|  |  |  |
| --- | --- | --- |
| **Exigences CCTP** | **Réponses de l’offre technique du candidat (Documents ou moyens / méthodes**  **mises en place/Plan/justificatif)** | **Référence dans l’offre technique** |
| **[Ex S1]** A la livraison, aucun des systèmes d’exploitations, micrologiciels (‘firmwares’), logiciels et leurs composants (modules, librairies, …) ne doit faire l’objet de vulnérabilité connue ni d’obsolescence ; à ce titre, ils doivent être à jour des derniers correctifs de sécurité disponibles. |  |  |
| **[Ex S2]** A la livraison, aucun matériel ne doit faire l’objet d’une obsolescence technique connue (avérée ou à moyen terme). |  |  |
| **[Ex S3]** Tout échange de données d’un support appartenant au titulaire avec le MI doit obligatoirement être réalisé via une station blanche antivirale du client par transfert sur un support du client. |  |  |
| **[Ex S4]** En cas d’absolue nécessité de connecter un poste informatique du titulaire à des fins d’investigation ou de dépannage sur le MI du client, des garanties doivent être apportées par le titulaire, quant au niveau de sécurité du poste et de son innocuité virale (cf. FiSSII en [DA2]). L’intervention est soumise à l’approbation du client. |  |  |
| **[Ex S5]** Les postes informatiques permettant le pilotage, la configuration et la supervision du MI doivent être équipés d’un système d’exploitation soutenu et pouvant être mis à jour des correctifs de sécurité pendant toute la durée légale de garantie, plus 3 ans (5 ans au total). MICROSOFT Windows 11 est le système à privilégier ; tout empêchement doit être explicité et justifié. |  |  |
| **[Ex S6]** Les postes informatiques doivent disposer d’une solution antivirale conforme à la politique du MINARM : TREND MICRO APEX ONE AGENT en mode isolé. En cas d’incompatibilité, le titulaire doit apporter des justifications techniques et demander une dérogation au client. |  |  |
| **[Ex S7]** Les mises à jour du système d’exploitation et de l’antivirus doivent pouvoir être faites par le client en s’appuyant sur les serveurs de dépôt du MINARM. |  |  |
| **[Ex S8]** Les applicatifs installés sur les postes informatiques doivent fonctionner sur un compte utilisateur restreint aux droits d’un utilisateur standard. |  |  |
| [Ex S9] Les postes informatiques doivent être isolés de tout réseau MINARM ; aucun accès externe type internet n’est autorisé. |  |  |
| [Ex S10] Si l’environnement physique est insalubre (poussières, liquides, produits chimiques, brouillard), des ordinateurs type industriels équipés de filtres doivent être mis en place. Ils doivent être conformes au degré de protection IP50 ( [DA4] ). |  |  |
| **[Ex S11]** Le BIOS doit être configuré à l’état de l’art, et en particulier :   * Configuration d’un mot de passe d’accès aux paramétrages du BIOS ; * Paramétrage de boot exclusif sur le disque dur principal ; * Désactivation des périphériques inutiles : USB, CD/DVD-ROM, cartes réseau, lecteurs divers, micro, caméra, Wifi, Bluetooth… ; à défaut, les périphériques non autorisés doivent être bloqués physiquement (bloqueur de port USB / Ethernet …). * La configuration des systèmes d’exploitation, logiciels métier et équipements doit être durcie conformément à l’état de l’art, et en particulier : * Suppression des logiciels/services non indispensables à la fonction ; à défaut les désactiver ; * Désactivation des services à accès externes type envoi de rapport d’erreur, accès distant, * Désactivation de la fonction de scan automatique de l’antivirus, ainsi que la mise en quarantaine et la suppression automatique ; * Utilisation des protocoles de communication dans leur version sécurisée ; * Désactivation ou destruction des comptes inutiles et en particulier ceux à privilèges qui ne sont pas indispensables ; * Modification des mots de passe par défaut et utilisation de mots de passe robustes ; * Configuration des comptes nominatifs requis pour l’utilisation et l’administration selon le principe du moindre privilège ; * Activation des journaux systèmes et de sécurité permettant la traçabilité et l’imputabilité des actions sur le système (en particulier redémarrages, échecs d’authentification, problèmes d’intégrité, rejets de flux non autorisés, alertes virales, mises à jour système/ applicatives/ base virale) ; fonctionnement des journaux sur rotation avec alerte préalable à la rotation ; ces traces doivent être sauvegardées régulièrement et archivées afin d’être conservées 1 an (durée réglementaire). |  |  |
| **[Ex S12]** La configuration des automates et de leurs logiciels de gestion (configuration, diagnostic, supervision) doit être durcie conformément à l’état de l’art, et en particulier :   * Modification des mots de passe par défaut, usage de mots de passe robustes et suppression des comptes par défaut ; * Désactivation des services non utilisés ; * Désactivation des fonctions de débogage ; * Désactivation de la programmation à distance ; * Activation des fonctions de sécurité quand elles existent : contrôle d’accès des usagers et des flux autorisés, protection mémoire, protection du mode d’exécution, contrôle d’intégrité, communication sécurisée, journaux d’activité et d’erreurs, … |  |  |
| **[Ex S13]** La configuration de l’automate ainsi que les mises à jour du micrologiciel doivent être effectuées en point à point hors réseau. |  |  |
| **[Ex S14]** Le logiciel de configuration de l’automate doit être déconnecté en fonctionnement normal. |  |  |
| **[Ex S15]** Les automates et équipements réseau doivent être placés dans des boitiers sécurisés ou dans des armoires fortes fermées à clés. |  |  |
| **[Ex S16]** En complément aux exigences techniques précisées dans le CCTP, les livrables documentaires doivent être conformes à une nomenclature stable et pour la durée du contrat, du type : AAMMJJ\_NOM LIVRABLE\_sujet\_version |  |  |
| **[Ex S17]** La documentation technique et de maintenance est livrée sur support informatique au format bureautique standard ; en sus, 2 exemplaires papier des livrables notés (P) dans l’exigence suivante doivent être fournis. |  |  |
| **[Ex S18]** La documentation technique et de maintenance doit contenir :   * [ARCHI] L’architecture fonctionnelle et technique de l’ensemble des composants du MI : schémas technico-opérationnels, description du fonctionnement de la solution et des fonctions/services de chaque composant (y compris ceux de maintenance, configuration, supervision, diagnostic). Les protocoles de communication, interfaces, flux de données et de service doivent y être décrits. Les mesures de sécurisation doivent être explicitées. * [INV] L’inventaire de la configuration matérielle et logicielle du MI (systèmes d’exploitation, logiciels, composants logiciels, librairies, micrologiciels, …) des matériels informatiques et programmables (postes informatiques, périphériques, automates, cartes, équipements, …) à la livraison, et à chaque mise à jour, conforme au [DA3] . * La traçabilité des mises à jour et des correctifs des logiciels et micrologiciels effectuées sur le MI doit être incluse dans l’inventaire, ainsi que la liste des sources publiques utilisées pour les logiciels/micrologiciels. * [CONF] Les méthodes, rôles et moyens d’accès aux matériels informatiques et programmables, aux applications ; * La description des programmes, des configurations et paramétrages appliqués à tous les composants du MI ; la description de l’arborescence des dossiers des systèmes ; * Les guides de durcissement utilisés et les mesures de sécurisation appliquées. * [INST] La procédure d’installation et de paramétrage permettant la réinstallation du système complet ; les configurations à appliquer (paramètres, politique, …). * [ADMIN] (P) Les manuels d’administration (configuration/paramétrage, tâches de maintenance préventive [périodicité, durée] et d’exploitation de niveau administrateur) de tous les composants du MI ; * Les tâches de mise à jour, la procédure de sauvegarde et de restauration de chacun des composants numériques du MI (étapes, durées, outils et niveau d’expertise requis, spécificités liées au composant) ; * La supervision du MI, l’archivage, l’analyse des journaux, … * Le mode opératoire de contrôle des signatures numériques des logiciels/micrologiciels ; * Les procédures de diagnostic, dépannage d’urgence et de remise en service ; * Les manuels de programmation le cas échéant. * [MAN] (P) Les manuels d’utilisation de tous les composants du MI avec les tâches de maintenance préventive et d’exploitation de niveau utilisateur [périodicité, durée] ; * Les manuels de référence des constructeurs ; * [MDP] L’inventaire des comptes et des mots de passe du MI. * [EVOL] L’analyse annuelle des évolutions logiciel/micrologiciel. |  |  |
| **[Ex S19]** En complément aux exigences de formation précisées dans le CCTP, La formation au MI doit être réalisée sur site pour chaque profil d’utilisation (utilisateur / administrateur). Les tâches de maintenance et de diagnostic doivent être explicitées et expérimentées. Toutes les procédures de sauvegarde/restauration de chaque composant du MI (postes informatiques, automates, équipements réseau, …) doivent être déroulées. |  |  |