ANNEXE CYBERSECURITE

1. INTRODUCTION 2

2. ACTEURS ET CHAINE DE RESPONSABILITE 2

3. FORMATION 2

4. GESTION DES DOCUMENTS 3

4.1. MISE A JOUR DOCUMENTAIRE 3
4.2. SENSIBILITE DES INFORMATIONS ET DES DOCUMENTS 3
4.3. GESTION DES INTERVENTIONS 4
4.4. SAUVEGARDE/RESTAURATION 4

5. GESTION DES MEDIAS AMOVIBLES 4

6. ANTIVIRUS ET SAS 4

7. FILTRAGE DE SECURITE 5

7.1. INTERCONNEXION AVEC UN SYSTEME D'INFORMATION (INFORMATIQUE OU INDUSTRIEL) VIA UNE CONNEXION INTERNET 5

8. ADMINISTRATION DES COMPTES ET DES PROFILS 5

8.1. MOTS DE PASSE 5

9. ACCES AU SYSTÈME 5

9.1. ACCES PHYSIQUE AU SYSTEME 5
9.2. ACCES PHYSIQUE A LA SUPERVISION, AU PILOTAGE ET A L'INGENIERIE 5
9.3. TELEGESTION, TELEMAINTENANCE ET TELEDIAGNOSTIC DU SYSTEME 6

10. GESTION DE LA SECURITE 6

10.1. DURCISSEMENT DU SYSTEME 6
10.2. DURCISSEMENT DE LA SUPERVISION, DU PILOTAGE ET DE L'INGENIERIE 6

11. GESTION DES ELEMENTS CRYPTOGRAPHIQUES DES SYSTEMES DE CONTRÔLE D'ACCES PHYSIQUE ET DE VIDEOPROTECTION 7

12. TRAITEMENT DES DONNES SENSIBLES 7

12.1. MANIPULATIONS ET ECHANGES DE DONNEES SENSIBLES 7
12.2. GMAO 7

13. GESTION DE CRISES 8

14. CONTRÔLES ET AUDIT 8

1. INTRODUCTION

Le titulaire doit respecter les exigences de cybersécurité décrites dans cette annexe pour toute intervention de maintenance sur un système industriel d'infrastructure.

Un « Système Industriel d'Infrastructure » (S2I) désigne un système d'information pilotant automatiquement des installations physiques d'infrastructure (chauffage, climatisation, sas d'accès, extinction incendie, générateur électrique, etc.) à partir de données collectées par des capteurs (sondes thermiques, caméras, badgeuses, détecteurs de fumées, etc.).

L'application de ces exigences de cybersécurité doivent se faire en conformité avec les référentiels réglementaires suivant :

- [II 901] Instruction interministérielle n°901 du 28/01/2015 relative à la protection des systèmes d'information sensibles.
- [IM 900] Instruction Ministérielle n°900 du 15/03/2021 relative à la protection du secret et des informations *diffusion restreinte* et sensibles.
- [PSSI-E] Politique de sécurité des systèmes d'information de l'Etat du 17/07/2014.
- [PSSI-A] Politique de sécurité des systèmes d'information des Armées du 08/07/2016.
- [DIR 39] Directive DGNUM n°39 du 05/07/2016 relative à la sécurité des systèmes industriels.

2. ACTEURS ET CHAINE DE RESPONSABILITE

REF	LIBELLE
1	Le titulaire doit désigner en son sein un point de contact (POC) Cyber qui est en charge de la liaison avec la chaîne fonctionnelle SSI du MINARM (RSSI-A, OSSI…).
2	Le titulaire à la responsabilité pleine et entière de l'application de ces exigences de cybersécurité conformément aux référentiels réglementaires pour son entreprise et ses sous-traitants.

3. FORMATION

REF	LIBELLE
3	Le personnel intervenant sur les systèmes industriels doit avoir été sensibilisé à la cybersécurité, à l'usage du réseau informatique du Ministère et aux risques numériques propre à ces systèmes.

4. GESTION DES DOCUMENTS

4.1. Mise à jour documentaire

REF	LIBELLE
4	Toute maintenance impliquant la modification de l'architecture du système doit faire l'objet de l'actualisation de sa cartographie : — physique et logique ; — des applications (flux) ; Ces mises à jour doivent être remises au RSSI-A du Ministère en charge du suivi du système.
5	Toute maintenance impliquant la modification des documentations techniques du système doit faire l'objet de l'actualisation : — de la politique d'exploitation de sécurité (PES) quand elle existe ; — des guides utilisateurs et administrateurs ; — des fiches techniques de maintenance ; Ces mises à jour doivent être remises aux RSSI-A du Ministère en charge du suivi du système.

4.2. Sensibilité des informations techniques et des documents

REF	LIBELLE
6	La documentation relative à la cybersécurité (PES, plan d'adressage IP, configuration des équipements réseaux, etc.) du système industriel fait l'objet d'une mention de protection au minimum Diffusion Restreinte. Les exigences de l'[IM 900] doivent être appliquées. Le chiffrement de ces documents avant leur transfert via des réseaux non protégés (Internet…) est obligatoire. Les logiciels autorisés pour chiffrer sont : • ACID • ZED!, pour les industriels ne disposant pas d'ACID et n'ayant pas de contrat d'armement avec le ministère.

4.3. Gestion des interventions

REF	LIBELLE
7	Une procédure de gestion des interventions doit être mise en place afin de pouvoir identifier : — la personne qui exécute le travail et son commanditaire ; — 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 (avec les numéros d'identification) ; — les modifications apportées et leur impact. L'intervention est tracée dans un registre de suivi.

4.4. Sauvegarde/restauration

REF	LIBELLE
8	La configuration du système doit être sauvegardée avant et après toutes modification, y compris lorsque l'intervention n'a pas nécessité de redémarrage. La sauvegarde doit être tracée dans le registre de suivi des interventions.

5. GESTION DES MEDIAS AMOVIBLES

REF	LIBELLE
9	Des médias amovibles doivent être identifiés et dédiés à la maintenance des S2I. L'utilisation de ces médias pour tout autre usage est interdite. Réciproquement, l'utilisation de tout autre média externe au Ministère est interdite.

6. ANTIVIRUS ET SAS

REF	LIBELLE
10	Lorsqu'un échange de données via média amovible avec le système est nécessaire, l'usage d'un sas est obligatoire. Le sas ne doit pas être connecté au système industriel. L'échange d'information entre le sas et le système industriel s'effectue via un média amovible strictement dédié à cet usage. Le Ministère est responsable de la mise à disposition du média et de la mise à jour du sas.
11	Le titulaire et ses sous-traitants sont responsables de la mise à jour antivirus des équipements informatiques (tablette, pc portable, etc.) dédiés à la maintenance des systèmes industriels à chaque usage de ces derniers.
12	Pour tout systèmes industriels mettant en œuvre un antivirus, le titulaire et ses sous-traitants sont responsables de la mise à jour de l'antivirus à chaque introduction de codes sur ces mêmes systèmes.

7. FILTRAGE DE SECURITE

7.1. Interconnexion avec un système d'information (informatique ou industriel) via une connexion internet

REF	LIBELLE
13	Les postes de supervision, d'administration ainsi que les équipements de terrain du système industriel ne doivent pas avoir d'accès à Internet lors d'une opération de maintenance.

8. ADMINISTRATION DES COMPTES ET DES PROFILS

8.1. Mots de passe

REF	LIBELLE
14	Les mots de passe par défaut (mot de passe constructeur) des équipements composant le système industriel doivent être modifiés en respectant la stratégie des mots de passe définie dans la [PSSI-A]. Les mots de passe sont détenus par l'ESID (RSSI-A) sous enveloppe scellée. A chaque modification du contenu de l'enveloppe, une trace doit être consignée dans un registre tenu par l'administration.
15	Les mots passe des équipements composant le système industriel devront être renouvelés périodiquement tous les 2 ans ou sur demande de l'administration.

9. ACCES AU SYSTÈME

9.1. Accès physique au système

REF	LIBELLE
16	L'accès à des équipements du système protégés physiquement et nécessitant l'usage de clés ou de scellés doit être tracé dans le registre de suivi des interventions.

9.2. Accès physique à la supervision, au pilotage et à l'ingénierie

REF	LIBELLE
17	L'accès aux locaux où sont situés les postes de travail (supervision/administration) et les serveurs doit être tracé dans le registre de suivi des interventions.

9.3. Télégestion, télémaintenance et télédiagnostic du système

REF	LIBELLE
18	L'usage de la télémaintenance pour les systèmes de contrôle d'accès et de vidéoprotection est interdit.
19	En cas d'opérations de télégestion, télémaintenance ou télédiagnostic, le titulaire doit appliquer les règles suivantes : - les connexions doivent être faites à la demande ou d'après une périodicité définie par le Ministère ; - l'équipement de connexion distant doit être authentifié ; - le mot de passe de connexion devra être changé tous les 90 jours ou sur demande de l'administration ; - la journalisation doit être activée ; - après un délai d'inactivité de 5 minutes, la connexion doit être fermée ; - l'équipement doit être cloisonné et seuls les flux requis doivent être autorisés entre l'équipement et le reste du système industriel ; - les opérations de télémaintenance ne doivent être faites qu'à l'aide de protocoles sécurisés, assurant notamment l'intégrité, la confidentialité et l'authenticité des échanges.

10. GESTION DE LA SECURITE

10.1. Durcissement du système

REF	LIBELLE
20	Lors du remplacement d'un équipement défaillant, la configuration de sécurité initiale doit être conservée : désactivation des points d'accès physiques (ex : Ethernet et USB) et/ou sans-fil (ex : Wi-Fi, Bluetooth, NFC, RFID, etc.).

10.2. Durcissement de la supervision, du pilotage et de l'ingénierie

REF	LIBELLE
21	Les équipements d'administration et les stations de maintenance ou d'ingénierie du système industriel, que ces équipements soient fixes ou nomades, doivent être dédiés à ce seul usage et suivent des règles de durcissement de leur configuration (guides et recommandations ANSSI). La mise à jour de ces moyens et leur éventuelle connexion à des réseaux tiers ne doit pas remettre en cause leur intégrité ni celle du système industriel. Dans le cas où l'intervenant apporte ses propres outils (outils de diagnostic propriétaires à l'équipementier), 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.

11. GESTION DES ELEMENTS CRYPTOGRAPHIQUES DES SYSTEMES DE CONTRÔLE D'ACCES PHYSIQUE ET DE VIDEOPROTECTION

REF	LIBELLE
22	Lorsque qu'un dispositif susceptible de contenir des éléments cryptographiques est en panne, le titulaire doit, lorsque cela est possible, effacer voire supprimer ces éléments cryptographiques avant envoi du dispositif pour réparation chez un prestataire. Lors d'une mise au rebut d'un dispositif, le titulaire doit s'assurer que ces éléments cryptographiques ne pourront pas être extraits. Dans le cas où ces éléments ne peuvent pas être effacés, il conviendra de procéder à la destruction physique du dispositif.
23	Les certificats de chiffrement des équipements composant le système industriel de contrôle d'accès et de vidéoprotection doivent être renouvelés périodiquement tous les 2 ans ou sur demande du Ministère.

12. TRAITEMENT DES DONNES SENSIBLES

12.1. Manipulations et échanges de données sensibles

REF	LIBELLE
24	Le titulaire applique et fait appliquer les règles définies dans l'[II 901] dès lors qu'il traite, stocke ou échange des données sensibles. Le chiffrement des fichiers doit être utilisé pour l'échange des données sensibles via des réseaux non protégés (Internet…). Les logiciels autorisés pour chiffrer sont: • ACID • ZED!, pour les industriels ne disposant pas d'ACID et hors contrat d'armement.
25	Une politique de sécurité des systèmes d'information (PSSI) doit être appliquée et validée au plus haut niveau de l'entreprise du titulaire afin de couvrir tous les aspects, techniques ou non, de la cybersécurité (communication, ressources humaines et financières, juridiques, etc.).

12.2. Gestion de maintenance assistée par ordinateur (GMAO)

REF	LIBELLE
26	Le service de GMAO délivré par le titulaire doit prendre en compte les mesures de protection recommandées par le guide d'hygiène informatique de l'ANSSI.
27	Le titulaire doit disposer d'une cartographie de l'ensemble des systèmes d'information sur lesquels repose le service de GMAO dont il est responsable. Cette cartographie doit être tenue à jour.
28	L'hébergement des données sensibles du Ministère sur le territoire national est obligatoire.

13. GESTION DE CRISES

REF	LIBELLE
29	Le titulaire et ses sous-traitants doit obligatoirement alerter le Ministère de tout incidents de cybersécurité majeurs survenant sur ses systèmes d'information. Il devra tenir informé l'administration de la remédiation et du retour à la normale.

14. CONTRÔLES ET AUDIT

REF	LIBELLE
30	Durant la réalisation du marché, le Ministère peut conduire ou mandater des contrôles et audits de sécurité informatique des fournitures, prestations, moyens utilisés et services proposés par le titulaire ou ses sous-traitants afin de contrôler le bon respect des référentiels réglementaires cités en introduction de cette annexe.