

[E041] - Le titulaire doit fournir un **Plan d'Assurance Sécurité**, document décrivant toutes les mesures prises pour répondre aux exigences de cybersécurité demandées ci-après et numérotées [Exxx].

[E001] - Le titulaire **désigne un interlocuteur cybersécurité, et communique son identité et ses coordonnées au prescripteur**. Durant le déroulement du marché, cet interlocuteur **sert d'interface avec le prescripteur** lors des discussions cybersécurité. Il est en charge de contrôler la mise en place de ces exigences, il **informe le prescripteur** de l'état de prise en compte des exigences et de leur avancement, des éventuelles divergences par rapport aux exigences et autres non-conformités.

[E002] - Le titulaire est responsable du Système Industriel durant les différentes phases du marché : du développement, de l'intégration, du fonctionnement, des essais, etc. Il assure les missions d'administration, d'exploitation, de surveillance et de maintenance du Système Industriel **jusqu'à la réception du marché**. Après réception du Système Industriel, l'ensemble des missions est transféré à l'exploitant.

[E015] – Le niveau de sensibilité de la documentation doit être défini et apparaître clairement sur les documents. Les documents doivent être traités en conséquence.

[E033] - **L'ensemble des outils employés sur le système** (ordinateurs, ordinateur portable de maintenance, média amovibles, etc) **deviennent la propriété du CEA et restent à demeure sur le site**. Au besoin ces outils peuvent être mis à disposition de l'intervenant le temps des opérations de maintenance prévues contractuellement.

En particulier, hors matériel très spécifique, les postes de travail sont fournis par le CEA. A ce titre **le titulaire fournit la liste complète des éléments (prérequis matériels minimaux (CPU, RAM, etc.), logiciels, procédures d'installation, etc.) nécessaires à l'installation, le paramétrage, l'exploitation et la maintenance du système**.

Les solutions logicielles et éventuels modules matériels doivent être compatibles avec Windows 10 Enterprise et supporter la présence de l'antivirus *Symantec Endpoint Protection*.

[E091] - **Les systèmes doivent intégrer un mécanisme permettant de s'arrêter sans provoquer de dégâts** (matériels ou humains). Il est demandé de mettre en place des mécanismes de sécurité ou d'arrêt d'urgence **s'appuyant sur des technologies robustes** (par exemple de type logique câblée). Ce mécanisme doit permettre au système industriel de s'arrêter ou de se mettre en sécurité **sans utiliser de composants pouvant faire l'objet d'une cyberattaque**.

[E135] – **Les accès du système industriel depuis et vers Internet sont interdits. Cette exigence s'applique dès la conception** : le système n'ayant pas vocation à accéder à Internet en exploitation, il ne doit pas non plus l'être en phase de conception. En particulier les logiciels devront pouvoir être installés, activés, configurés et utilisés sans accès direct à Internet.

[E155] – L'utilisation de **technologies de communications sans fil est interdite**.

[E186] – **L'emploi des médias amovibles** (clef USB, disquette, disque dur, etc.) **doit être limité au strict minimum nécessaire**. Le cas échéant, une politique d'utilisation des médias amovibles doit être définie.

[E198] – **L'usage des périphériques personnels, quels qu'ils soient** (téléphone, ordinateur, tablette, clef USB, appareil photo, etc) **est interdite**.