



ANNEXE 2
CCTP CYBER - SOCLE DE SECURITE
Relatif A LA MAINTENANCE DE LA STATION DE DISTRIBUTION DE
CARBURANTS DE LA BASE NAVALE DE BREST

S'assurer de la validité de toute copie avant usage

	Nom	Fonction	Date/Visa
Rédaction	ICDD KERNEVES	Conseiller CYBER	<i>Acquis par visa</i>
Vérification	RCO A COMPLETER	RSSI-P/RCO	<i>Acquis par visa</i>
Vérification	SUPERIEUR A COMPLETER	Chef du RSSI-P/RCO	<i>Acquis par visa</i>
Validation	IC2ETA NEVEU	OSSI infra ou OSSI-L	<i>Acquis par visa</i>



SOMMAIRE

1.	INTRODUCTION	3
1.1.	Objet du document.....	3
1.2.	Structure du document.....	3
1.3.	Lecture du document	3
2.	EXIGENCES	4
2.1.	Acteurs et chaine de responsabilité.....	4
2.2.	Formation	4
2.3.	Gestion des documents	4
2.4.	Gestion des interventions.....	4
2.5.	Sauvegarde/restauration.....	5
2.6.	Gestion des médias amovibles.....	5
2.7.	Codes malveillants.....	5
2.8.	Filtrage de sécurité : interconnexion avec un SI via une liaison internet.....	5
2.9.	Administration des profils et des comptes	5
2.10.	Accès physique au système	6
2.11.	Accès physique à la supervision, au pilotage et à l'ingénierie	6
2.12.	Durcissement du système	6
2.13.	Durcissement de la supervision, au pilotage et à l'ingénierie	6
3.	ANNEXE 1 : SUIVI DU DOCUMENT	7
3.1.	Historique des versions.....	7
3.2.	Documents abrogés par la présente édition	7
4.	ANNEXE 2 : REFERENCES DOCUMENTAIRES	8
4.1.	Documents applicables	8
4.2.	Documents de référence	8

	<p style="text-align: center;">CCTP CYBER - SOCLE DE SECURITE Relatif A LA MAINTENANCE DE LA STATION DE DISTRIBUTION DE CARBURANTS DE LA BASE NAVALE DE BREST</p>
---	--

1. INTRODUCTION

1.1. Objet du document

Le socle de sécurité doit permettre d'établir les règles cybersécurité à mettre en place au profit du système à l'étude. Ce document est à destination de l'autorité d'homologation (AH).

Ce document est construit à partir de la Directive 39 version 2 de juin 2023 (DIR SNSI).

Il est structuré de telle manière que l'autorité peut ajouter, modifier ou déroger à certaines règles.

1.2. Structure du document

L'étude du système n'engageant que la mise en place d'un socle élémentaire, le présent document ne présente que ce socle.

1.3. Lecture du document

L'ensemble des exigences est applicable.

v 1.0	NP_8224_MCO_DISTRIBUTION_CARBURANT_BNB_CCTP_CYBER.docx	3 / 8
-------	--	-------

2. EXIGENCES

2.1. Acteurs et chaîne de responsabilité

1 (ORG) : Le prestataire doit désigner en son sein un point de contact CYBER (POC CYBER).

Une attestation de l'entreprise devra être fournie dès l'offre.

A chaque changement de ce POC CYBER une nouvelle attestation devra être fournie.

2.2. Formation

29 (ORG) : Le personnel intervenant sur les systèmes industriels doit être formé à la cybersécurité et attester avoir suivi une formation/sensibilisation.

Le support de sensibilisation sera fourni à l'Administration pour avis. Le titulaire peut se baser sur les supports et autres présentations de l'ANSSI.

2.3. Gestion des documents

8 (ORG) : Il est nécessaire d'établir/mettre à jour une cartographie :

- physique du système industriel ;
- logique du système industriel ;
- des applications (flux) ;
- de l'administration du système.

Une cartographie V0 sera fournie au titulaire à la notification de l'accord-cadre.

Nota : Le titulaire se basera sur l'annexe A du document « Mesures détaillées » de l'ANSSI en version 1.0 de janvier 2014 et sur le document « Cartographie du système d'information » de l'ANSSI en version 1.0 de novembre 2018.

20 (ORG) : La documentation relative au dossier cybersécurité du système industriel fait l'objet d'une mention de protection au minimum Diffusion Restreinte. Les exigences de l'instruction interministérielle 901 (II 901) doivent être appliquées.

Le chiffrement de fichiers doit être utilisé pour tous les échanges sensibles sur des réseaux non protégés (Internet...). Les logiciels autorisés sont :

- ACID
- ZED, pour les industriels ne disposant pas d'ACID et n'ayant pas de contrat d'armement avec le ministère.

2.4. Gestion des interventions

35 (ORG) : Une procédure de gestion des interventions doit être mise en place afin de pouvoir identifier :

- la personne qui exécute le travail et son donneur d'ordre ;
- 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 (y compris, le cas échéant, les numéros d'identification) ;

— les modifications apportées et leur impact.

36 (ORG) : Les équipements autorisés à se connecter aux installations dans le cadre des interventions doivent être clairement identifiés et validés. Ils doivent être marqués.

Une attestation de contrôle cyber de l'équipement doit être en permanence présentable à l'Administration et présent avec l'équipement.

99 (ORG) : Tout personnel devant intervenir sur les systèmes doit y être autorisé préalablement par l'administration.

2.5. Sauvegarde/restauration

15 (ORG TECH) : Un processus de sauvegarde des données et configurations du système industriel doit être défini, mis en œuvre et régulièrement 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

Les configurations doivent être sauvegardées avant et après toutes modifications, y compris lorsque celles-ci ont été apportées « à chaud ».

2.6. Gestion des médias amovibles

237 (ORG TECH) : Seuls les médias amovibles dédiés au système industriel peuvent 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.

2.7. Codes malveillants

241 (ORG TECH) : Un SAS doit être mis en place lorsqu'un échange de données via média amovible avec le système est nécessaire. Le SAS ne doit pas être connecté au système industriel. L'échange d'information entre le SAS et le système industriel s'effectue par médias amovibles strictement dédiés à cet usage.

Si l'accès à un SAS n'est pas possible, le prestataire s'engage auprès de l'administration à ce que les médias utilisés ont été vérifiés et sont sains.

2.8. Filtrage de sécurité : interconnexion avec un SI via une liaison internet

311 (TECH) : L'ensemble des postes de supervision et des équipements de terrain ne doivent pas avoir d'accès à Internet.

2.9. Administration des profils et des comptes

136 (ORG TECH) : Les mots de passe par défaut des équipements composant le système industriel doivent être modifiables et changés.



Les mots de passe doivent être transmis à l'ESID (RSSI-A) sous enveloppe scellée et datée/signée par le POC CYBER. A chaque modification du contenu de l'enveloppe, une trace doit être consignée dans un registre tenu par l'Administration.

2.10. Accès physique au système

104 (TECH) : L'accès aux équipements du système doit être protégé physiquement : armoires fermées à clé, mise en place de scellés, ...

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

102 (TECH) : Les postes de travail, les serveurs doivent être installés dans des locaux à accès limité (fermés à clé, digicode, mobiliers sécurisé, ...)

2.12. Durcissement du système

239 (TECH) : Bloquer les accès physiques (ex : Ethernet et USB) et/ ou sans-fil (ex : Wi-fi, bluetooth, NFC, etc.) du système si ces derniers ne sont pas utilisés.

2.13. Durcissement de la supervision, au pilotage et à l'ingénierie

259 (TECH) : 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 (ordre de priorité : guides DGA-MI, guides ANSSI, guides CIS). 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

Pour les cas particuliers où l'intervenant apporte ses propres outils (des 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.

3. ANNEXE 1 : SUIVI DU DOCUMENT

3.1. Historique des versions

Version	Date	Rédacteur	Vérificateurs	Approbateur	Nature de l'évolution
1.0		ICDD KERNEVES	RCO A COMPLETER SUPERIEUR A COMPLETER OSSI-L A COMPLETER	Représentant de l'AH	Édition initiale du document à codification unique

Important : Il appartient aux destinataires de détruire ou d'identifier les versions périmées du présent document

RÉPERTOIRE DE SUIVI DES ÉVOLUTIONS					
Version	Date	n° page	§	Référence du document traçant la modification	Description de la modification/observations

3.2. Documents abrogés par la présente édition

RÉFÉRENCES	DATE	OBJET

	<p style="text-align: center;">CCTP CYBER - SOCLE DE SECURITE Relatif A LA MAINTENANCE DE LA STATION DE DISTRIBUTION DE CARBURANTS DE LA BASE NAVALE DE BREST</p>
---	--

4. ANNEXE 2 : REFERENCES DOCUMENTAIRES

4.1. Documents applicables

Le tableau suivant présente les documents applicables.

REF.	DOCUMENT APPLICABLE
[PSSI-M]	Instruction ministérielle n° 7326/ARM/CAB du 25 juin 2018, édition 2, relative à la politique de sécurité des systèmes d'information du ministère des armées.
[PSSI-M-T]	Instruction N°7326-2/ARM/CAB édition n°2 relative au volet technique de la politique de sécurité des systèmes d'information (PSSI-M) diffusée par note n° 3475/ARM/CAB/ DR du 21 juillet 2021.
[II 901]	Instruction interministérielle n° 901/SGDSN/ANSSI du 28 janvier 2015 relative à la protection des systèmes sensibles.
[DIR HSI]	Directive n°27/DEF/DGNUM édition 3 du 7 juin 2022 portant sur l'homologation des SI du ministère.
[DIR S.INDUS]	Directive ministérielle DPID n°39, édition 2, portant sur la sécurité numérique des systèmes industriels, approuvée par la note n°DEP-00109/2023/ARM/DPID/NP du 9 juin 2023.
[IM 900]	Arrêté du 15 mars 2021 portant approbation de l'instruction ministérielle n° 900/ARM/CAB/NP sur la protection du secret et des informations <i>diffusion restreinte</i> et sensibles.
[DIR 27]	Directive n° 27 portant sur l'homologation des systèmes d'information du ministère des armées (DIR HSI), approuvée par la note n°DEP-00337/2022/ARM/DPID/NP du 7 juin 2022.
[GUIDE 7]	Guide DGNUM n°7, 4ème édition du 21 septembre 2022, portant sur l'intégration de la sécurité numérique dans le cycle de vie d'un système d'information.

4.2. Documents de référence

Le tableau suivant présente les documents de référence.

REF.	DOCUMENT APPLICABLE
[IM 1707]	INSTRUCTION N° 1707/ARM/CAB du 25 octobre 2021 relative aux infrastructures du ministère de la défense.
[CLASSIF]	Guide ANSSI Méthode de classification et mesures principales version 1.0 de janvier 2014
[MESURES DETAILLEES]	Guide ANSSI Mesures détaillées version 1.0 de janvier 2014

Signature du candidat :

v 1.0	NP_8224_MCO_DISTRIBUTION_CARBURANT_BNB_CCTP_CYBER.docx	8 / 8
-------	--	-------