivirale).</p> <p>Le titulaire devra décrire un processus de restauration des sauvegardes sur les équipements ; il sera fourni et contrôlé lors de la phase de réception.</p>
