

ACCORD CADRE UNIK

EXIGENCES DE CYBERSECURITE

Objet	Fonction	Grade – Nom (Unité ou Organisme)
Rédaction	Spécialiste cyberdéfense	Valentine ROULETTE
Vérification	SUPERIEUR HIERARCHIQUE	Christophe NEVEU
Validation	OSSI Infra ESID	Christophe NEVEU

Table des matières

1. Sensibilisation CYBER des intervenants	3
2. Modalités de reconstruction du SII après un incident.....	3
3. Documentation relative au SII.....	3
4. Gestion des mots de passe et des comptes	4
5. Verrouillage des modes de connexions inutiles au SII	4
6. Accessibilité physique au SII	4
7. Connexion à d'autres réseaux	4
8. Connexion d'équipements mobiles	5

1. Sensibilisation CYBER des intervenants

HYG-CYB-029 - Le personnel intervenant sur les systèmes industriels doit être formé à la cybersécurité et attester avoir suivi une formation/sensibilisation.

HYG-CYB-001 - 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. Modalités de reconstruction du SII après un incident

HYG-CYB-015 - 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 ».

3. Documentation relative au SII

HYG-CYB-008 - 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.

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.

HYG-CYB-020 - 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.

CYB-324 - Le titulaire doit fournir les procédures d'exploitation de la sécurité (PES) qui peuvent être incluses dans un dossier d'utilisation et d'administration (DAU) ou un dossier d'exploitation et de maintenance (DEM).

4. Gestion des mots de passe et des comptes

HYG-CYB-136 - 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.

CYB-319 - Les mots de passe des utilisateurs doivent être robustes, et spécifiques. La réutilisation de mots de passe pour différents systèmes d'information doit être proscrite par les règles organisationnelles.

CYB-129 - Les comptes par défaut et génériques ne doivent pas être utilisés sauf contrainte opérationnelle forte. Les comptes disposant de privilèges comme les comptes administrateurs ne doivent pas être des comptes génériques et doivent être distincts des comptes utilisateurs.

5. Verrouillage des modes de connexions inutiles au SII

CYB-209 - Sur les équipements, on doit désactiver :

- les comptes par défaut ;
- les ports physiques non inutilisés ;
- les supports amovibles, s'ils ne sont pas utilisés ;
- les services non indispensables (service web par exemple).

HYG-CYB-239 - 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.

6. Accessibilité physique au SII

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

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

7. Connexion à d'autres réseaux

HYG-CYB-311 - L'ensemble des postes de supervision et des équipements de terrain ne doivent pas avoir d'accès à Internet.

8. Connexion d'équipements mobiles

HYG-CYB-035 - 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.

HYG-CYB-036 - 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.

HYG-CYB-099 - Tout personnel devant intervenir sur les systèmes doit y être autorisé préalablement par l'administration.

HYG-CYB-237 - 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.

HYG-CYB-259 - 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.

HYG-CYB-241 - 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.

Remarque : les guides CIS peuvent servir de base pour estimer la charge de travail.