

Table des matières

1	Références.....	1
2	Introduction.....	2
3	Cybersécurité du marché	3
3.1	Point de contact	3
3.2	Sensibilisation.....	3
3.3	Sécurisation des transferts avec une mention de protection « DR » ou « DR SF ».....	3
3.4	Travailler en toute sécurité avec des informations NP	4
3.5	Stockage des informations DR ou DR-SF	5
3.6	Devoir de conseil	5
3.7	Etat de l’art	5
3.8	Rapport d’intervention.....	5
3.9	Accès à l’intranet du MinArm.....	6
3.10	Sauvegarde	6
3.11	Maintien en condition de sécurité (MCS).....	6
3.12	Gestion de l’obsolescence	7
3.13	Cartographie.....	7
3.14	Documents à fournir.....	7
3.15	Réversibilité	8
3.16	Incidents	8
3.17	Suppression des données du donneur d’ordre en fin de contrat	9
3.18	Hébergement Cloud	9
4	Synoptique.....	10
5	Exigences relatives au réseau.....	11
5.1	Plan d’adressage.....	11
5.2	Exigences relatives aux routeurs et WI-FI	11
5.3	Pare-feu	12
5.4	Réseau et commutateur.....	13
5.5	Télémaintenance	15
5.6	Liaison sécurisée.....	16
5.7	Exigences « radio »	16
6	Exigences relatives au matériel	19
6.1	Sécurité physique du matériel (poste informatique, EAR, etc).....	19
6.2	Périphériques sans fil	19
6.3	Support de stockage.....	19

6.4	Support de maintenance et équipement d'administration	19
6.5	Supports de logiciels.....	20
6.6	Automates	20
6.7	NAS (Network Attached Storage)	21
6.8	Nommage des équipements dans les systèmes.....	22
6.9	Ecran IHM	25
7	Exigences relatives aux systèmes d'exploitation, services et applications	26
7.1	Licences	26
7.2	Durcissement des systèmes d'exploitation	26
7.3	Politique des comptes et mots de passe	27
7.4	Exigences relatives aux annuaires	28
7.5	Configuration de l'anti-virus.....	30
8	Pénalités	32
9	Glossaire	33
	ANNEXE 1.....	36
	ANNEXE 2.....	38

1 Références

a) Guide d'hygiène informatique - ANSSI

<https://cyber.gouv.fr/publications/guide-dhygiene-informatique>

b) Maîtriser la SSI pour les systèmes industriels - ANSSI

https://cyber.gouv.fr/sites/default/files/IMG/pdf/Guide_securite_industrielle_Version_finale-2.pdf

c) Mesures détaillées pour la cybersécurité des systèmes industriels

<https://cyber.gouv.fr/publications/la-cybersecurite-des-systemes-industriels>

d) Référentiel des exigences de cybersécurité pour les prestataires d'intégration et de maintenance de systèmes industriels.

https://cyber.gouv.fr/sites/default/files/2016/03/Referentiel_exigences_prestataires_integration_maintenance_V1_0.1.pdf

e) Exigences de sécurité matérielle pour plateformes X86 - ANSSI, 08/11/2019

https://cyber.gouv.fr/sites/default/files/2019/11/anssi-guide-exigences_securite_materielle.pdf

f) Recommandations relatives à l'administration sécurisée des systèmes d'information - ANSSI, 11/05/2021

<https://cyber.gouv.fr/publications/recommandations-relatives-ladministration-securisee-des-si>

g) Cartographie du système d'information – ANSSI novembre 2018

<https://cyber.gouv.fr/publications/cartographie-du-systeme-dinformation>

h) Site de l'ANSSI <https://cyber.gouv.fr/>

2 Introduction

Ce document référence les exigences en matière de cybersécurité pour les prestataires d'intégration et de maintenance de systèmes industriels.

Il constitue également une aide pour les commanditaires qui voudront intégrer dans leur cahier des charges des clauses de cybersécurité issues des exigences du présent document. Ils pourront demander à leurs titulaires d'être conformes à ce référentiel d'exigences.

Il aborde successivement les exigences relatives :

- à la cybersécurité du marché ;
- au réseau ;
- au matériel ;
- aux systèmes d'exploitation, services et applications.

Il se termine par une notion des pénalités engendrées en cas de non-respect.

Le **Synoptique** en page **10** représente schématiquement des configurations de systèmes industriels d'infrastructure (S2I) connues à ce jour. Sous chaque matériel, des exigences surlignées en jaune renvoient vers les différents chapitres du document.

Les titulaires s'engagent en fonction du matériel, du réseau et de la technologie adoptée, à appliquer les exigences adéquates. Le bureau cyber du SID SO vérifiera lors de contrôles que l'ensemble des mesures de sécurité numérique demandées sont bien appliquées

Les titulaires s'engagent en fonction du matériel utilisé, du réseau déployé et de la technologie adoptée, à appliquer les exigences adéquates.

Dans le cas des opérations de maintenance si un matériel est présent mais non sécurisé ou les documents sont absents, le titulaire en relation avec le commanditaire et le Bureau cyber du SID SO appliquera les exigences en se référant au BPU.

Dans le cadre d'une homologation et en fonction de la spécificité du S2I, des exigences en concertation avec le bureau cyber pourront être rajoutées.

3 Cybersécurité du marché

3.1 Point de contact

Le titulaire devra désigner en son sein un point de contact cyber (POC cyber) pour les besoins des prestations ; **celui-ci sera garant des obligations contractuelles de cybersécurité de l'entreprise et de ses sous-traitants**. Son niveau minimal requis correspond à la formation en ligne de l'ANSSI dite MOOC (« massive on line open course » = cours en ligne), gratuite : [MOOC SecNumacadémie](#)

Une attestation de désignation du POC cyber devra être fournie dans l'offre par le titulaire. En cas de changement de ce POC en cours d'opération, une nouvelle attestation devra être fournie.

Remarque : les fonctions de RSSI-P et A (« Responsable de Sécurité du Système d'Information –Projet et Aval ») sont réservées à l'organisation du ministère.

3.2 Sensibilisation

Le titulaire doit s'assurer, pour chaque prestation, que les intervenants désignés pour réaliser la prestation ont les qualités et les compétences requises en matière de cybersécurité pour mettre en œuvre les mesures figurant dans ce guide.

De ce fait, les intervenants :

- doivent avoir suivi une formation en cybersécurité des systèmes industriels ;
- s'engagent à respecter les règles d'hygiène cyber et signent l'attestation de reconnaissance de responsabilité¹ de l'IM 2004² auprès du RSSI-P ou A.

3.3 Sécurisation des transferts avec une mention de protection « DR » ou « DR SF »

Le traitement des documents Diffusion Restreinte (DR) doit respecter les règles de l'instruction interministérielle 901.

Au format numérique, les documents DR doivent être échangés sous forme chiffrée par les logiciels ACID ou ZED! (version qualifiée par l'ANSSI), autorisés par le ministère pour effectuer l'envoi sur Internet de fichiers de niveau DR.

Cela implique que :

- le titulaire dispose d'un poste informatique spécifique, isolé d'internet, pour les informations « DR », avec ACID ou ZED! installé ;
- le titulaire devra identifier parmi son personnel (et celui de ses sous-traitants), les acteurs concernés par la cybersécurité et ayant besoin d'en connaître pour mener à bien leur mission et activités dans le cadre du présent contrat.

Le logiciel de chiffrement **ZED! Free** est interdit pour le chiffrement des données DR.

¹ Annexe 1

² Instruction ministérielle relative à la fonction d'administrateur de systèmes d'information et de communication au sein du ministère de la Défense
<https://www.legifrance.gouv.fr/download/pdf/circ?id=30268>

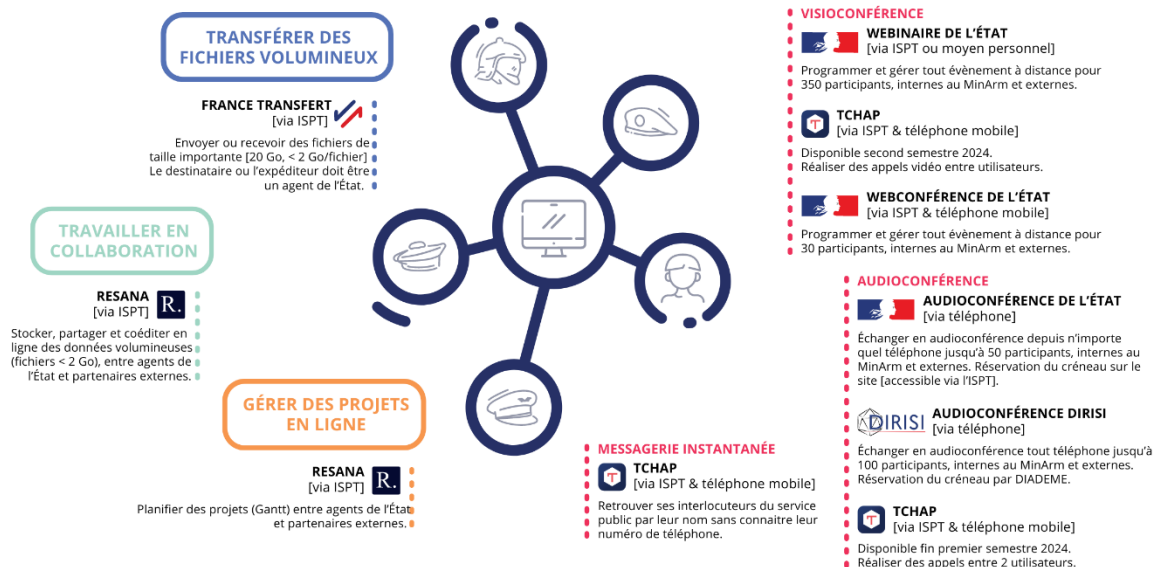
Il est aussi possible de transmettre les documents sensibles ou « DR » en format papier, sous double enveloppe.

3.4 Travailler en toute sécurité avec des informations NP

Le besoin de transférer des fichiers volumineux, communiquer à distance ou gérer des projets en ligne est réel.

LES OUTILS COLLABORATIFS

NON PROTÉGÉ (NP)



3.4.1 TRANSFÉRER DES FICHIERS VOLUMINEUX

- France transfert (via ISPT) :

Service créé par l'État pour aider ses usagers (citoyens, professionnels, entreprises, associations...), partenaires ou prestataires à envoyer aux agents de l'État ou recevoir des agents de l'État, des fichiers et dossiers volumineux (20 Go, <2Go/fichiers) qui ne peuvent pas transiter par les messageries électroniques.

- RESANA (via ISPT)

RESANA est ouvert à **tous les agents de l'État** et de ses **établissements publics**. Cet outil permet de stocker des fichiers NP en ligne pour une longue durée, et de les partager (fichiers < 200 Mo) de manière collaborative

Stocker, partager et coéditer en ligne des données volumineuses (fichiers < 2 Go), entre agents de l'État et partenaires externes.

3.4.2 COMMUNIQUER À DISTANCE

3.4.2.1 VISIOCONFÉRENCE

- WEBINAIRE DE L'ÉTAT (via ISPT ou moyen personnel)

Programmer et gérer tout évènement à distance pour 350 participants, internes au MinArm et externes.

L'outil vient en complément de la [Webconférence de l'État](#).

- WEBCONFÉRENCE DE L'ÉTAT [via ISPT & téléphone mobile]

Programmer et gérer tout évènement à distance pour 30 participants, internes au MinArm et externes.

3.4.2.2 AUDIOCONFÉRENCE

- AUDIOCONFÉRENCE DE L'ÉTAT [via téléphone]

Échanger en audioconférence depuis n'importe quel téléphone jusqu'à 50 participants, internes au MinArm et externes. Réservation du créneau sur le site [accessible via l'ISPT].

- AUDIOCONFÉRENCE DIRISI [via téléphone]

Échanger en audioconférence tout téléphone jusqu'à 100 participants, internes au MinArm et externes. Réservation du créneau par DIADEME.

3.5 Stockage des informations DR ou DR-SF

Les informations DR ou DR SF doivent être accessibles aux seules personnes ayant besoin d'en connaître. Elles seront donc stockées chiffrées de manière à limiter l'accès.

3.6 Devoir de conseil

Le titulaire est tenu à une obligation permanente de conseil et de mise en garde, relative aux matériels, logiciels et prestations fournis à l'acheteur. Dans ce cadre, le titulaire notifie à l'acheteur toute information permettant d'améliorer le niveau de sécurité du système d'information et signaler les difficultés et risques que certains choix peuvent entraîner.

3.7 Etat de l'art

La sécurisation des systèmes informatiques dépend de l'évolution des technologies. Il appartient au titulaire de mettre en œuvre les pratiques de sécurité, d'employer les outils qui soient adaptés aux enjeux de sécurité de l'acheteur et proportionnés à la menace pouvant s'exercer sur les biens à protéger...

3.8 Rapport d'intervention

Les interventions sur les systèmes industriels doivent être tracées. 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.

A l'issue de la prestation, un procès-verbal (PV) sera obligatoirement établi par le titulaire, et inséré dans le registre de l'USID dont une copie est envoyée au bureau cyber.

Le rapport doit contenir une liste de contrôle (check-list) des actions à réaliser après l'intervention, et en particulier confirmer que les sauvegardes des données (données de configuration, modifications de programmes, etc.) ont été réalisées.

3.9 Accès à l'intranet du MinArm

Si le contrat le stipule, les titulaires peuvent être amenés à accéder au réseau intranet du ministère, dit intradef, pour utiliser l'outil « Gestion Technique du Patrimoine » (GTP).

Une autorisation est obligatoirement délivrée à l'issue d'un processus interne qui exige la **nationalité française**, un contrôle de sécurité en cours de validité, une sensibilisation à la cybersécurité spécifique ainsi que la signature d'une attestation de responsabilité.

Les USID initieront leurs demandes auprès du bureau cyber conformément aux directives de l'OSSI du SID Sud-Ouest.

3.10 Sauvegarde

Les sauvegardes sont une mesure de sécurité essentielle pour protéger les données contre les pertes ou les dommages. Que ce soit en raison d'une défaillance matérielle, d'une erreur humaine, d'une catastrophe naturelle ou d'une cyberattaque, les données peuvent être perdues ou endommagées à tout moment. Les sauvegardes permettent de récupérer rapidement et facilement les données perdues ou endommagées, minimisant ainsi les temps d'arrêt et les pertes financières.

Un processus de sauvegarde des données et configurations du système industriel devra être défini, mis en œuvre et 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 devront être sauvegardées avant et après toutes modifications, y compris lorsque celles-ci ont été apportées "à chaud". Les sauvegardes seront fournies dans un support amovible (clé USB) sain conformément aux recommandations énoncées au § 6.3 (c'est-à-dire contrôlé préalablement sur une station antivirale).

En l'absence d'un processus de sauvegarde des données et configurations du système industriel et en se référant au BPU, il sera défini, mis en œuvre et testé.

3.11 Maintien en condition de sécurité (MCS)

Le MCS est un processus continu visant à maintenir les systèmes et les réseaux à jour, à corriger les vulnérabilités et à prévenir les menaces de sécurité. Le maintien en condition de sécurité permet de minimiser les risques de cyberattaques, de réduire les temps d'arrêt et de protéger les données sensibles.

Le titulaire s'engage à mettre en place des procédures et des moyens techniques dans le but de permettre des opérations de maintenance préventives et curatives pour maintenir le niveau de cybersécurité demandé (logiciels, firmware,).

Un équipement informatique comportant une mémoire physique rémanente ayant vocation à stocker ou traiter des informations sensibles (DR, DCP) ou classifiées soient identifiables ne retournent pas chez les tiers en cas de maintenance ou réparation

3.12 Gestion de l'obsolescence

Le titulaire s'engage à mettre en place un plan de gestion des équipement et d'application en cas d'obsolescence.

En cas de changement de matériel, le titulaire s'assure de l'interopérabilité du matériel.

De plus le titulaire s'engage à vérifier le bon fonctionnement de l'ensemble des composants une fois les changements opérés.

3.13 Cartographie

La cartographie, telle que le définit l'ANSSI (référence [g](#)) permet de représenter le système d'information ainsi que ses connexions avec l'extérieur. Cette représentation peut inclure, les matériels, logiciels et les réseaux de connexion.

Concrètement, la cartographie doit permettre de :

- réaliser l'inventaire patrimonial du système d'information, à savoir la liste des composants et leur description détaillée ;
- présenter le système d'information sous forme de vues, à savoir des représentations partielles du SI, de ses liens et de son fonctionnement. Elles visent à rendre lisibles et compréhensibles différents aspects du système d'information.

Si la cartographie est existante, le titulaire devra la mettre à jour avant la fin de la Garantie de Parfait Acheminement (GPA) et de Garantie de Bon Fonctionnement (GBF), à chaque modification et au minimum une fois par an.

Dans le cas contraire, il établira soit dans le cadre de l'opération soit en se référant au BPU dans le cadre d'une maintenance:

- la **cartographie physique** du système industriel qui correspond à la description des équipements physiques qui composent le système, leur répartition géographique sur les sites et dans les bâtiments. ;
- la **cartographie des applications** (programmes automates, applications de supervision, version des firmwares, systèmes d'exploitation et services ...) ;
- la **cartographie des infrastructures logiques** qui correspond à la répartition logique du réseau, le cloisonnement et les liens ainsi que les équipements en charge du trafic ou de la sécurité.

3.14 Documents à fournir

Au sein du ministère, les mesures de protection doivent être adaptées au niveau de la menace. Elles se traduisent par une maîtrise du système et de son fonctionnement.

En relation avec le bureau cyber du SID Sud-Ouest en charge du suivi et du contrôle du système, le titulaire fournira les documents suivants :

- procédures : d'installation et de mise à jour du système ;
d'administration du système ;
d'administration de la sécurité ;
suivi d'intervention techniques et gestion de la configuration ;
- le Plan d'Assurance Sécurité (PAS) décrit l'ensemble des actions spécifiques que le candidat doit mettre en œuvre lors de l'exécution du marché pour garantir le respect des exigences de sécurité de l'acheteur. ;
- seulement dans le cadre des opérations de travaux, le Plan De Sécurité (PDS) décrit les mesures appliquées sur les systèmes dont les cartographies décrites ci-avant ainsi que les justifications des mesures non appliquées.

3.15 Réversibilité

En raison des investissements importants qu'il nécessite, le contrat d'externalisation est destiné à s'inscrire dans la durée. Néanmoins, la clause de réversibilité doit permettre au client de reprendre la gestion de la fonction externalisée, soit pour l'exploiter directement, soit pour en confier l'exploitation à un tiers de son choix.

Le prestataire s'engage à apporter l'assistance nécessaire durant la période de migration pour faciliter le transfert des moyens de sécurité matériels et logiciels, et la reprise de leur exploitation par le client, ou par un autre prestataire de service. Le prestataire s'engage à garantir, lors du transfert, la sécurité des données et des applications qui lui ont été confiées, conformément à ses obligations. En outre, la phase de réversibilité ne doit pas, en principe, modifier la qualité, les termes et les conditions des services fournis durant le contrat et définis dans le niveau de service. En cas d'arrêt des prestations confiées au titulaire par le donneur d'ordres, l'ensemble des matériels, logiciels et documentations confiés au titulaire doivent être restitués.

À la fin de l'exécution du présent marché, le titulaire est tenu :

- de transférer à l'équipe du futur titulaire les informations sur le contexte fonctionnel et technique de l'ensemble applicatif ainsi que sur les aspects de suivi du projet ;
- de préparer un support informatique défini par le donneur d'ordres contenant tous les éléments (documentations, programmes, chaînes de compilation...) gérés par le titulaire actuel et qui seront, à l'issue de cette prestation, placés sous la responsabilité du futur titulaire (cette mise à disposition devra être faite sous un format pouvant permettre au futur titulaire d'installer, le cas échéant, l'ensemble de ces éléments sur une plate-forme de son choix pour examen approfondi par celui-ci) ;
- d'assurer une formation fonctionnelle approfondie (du type formation utilisateur et administrateur) aux personnels du futur titulaire, avec travaux pratiques sur poste de travail, en présence de représentants du donneur d'ordres. Cette formation devra s'appuyer sur les documentations utilisateurs et techniques rédigées par le titulaire.

3.16 Incidents

3.16.1 Sur le S2I

Le titulaire s'engage à signaler au donneur d'ordres, au plus tôt, tout incident de sécurité ou anomalies, qu'il serait amené à rencontrer ou observer durant l'exécution des prestations qui lui sont confiées.

3.16.2 Sur le système d'information du titulaire

Le titulaire s'engage à signaler auprès des interlocuteurs en sécurité des systèmes d'information désignés par le donneur d'ordres, tout incident de sécurité susceptible d'affecter directement ou indirectement les données ou le S2I de l'acheteur.

3.17 Suppression des données du donneur d'ordre en fin de contrat

Le titulaire conserve en lieu sûr les supports de stockage de données en fin de vie hébergeant des données du donneur d'ordres, en attendant de procéder à leur effacement ou à leur destruction avec des moyens adaptés visant à s'assurer qu'aucune donnée ne puisse être récupérée.

Le cas échéant, le titulaire ne met pas au rebut ou ne fait pas emporter par une société de maintenance, ou encore réutilise ces supports de sauvegarde à d'autres fins que celles prévues initialement sans l'autorisation expresse du donneur d'ordres.

3.18 Hébergement Cloud

Pour répondre à cet enjeu, l'ANSSI a développé des recommandations pour l'hébergement dans le cloud qui précisent, en fonction du type de système d'information, de la sensibilité des données et du niveau de la menace associée, les types d'offres cloud à privilégier.

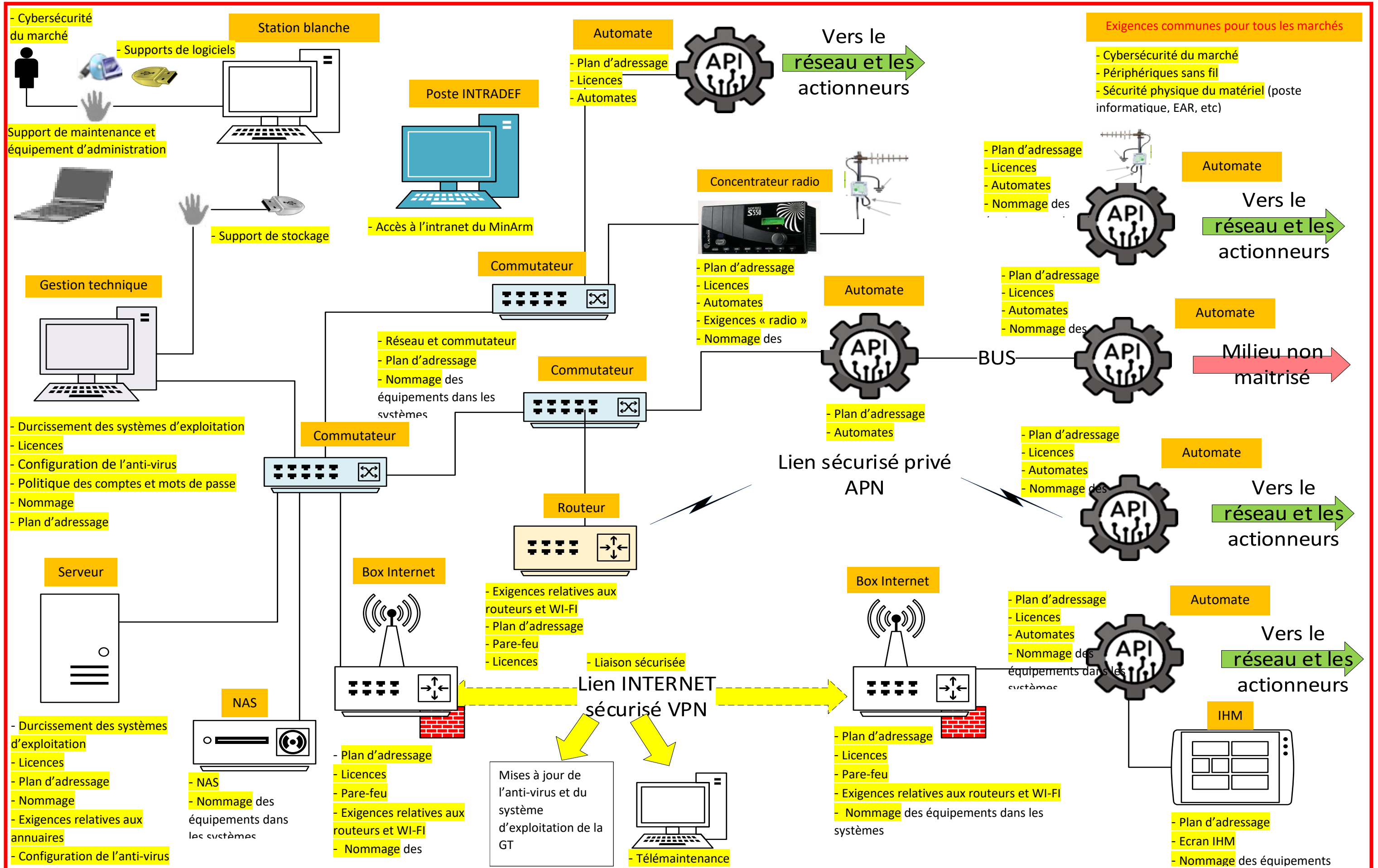
Pour des informations « DR », l'ANSSI préconise les offres cloud qualifiées SecNumCloud³ non commerciales (internes et communautaires) et commerciales privées permettant de disposer d'une infrastructure dédiée évitant le risque de latéralisation d'un attaquant depuis l'environnement d'un client vers un autre.

Il est notamment important pour le client de réaliser un certain nombre d'actions qui restent de sa responsabilité, notamment pour configurer les options de sécurité. À titre d'exemple, le déploiement ou la migration d'un système d'information sur une infrastructure cloud nécessitera la configuration des services de filtrage et de contrôle d'accès, pour s'assurer que seules les personnes légitimes accèdent aux interfaces d'administration et de supervision de sa solution.

Il est, par ailleurs, important de prévoir une clause de réversibilité permettant de faciliter la migration d'une technologie cloud vers une autre afin de limiter la dépendance à une seule offre cloud, et à ses évolutions fonctionnelles et de sécurité.

³ Élaboré par l'ANSSI, le référentiel SecNumCloud propose un ensemble de règles de sécurité et de bonnes pratiques d'hygiène informatique, garantissant un haut niveau d'exigence tant du point de vue technique, qu'opérationnel ou juridique

4 Synoptique



5 Exigences relatives au réseau

5.1 Plan d'adressage

Une adresse IP permet d'identifier chaque hôte connecté à un réseau informatique utilisant le protocole IP. Un ordinateur, une imprimante, un smartphone, un routeur, etc... tout périphérique connecté à un réseau et qui veut communiquer avec les autres hôtes du réseau doit disposer d'une adresse IP.

Les adresses IP privées ne peuvent pas être utilisées sur internet car elles ne peuvent pas être routées sur internet. Les hôtes qui les utilisent sont donc visibles uniquement dans le réseau local. Pour ces raisons, ces adresses seront à privilégier pour les S2I :

- Les adresses privées de la classe A : **10.0.0.0 à 10.255.255.255**
- Les adresses privées de la classe B : **172.16.0.0 à 172.31.255.255**
- Les adresses privées de la classe C : **192.168.0.0 à 192.168.255.255**

5.2 Exigences relatives aux routeurs et WI-FI

Les routeurs et les éléments actifs du réseau sont des composants clés de l'infrastructure réseau, et leur configuration incorrecte peut entraîner des vulnérabilités de sécurité qui peuvent être exploitées par des attaquants pour accéder au réseau et compromettre la sécurité des systèmes informatiques.

La mise en place de mesures de configuration des routeurs ou des éléments actifs d'un réseau est essentielle pour assurer la sécurisation du système dans son ensemble.

Mesures de sécurisation du routeur :

- mettre à jour le routeur avec le dernier micro-logiciel recommandé par le fournisseur :
 - o lors de la mise en place ;
 - o lors de la MCS ;
 - o lors d'une vulnérabilité critique ;
- créer des comptes nominatifs ou fonctionnels avec des privilèges limités en fonction des responsabilités de la ou des personne(s) conformément à la politique des comptes décrite au paragraphe 7.3 ;
- désactiver ou renommer tous les comptes par défaut ;
- désactiver les interfaces réseau non utilisées ;
- désactiver tous les services non utilisés ;
- désactiver le WPS ;
- désactiver l'IPv6 ;
- ne pas utiliser les plages d'adresses IP par défaut (exemple : 192.168.1.0/24) ;
- utiliser le HTTPS pour l'interface d'administration du routeur et désactiver l'interface une fois le routeur configuré ;
- dédier une interface physique à son administration ;
- conserver une sauvegarde sécurisée de la configuration du routeur en cas de panne ;
- utiliser les services IPS/IDS pour une meilleure protection, journalisation et gestion des alertes. Pour la journalisation, garder les journaux pendant maximum 1 ans.

Mesures de sécurisation du WI-FI:

- désactiver le wifi s'il n'est pas utilisé. Si celui-ci est utilisé⁴, le mot de passe par défaut doit être modifié par un mot de passe fort, utiliser le WPA3 et changer le SSID par défaut :
 - o longueur minimale des mots de passe de 14 caractères ;
 - o complexité des mots de passe avec l'utilisation de 3 types de caractères différents majuscules, minuscules, chiffres et caractères spéciaux ;
- désactiver l'accès à l'interface d'administration du routeur du réseau Wi-Fi (Accès seulement en filaire) ;
- s'assurer de la couverture d'un réseau Wi-Fi limitée au besoin :
 - o l'usage d'antennes directionnelles ou le réglage de la puissance des antennes permettent de contrôler la zone de couverture.

En présence de ce type de matériel et dont la sécurisation n'a pas été effectuée, le prestataire palliera à ce manque en appliquant ces exigences et en se référant au BPU.

5.3 Pare-feu

Un pare-feu est un élément clé de la sécurité réseau qui permet de protéger les systèmes et les réseaux contre les menaces de sécurité venant de l'extérieur et notamment d'internet telles que les attaques par déni de service, les intrusions et les logiciels malveillants. Cependant, pour qu'un pare-feu soit efficace, il doit être correctement configuré en fonction des besoins spécifiques des systèmes qu'il protège.

Mesures de sécurisation du pare-feu (Matériel) :

- mettre à jour le pare-feu avec le dernier micro-logiciel recommandé par le fournisseur (Système → Active Update) :
 - o Lors de la mise en place ;
 - o Lors de la MCS ;
 - o Lors d'une vulnérabilité critique ;
- créer des comptes nominatifs ou fonctionnels avec des privilèges limités en fonction des responsabilités de là ou des personne(s) ;
- créer des mots de passe complexes et sécurisés. conformément à la politique de mot de passe définie au paragraphe 7.3 ;
- désactiver ou renommer tous les comptes par défaut
- désactiver les interfaces d'administration de pare-feu de l'accès extérieur et public. (Système → Configuration → Administration du Firewall) ;
- dédier une interface Ethernet à l'administration ;
- désactiver l'interface WEB d'administration. Elle peut être réactivée uniquement pendant la configuration et modifications du pare-feu ;
- compléter les règles d'antispoofing ;
- désactiver les interfaces réseau non utilisées (Réseau → Interfaces) ;
- synchroniser au serveur NTP existant, s'il n'y a pas de serveur NTP configuré, utiliser celui du pare-feu qui lui sera synchronisé au serveur NTP sur internet :
 - o Serveur : 0.fr.pool.ntp.org
 - o Serveur : 1.fr.pool.ntp.org

⁴ L'utilisation est assujettie à une autorisation du bureau cyber.

- Serveur : 2.fr.pool.ntp.org
- Serveur : 3.fr.pool.ntp.org
- modifier le certificat par défaut de l'interface web d'administration en utilisant l'IGC du pare-feu comme StormShield ou autre si existant ;
- utiliser les certificats pour la connexion au VPN géré par l'IGC (les certificats par défaut sont interdits. Utiliser des certificats auto signés par l'éditeur du VPN);
- utiliser SNMPv3 si besoin de supervision à distance du pare-feu.

Les zones de pare-feu (Matériel) :

- isoler dans un réseau dédiée les équipements qui ont un service exposé sur le réseau extérieur (DMZ).

Les règles de pare-feu :

- désactiver les règles implicites par défaut ;
- ajouter une règle explicite qui bloque tout le trafic entrant et sortant de chaque interface, puis autoriser les flux souhaités ;
- les règles de pare-feu doivent être rendues aussi spécifiques que possible aux adresses IP source et/ou de destination et aux numéros de port exacts chaque fois que possible ;
- faire des tests de ce qui ne devrait pas être autorisé et vérifier que les services autorisés fonctionnent correctement.

Autres services de pare-feu (Matériel et logiciel) :

- utiliser les services IPS/IDS pour une meilleure protection, journalisation et gestion des alertes. Pour la journalisation, garder les journaux pendant maximum 1 ans ;
- certains pare-feu proposent des services supplémentaires comme DHCP, DNS, etc. Désactiver tous les services que vous n'avez pas l'intention d'utiliser.

Autres (Matériel et logiciel) :

- conserver une sauvegarde sécurisée de la configuration du pare-feu en cas de panne ;
- maintenir le micro-logiciel / logiciel à jour avec des tests de non régression (Effectuer une sauvegarde avant la mise à jour).

En présence de ce type de matériel et dont la sécurisation n'a pas été effectuée, le prestataire palliera à ce manque en appliquant ces exigences et en se référant au BPU.

5.4 Réseau et commutateur

Les commutateurs sont des équipements de transit pour une quantité importante d'informations. Il convient donc de porter une attention particulière à leur niveau de robustesse face à des attaques venant du réseau.

- dédier une interface physique du commutateur à son administration ;
- mettre en place une séparation physique ou un cloisonnement logique utilisant des VLAN pour appliquer cette séparation entre les réseaux d'administration et les réseaux métier ;
- ne pas désactiver le port console des commutateurs ;
- utiliser le protocole SSH en version 2 pour l'administration à distance des commutateurs ;

- désactiver le serveur web de gestion du commutateur, que ce soit en version sécurisée (HTTPS) ou non (HTTP) ;
- supprimer les certificats créés par défaut sur le commutateur ;
- ne pas utiliser le protocole Telnet pour l'administration à distance des commutateurs lorsque des protocoles plus sécurisés sont supportés par l'équipement. Si Telnet doit être utilisé du fait de l'absence de protocoles sécurisés, mettre en place les moyens adéquats de sécurisation du réseau sur lequel vont transiter ces flux ;
- un commutateur ne doit disposer que d'une seule adresse IP dédiée à son administration ;
- prendre les mesures nécessaires au sein du SI afin de n'autoriser l'accès à l'interface d'administration des commutateurs qu'aux administrateurs, notamment par l'utilisation de filtrage au niveau des pare-feu. Si cela n'est pas possible, la mise en place des ACL sur le commutateur peut être envisagée en tant que mesure palliative ;
- activer la journalisation des authentifications et tentatives d'authentification ;
- mettre en place des contre-mesures pour protéger le commutateur des attaques de type brute force. (Exemple commande CISCO : login block - for 300 attempts 3 within 120 / login delay 2) ;
- protéger les fichiers de configuration contenant des mots de passe, ceux-ci étant soit stockés en clair, soit retrouvables facilement par une personne malveillante. Supprimer les mots de passe des fichiers de configuration en cas de partage de ces fichiers avec d'autres personnes ou entités ;
- supprimer les comptes par défaut - au minimum, les désactiver - tout en veillant à conserver au moins un compte administrateur local « de secours » ;
- la politique de sécurité des mots de passe des comptes utilisateurs doit respecter la PSSI en vigueur ;
- désactiver les services de configuration automatique des VLAN, VTP, MVRP ou GVRP selon les commutateurs ;
- interdire la configuration automatique des ports (en mode trunk ou access) et configurer ceux-ci de façon sécurisée, notamment :
 - o Dans le cas des ports en mode access : ne configurer que le VLAN nécessaire sur un port donné ;
 - o dans le cas des ports en mode trunk : n'autoriser que les VLAN devant effectivement circuler sur le port trunk.
- tous les ports qui sont censés être inutilisés doivent être associés au VLAN de quarantaine. Les ports placés dans ce VLAN ne doivent donner accès à aucune ressource du système d'information et doivent interdire les communications avec toute autre machine, y compris les machines placées dans ce VLAN. Ces ports doivent aussi être désactivés, de même que le VLAN de quarantaine et l'interface associée ;
- le VLAN par défaut ne doit jamais être utilisé ;
- le VLAN natif :
 - o Doit être configuré afin d'être différent du VLAN par défaut ;
 - o ne doit être attribué à aucun port en mode access (il ne doit pas être utilisé pour faire circuler du trafic métier ou d'administration ;
 - o doit être le même sur tous les commutateurs du même domaine de diffusion (et de préférence dans tout le système d'information par principe d'homogénéité) afin d'éviter les comportements inadéquats.

- le routage interVLAN doit être assuré par des équipements de niveau 3. Celui-ci doit donc être désactivé sur les commutateurs d'accès ;
- désactiver la fonctionnalité de Source routing ;
- activer les fonctions de DHCP snooping et d'IP Source Guard afin de pallier les faiblesses de sécurité du protocole DHCP ;
- activer les fonctions d'inspection ARP ;
- activer des protections contre la propagation des trames Spanning Tree sur les ports d'accès ;
- activer le mode portfast ou edge port (selon le constructeur) sur les ports connectés à des machines clientes. Ne pas activer ce mode sur les interfaces connectées à d'autres commutateurs ;
- synchroniser l'heure des commutateurs de son système d'information de manière automatisée afin de garantir une cohérence de l'heure de ses équipements. Utiliser si possible plusieurs sources de temps situées au sein du système d'information ;
- régler le niveau de journalisation des commutateurs pour l'adapter aux besoins de journalisation du SI et si possible activer l'envoi des journaux vers un serveur de collecte (exemple : syslog) ;
- dans le cadre de la centralisation des journaux du commutateur, faire remonter les événements par le réseau d'administration afin d'éviter la fuite d'informations sensibles ;
- activer la journalisation des commandes entrées par les administrateurs ;
- utiliser SNMP en version 3 AuthPriv, si cela n'est pas possible techniquement, utiliser à défaut la version 2c. Ne pas utiliser le protocole SNMP en mode set pour administrer les commutateurs ;
- afin d'augmenter la bande passante ou d'assurer une redondance sur les liens réseau entre les commutateurs de desserte et de distribution, il est recommandé de mettre en place l'agrégation de lien (aussi appelée EtherChannel ou Bridge Aggregation) ;
- homogénéiser les configurations matérielles et logicielles des commutateurs de son système d'information afin de faciliter leur MCO/MCS ;
- mettre à jour régulièrement le système d'exploitation des commutateurs afin de les protéger contre les failles de sécurité corrigées par ces mises à jour ;
- centraliser l'administration des commutateurs au sein du système d'information.
- mettre en place une procédure de sauvegarde, restauration de la configuration des commutateurs. Tester les procédures de façon régulière ;
- activer le chiffrement des mots de passe contenus dans le fichier de configuration.

En présence de ce type de matériel et dont la sécurisation n'a pas été effectuée, le prestataire palliera à ce manque en appliquant ces exigences et en se référant au BPU.

5.5 Télémaintenance

Dans le cadre d'un accès de télémaintenance à une ressource informatique (matériel, logiciel) du SID Sud-Ouest, le titulaire doit obtenir l'accord et présenter des mesures de sécurité renforcées au bureau cyber.

Exemples de mesures de sécurité renforcées :

- sécurisation de l'infrastructure de raccordement réseau ;

- mise en place de mots de passe spécifiques pour l'accès en télémaintenance respectant des règles de robustesse et de renouvellement ;
- activation sur demande des accès entrant en télémaintenance. Par défaut, les accès entrants doivent être inactifs ;
- journalisation des accès en télémaintenance ;
- interdiction des possibilités de rebond depuis l'accès en télémaintenance vers le reste du réseau local de l'acheteur.

5.6 Liaison sécurisée

L'utilisation d'un lien Internet est assujéti à l'accord du bureau cyber du SID SO.

Cette liaison sera accessible via un accès internet (par exemple à partir d'une BOX, 4G, ...).

Les différents abonnements retenus (BOX, VPN, 4G...) seront à intégrer dans le marché.

Exigences à mettre en place sur le matériel informatique :

- prévoir un maintien en condition sécurisé (MCS) hors ligne ;
- le poste ne doit pas atteindre l'Internet (WWW) ;
- mot de passe WIFI usine modifié par mot de passe renforcé et chiffré en WPA2/PSK ;
- modification du mot de passe par default de la page d'administration de la BOX (14 caractères).

Les mots de passe devront être transmis à l'Administration (RSSI-A) sous enveloppe scellée et datée/signée par le POC Cyber. Celle-ci sera stockée dans un lieu sûr.

5.7 Exigences « radio »

L'utilisation de fréquences nécessite un examen administratif et le paiement d'une redevance.

Mais, un certain nombre de bandes de fréquences, dites « libres », peuvent être exploitées sans autorisation administrative, facilitant ainsi leur utilisation.

Bandes libres	Bandes soumises à autorisation individuelle
<ul style="list-style-type: none"> • Pas de demande d'autorisation • Gratuité d'utilisation des fréquences • Droit collectif d'utilisation • Pas de garantie de protection contre les brouillages. <p><i>Exemples : Wi-Fi, télécommandes, implants médicaux.</i></p>	<ul style="list-style-type: none"> • Autorisation individuelle préalable • Redevance d'utilisation des fréquences • Droit exclusif d'utilisation • Garantie de protection contre les brouillages <p>Exemples : opérateurs mobiles, liaisons de faisceaux hertziens.</p>

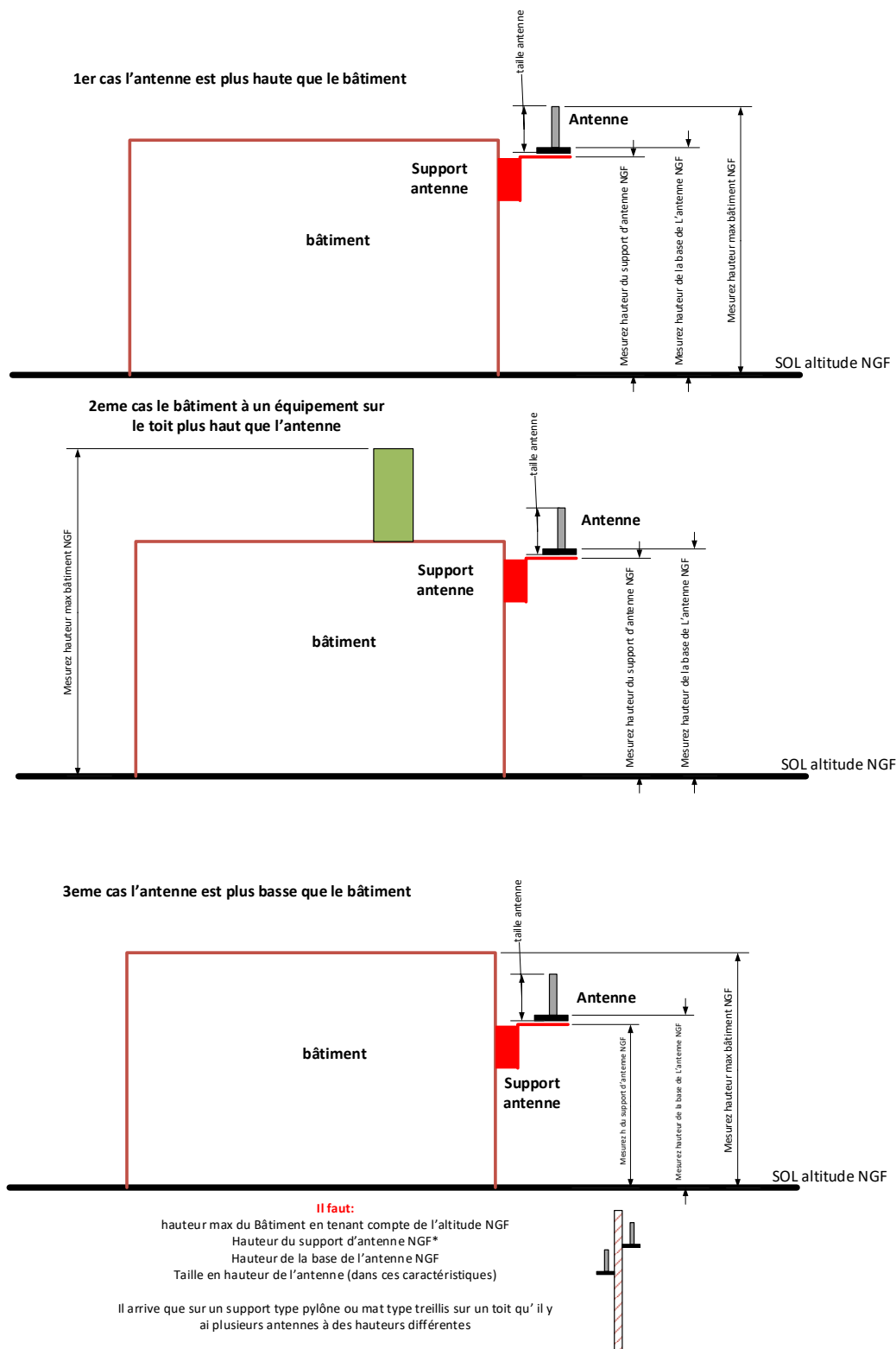
Quelques bandes libres remarquables

Fréquences	Utilisations notables
13 553 – 13 576 kHz	RFID, NFC
169,4 – 169,8125 MHz	Wize

433,05 – 434,79 MHz	Talkies-walkies, télécommandes, LoRa
863 – 868,6 MHz	z-Wave, Sigfox, LoRa, RFID UHF, Zigbee
868,7 – 869,2 MHz	
869,3 – 869,65 MHz	
869,7 – 870 MHz	
2400 – 2483,5 MHz	Wi-Fi, Bluetooth, Zigbee, Thread
5150 – 5350 MHz	Wi-Fi
5470 – 5725 MHz	

Procédures pour l'USID:

- envoyer un message officiel (NeMO) pour expliquer le besoin à l'ESIC AERO pour les bases aériennes ou à la DIRISI de Bordeaux pour les autres organismes. Les fiches techniques du matériel et l'implantation des antennes sont à fournir ;
- après accord et une fois que l'installation est terminée, fournir un plan détaillé précisant les éléments des antennes en fonction des cas décrits ci-dessous.



La contrepartie de la simplicité d'usage des bandes libres est l'absence de garantie contre le risque de brouillage. Le titulaire doit s'assurer que le matériel, les logiciels et le réseau qu'il aura choisis satisferont aux besoins et garantissent une disponibilité du système.

6 Exigences relatives au matériel

6.1 Sécurité physique du matériel (poste informatique, EAR, etc)

Dans le cadre des opérations de travaux, l'accès aux équipements du système (poste de travail, serveur, ...) devra être protégé physiquement : locaux à accès limité (fermés à clé, ou digicode, ou mobiliers sécurisés, mise en place de scellés...).

6.2 Périphériques sans fil

L'utilisation de périphériques sans fil (clavier, souris, ...) est interdite.

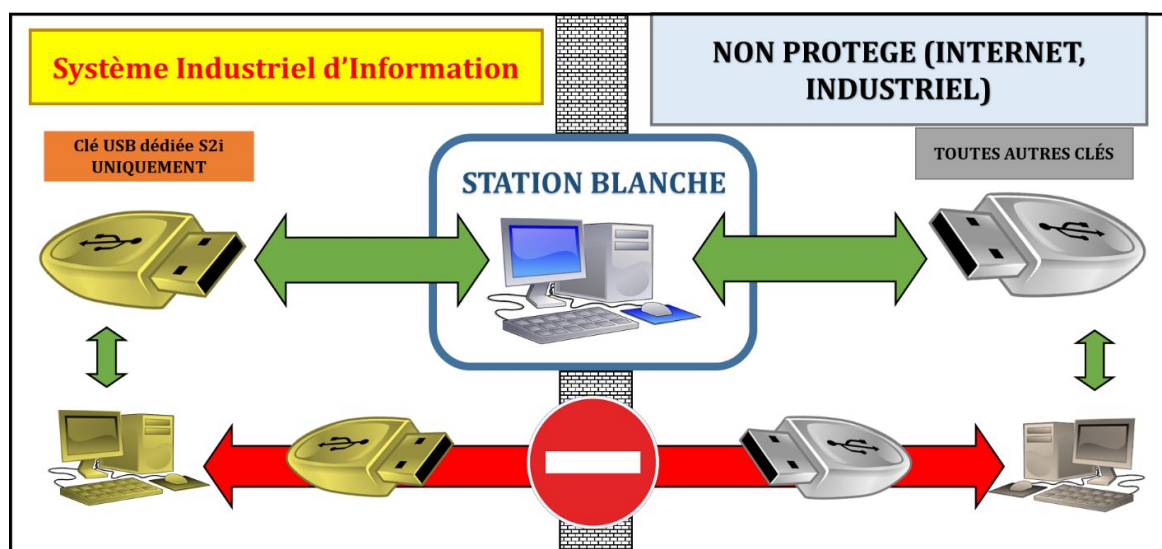
6.3 Support de stockage

Seuls les médias amovibles (clef USB, disques durs, carte SD...) dédiés au système industriel (c'est-à-dire étiquetés comme tels) pourront se connecter sur le système. L'utilisation de ces médias pour tout autre usage est interdite.

Les médias amovibles seront fournis par le titulaire. Ils seront préparés par le bureau cyber avant toute utilisation.

En l'absence de supports et en se référant au BPU, le titulaire de maintenance fournira ces supports.

Les supports extérieurs dits « non maîtrisés » seront connectés à un sas antiviral (ordinateur de l'USID dit "station blanche") pour le transfert des données vers les supports dédiés au système.



6.4 Support de maintenance et équipement d'administration

Le titulaire doit s'assurer que les outils de maintenance qu'il utilise ne contiennent pas de données sensibles du commanditaire ou alors que les outils pour en assurer la confidentialité sont bien mis en œuvre.

Le titulaire doit mettre en œuvre des éléments pour renforcer la sécurité des outils de maintenance. Il pourra pour cela, s'appuyer sur les guides et notes techniques publiés sur le site de l'ANSSI.

Les équipements utilisés devraient être exclusivement dédiés aux systèmes industriels du commanditaire.

Pour les cas particuliers où l'intervenant utilise ses propres outils (des outils de diagnostic propres à l'équipementier par exemple), il s'engage à utiliser du matériel avec un niveau de sécurité satisfaisant.

Le titulaire s'engage donc à :

- n'utiliser, sur les matériels et systèmes du MINARM, que des médias amovibles neufs, formatés, enregistrés auprès du bureau cyber ou du CSSI de l'USID, excepté si une contrainte le justifiant a été acceptée par le donneur d'ordres ;
- effectuer un contrôle d'innocuité de ces médias avant toute connexion sur les matériels dont il a la charge ;
- signaler, au plus tôt, tout incident concernant ce type de média ;
- utiliser un PC de maintenance dédiés pour un usage professionnel et remplir l'attestation sur l'honneur en annexe 2.

6.5 Supports de logiciels

Les livraisons de productions logicielles effectuées par le titulaire devront avoir fait l'objet en amont d'un contrôle antivirus.

Dans ce cadre un certificat d'innocuité précisant à minima le nom de la suite antivirus utilisée, les numéros du moteur et de la base de signature en exploitation lors de l'opération, la date du contrôle et son résultat sera fourni au donneur d'ordres en accompagnement de la fourniture logicielle.

6.6 Automates

Dans le cadre des opérations de travaux, l'accès aux équipements du système devra être protégé physiquement : armoires fermées à clé, mise en place de scellés.

Les postes de supervision et des équipements de terrain (automates) ne devront pas avoir d'accès possible à Internet. L'accès aux ports Ethernet et USB du système, ainsi que les connexions sans fil (Wi-Fi, Bluetooth, NFC, etc.), seront bloqués si ces derniers ne sont pas utilisés.

Les équipements autorisés à se connecter aux installations dans le cadre des interventions devront être clairement identifiés et validés (PC dédiés validés par le bureau cyber du SID Sud-Ouest) ; ils devront être marqués par le bureau cyber du SID Sud-Ouest. Une attestation de contrôle cyber de l'équipement devra être en permanence présentable à l'Administration et présente avec l'équipement

Lors de la mise en place ou d'un remplacement, les mots de passe par défaut de sortie d'usine devront être modifiables et modifiés.

Les mots de passe devront être transmis à l'Administration (RSSI-A) sous enveloppe scellée et datée/signée par le POC Cyber. Elle sera stockée dans un lieu sûr. Chaque modification du mot de passe devra être tracée dans un registre tenu par l'Administration.

La longueur et la complexité des mots de passe doivent être adaptées à chaque composant. Ces exigences seront transmises durant la période préparatoire au titulaire.

Si la modification des mots de passe n'est pas réalisée et en se référant au BPU, le titulaire du marché de maintenance réalisera cette exigence.

6.7 NAS (Network Attached Storage)

Un NAS est un serveur de fichier connecté à un réseau informatique. Il permet de stocker, partager et sauvegarder des données de manière centralisée, accessibles depuis plusieurs appareils connectés au réseau.

Comme tous les éléments actifs du réseau, le NAS doit respecter les exigences suivantes :

- désactiver le compte Admin par défaut ;
- installer un anti-virus ;
- le pare-feu doit être activé ;
- désactiver toutes les règles de pare-feu non utilisées, laisser que les flux utiles (IP serveurs administration et VMs) ;
- activer le HTTPS ;
- activer la règle de redirection des flux http vers HTTPS ;
- changer les ports DSM (HTTP et HTTPS) par défaut ;
- désactiver TELNET ET SSH ;
- désactiver QUICKconnect ;
- activer la protection DDOS ;
- désactiver IP V6 ;
- mettre la synchronisation du temps (NTP) en cas d'absence d'un active-directory ;
- désactiver les ports Ethernet non utilisés ;
- désactiver les ports USB ;
- privilégier les comptes nominatifs et à faibles privilèges ;
- les droits utilisateurs doivent être limités au strict nécessaire ;
- créer un compte Administrateur nommé RSSI-A ;
- mettre en place une politique de mots de passe :
 - o 9 caractères minimum ;
 - o 14 pour les comptes d'administration ;
 - o Utilisation de 3 types de caractères différents sur les 4 possibles (Majuscule, minuscule, chiffre et caractères spéciaux).
- créer un utilisateur dédié pour tout partage SMB ;
- activer la journalisation des événements ;
- désinstaller toutes les applications et fonctions non essentielles ;
- utiliser les sauvegardes immuables (à partir de la version DSM 7.2) ;
- mettre en place une sauvegarde régulière, stockée sur un équipement déconnecté et dédié au système ;
- pour tout nouveau système, mettre à jour l'OS avant sa mise en production.

Dans le cadre d'une opération de maintenance, en présence de ce type de matériel et dont la sécurisation n'a pas été effectuée, le prestataire palliera à ce manque en appliquant ces exigences et en se référant au BPU.

6.8 Nommage des équipements dans les systèmes

La règle de nommage est la suivante :

Nom de l'Équipement = CI " _ " Site " _ " Métier " - " TypeEqpt " - " TypeMachine " - " Num "

6.8.1 Détail de l'élément <CI>

Mention de protection de l'équipement dont les valeurs possibles sont :

- NP ;
- NP-INT ;
- DR ;
- DR-SF ;
- S ;
- S-SF.

6.8.2 Détail de l'élément <Site>

Composé de 3 caractères alphanumérique, cet élément représente le site sur lequel est installé l'équipement.

Exemples :

PAB : PAU - BERNADOTTE

CGC : COGNAC

LRB : LA ROCHELLE – BEAUREGARD

L'élément sera à demander au bureau cyber.

6.8.3 Détail de l'élément <Métier>

Composé de 2 à 3 caractères alphanumérique, cet élément représente le métier associé à l'équipement.

Exemples :

GT : Gestion technique

GF : Gestion des Fluides

M : Manutention

L'élément sera à demander au bureau cyber.

6.8.4 Détail de l'élément <TypeEqpt>

Composé de 2 à 4 caractères alphanumérique, cet élément permet de connaître rapidement le type d'équipement et sa fonction dans le système

Le tableau ci-dessous définit la valeur du type (2^{ème} colonne).

Equipement	TYPE	
Equipements réseaux		
Borne Wi-Fi	WIF	
Borne Radio	RAD	Radios et autres protocoles sans fil (LoRa, ZigBee, etc.)
Borne lumineuse	LUX	Borne Li-Fi, infrarouge, etc.
Borne 3-4-5-6G	BxG	B4G, B5G
Concentrateur HUB ⁵	HUB	déprécié
Commutateur de niveau 2	SWI	Y compris les boîtiers de type RED BOX, Modbus, etc.
Commutateur de niveau 3	SWR	
Modem	MOD	
Routeur	RTE	
Equipements de sécurité réseaux		
Chiffreur	CHI	Y compris SAM
Firewall	FWL	
Boîtier TAP	TAP	
Sonde	SND	
Diode	DIO	
Equipements industriels		
Automate	PLC	Y compris UTL
IO déporté	IOD	
Capteur/Actionneur numérique	CAR	y compris les caméras, variateurs de vitesse, etc.
Equipements d'exploitation		
IHM	HMI	Locale au plus près de l'automate (en général positionnée sur l'armoire de l'installation)
Gestion technique	GTx	Y compris les SCADA
Admin système et/ou sécurité de la GTx	ADMS	Supervise et administre le système ou la sécurité du système. Ne contrôle pas la partie métier (niveau GTx)
Analyse industrielle	ALY	
Historian	HIS	
GMAO	GMAO	
Equipements de protection énergie		
Onduleur	POW	Onduleur pour le système, protège par exemple la GTx
Equipements de services système		
Stockage de données (Bdd, SAN,NAS,...)	SDD	
Serveur de nom de domaine	DNS	
Serveur de fichiers	FS	
Serveur impression	IMP	
Serveur identité (AD)	IAM	
Service web	WEB	

⁵ Ce type d'équipement n'est plus autorisé. Cependant, il se peut qu'il existe encore sur d'anciennes installations. Il est donc important de l'identifier pour traiter l'obsolescence.

Equipement	TYPE	
Services multiples	MLT	
Historisation	LOG	
Gestion du temps	NTP	
Sauvegarde	BKP	
Equipements de services cyber		
Détection d'intrusion	XDR	
Autre service de sécurité (Proxy, rev,...)	ASS	
Antivirus	AVIR	
Mise à jour (MCS)	MAJ	
Intégrité logiciel	FIM	
Analyse de comportement	SIEM	
Equipements de maintenance		
Maintenance	MNT	Y compris station d'ingénierie
Autres équipements		
Autre	AUT	

6.8.5 Détail de l'élément <TypeMachine>

TypeMachine = (<Os>"P") ou (<Os>"V"<TypeHyper>)

; type de machine et dominante du système d'exploitation de l'équipement

Elément <OS>

Composé d'un caractère alphanumérique, cet élément permet de connaître rapidement le système d'exploitation présent sur l'équipement

Equipement	TYPE
Equipements de maintenance	
UNIX	U
ANDROID	A
iOS	I
LINUX	L
WINDOWS	W
MAC OS	M
Equipements d'automatisme	
FIRMWARE AUTOMATE	F
Equipements réseau	
OS EQUIPEMENT RESEAU	R
Equipements de sécurité réseaux	
OS EQUIPEMENT SECURITE	S
Autres Equipements (ex : maintenance)	
AUTRE	Z

P=physique

V=virtuel

Elément < TypeHyper>

Composé d'un caractère alphanumérique, cet élément permet de connaître rapidement l'éditeur associé à la virtualisation

Equipement	TYPE
Broadcom ESx	V
KVM	K
Oracle VirtualBox	O
Red Hat Virtualization	R
AWS (Amazon Cloud)	A
Docker	D
Microsoft Hyper-V	V
PROXMOX	P
Citrix	C
Parallels (Mac OS)	M
Google (Cloud)	G
AUTRE	Z

6.8.6 Détail de l'élément <Num>

Composé de 3 chiffres, cet élément permet de connaître rapidement le contexte d'emploi de l'équipement

Contexte d'emploi	Plage de numéro
Environnement DEVELOPPEMENT	001-099
Environnement VALIDATION	100-199
Environnement INTEGRATION	200-299
Environnement FORMATION	300-399
Environnement SECOURS	400-499
Environnement PREPRODUCTION	500-599
Environnement PRODUCTION	600-999

6.8.7 Exemples

Le tableau ci-dessous présente des exemples de noms d'équipements.

Type de logiciel	Nom de la machine
Un automate TREND (Honeywell)	NP-INT_LBH_CVC-PLC-ZP-604 (Trend)
Une machine virtuelle sous Windows	NP-INT_LBH_CVC-IAM-WVV-501

Si le nommage n'est pas réalisé et en se référant au BPU, le titulaire du marché de maintenance réalisera cette exigence.

6.9 Ecran IHM

A l'identique d'un poste informatique, l'accès à un écran IHM est assujéti à un processus d'identification/authentification

Les règles à appliquer sont référencées dans le paragraphe des « **Politique des comptes et mots de passe** »

7 Exigences relatives aux systèmes d'exploitation, services et applications

7.1 Licences

Toutes les licences doivent être valides au moins pendant la durée du marché.

Le SID doit être nommé propriétaire des licences et détenir les numéros de licence.

En cas de détection d'anomalie et en se référant au BPU, des licences conformes à cette exigence seront mises en place.

7.2 Durcissement des systèmes d'exploitation

Les systèmes d'exploitation sont la base de tous les systèmes informatiques. Ils gèrent les ressources matérielles et logicielles des ordinateurs, assurent la communication entre les différents composants du système et fournissent un environnement d'exécution pour les applications. Cependant, ces systèmes présentent également des vulnérabilités qui peuvent être exploitées par des attaquants pour compromettre la sécurité du système dans son ensemble.

Pour cette raison, il est essentiel de prendre des mesures pour sécuriser et durcir les systèmes d'exploitation, tels que Microsoft Windows et Linux. Le durcissement consiste à éliminer ou à limiter les fonctionnalités inutiles ou dangereuses des systèmes d'exploitation, à configurer les paramètres de sécurité de manière appropriée et à installer les mises à jour de sécurité régulièrement.

En renforçant la sécurité des systèmes d'exploitation, il est possible de minimiser les risques de cyberattaques et de protéger les actifs numériques de l'entreprise ou du particulier. Cela permet également de garantir la confidentialité, l'intégrité et la disponibilité des données, qui sont essentielles pour la continuité des activités et la réputation de l'organisation.

Les mesures à appliquer sont :

- désactiver tous les services non utilisés ;
- désactiver le service du spooler d'impression ;
- désactiver le service Windows update ;
- activer le pare-feu Windows ;
- désactiver toutes les règles de pare-feu non utilisées, ne laisser que les flux utiles ;
- désactiver l'exécution automatique pour tous les médias et pour tous les comptes ;
- supprimer les tâches planifiées non utilisées par le système ;
- désinstaller toutes les applications non essentielles au système (jeux, Xbox, météo etc..) et pour tous les comptes ;
- installer un antivirus sur tous les postes et serveurs et le maintenir à jour ;
- désactiver les protocoles LLMNR, NetBIOS, Wins ;
- désactiver IP V6 ;
- mettre un mot de passe d'accès au BIOS pour interdire une modification du BIOS non autorisée (nommage donné par le bureau cyber) ;
- interdire la séquence de démarrage sur un autre média que la partition d'amorçage du disque dur ;
- mettre la synchronisation du temps (NTP) en cas d'absence d'un active-directory ;

- désactiver le wifi et/ou le Bluetooth via le BIOS si possible sinon dans le système d'exploitation ;
- désactiver les ports Ethernet non utilisés ;
- privilégier les comptes nominatifs et à faibles privilèges ;
- dans le cas de comptes fonctionnels, le RSSI-A s'assurera de la traçabilité des connexions (mise en place d'un cahier, PV d'intervention,..) ;
- créer un compte RSSI-A avec un profil administrateur pour ouvrir une session ;
- créer un compte RSSI-A avec un profil administrateur pour ouvrir une session sur le logiciel de supervision.
- limiter les droits utilisateurs au strict nécessaire ;
- mettre en place une politique de mots de passe :
 - o 9 caractères minimum ;
 - o 14 pour les comptes d'administration ;
 - o Utilisation de 3 types de caractères différents sur les 4 possibles (Majuscule, minuscule, chiffre et caractères spéciaux) ;
- mettre en place une politique USB en autorisant techniquement que les supports identifiés (principe de white list) ;
- mettre en place une sauvegarde régulière, stockée sur un équipement déconnecté et dédié au système ;
- pour tout nouveau système, mettre à jour l'OS et logiciel(s) métier(s) avant la réception ;
- tous les comptes accompagnés des mots de passe seront donnés au RSSI-A de l'USID ;
- Si la limitation d'accès à l'Internet ne peut pas intégrer les mises à jour (anti-virus et de sécurité), le maintenancier doit prévoir une procédure en mode hors connexion ;
- dans le cas de systèmes d'exploitation Microsoft, la version est Windows 10 pro ou entreprise au minimum avec la dernière version soutenue par Microsoft .

Dans le cadre d'une opération de maintenance, si ces mesures ne sont pas appliquées, le titulaire comblera ce manque en se référant au BPU.

7.3 Politique des comptes et mots de passe

L'accès au système d'exploitation, à un logiciel ou un réseau ne doit être possible qu'après un processus d'identification/authentification.

L'identification est le fait de donner son identité. Les comptes sont nominatifs lorsqu'ils sont associés à une personne spécifique, ou fonctionnels lorsqu'ils sont associés à une fonction ou à un rôle spécifique⁶.

L'authentification est le fait d'apporter la preuve de son identité par un secret (mot de passe par exemple) ou un élément physique (badge).

Un compte pour les applications métiers, et non pour l'administration des systèmes permet soit :

- la lecture, profil utilisateur ;
- des modifications techniques, on parle de profil technicien ;
- des modifications de programmation, on parle de profil administrateur.

⁶ La mise en place d'un compte fonctionnel sera autorisée par le bureau cyber et des mesures organisationnelles assureront la traçabilité de connexion.

La politique des mots de passe est la même que celle décrite dans le **Durcissement des systèmes d'exploitation**

Pour tous les S2I, un compte RSSI-A sera créé conformément au tableau ci-dessous avec le profil administrateur.

En fonction du S2I, la synthèse des accès pourra être illustrée de la manière suivante :

Matériels-Logiciels	PC				
Acteurs	Supervision Session Windows	BOX Internet	PC maintenance Session Windows	Logiciel supervision	Automate IHM
USID	Compte nominatif Profil utilisateur		Compte fonctionnel Profil utilisateur	Compte nominatif Profil administrateur	Compte fonctionnel Profil utilisateur Compte fonctionnel Profil technicien
RSSI-A	Compte fonctionnel Profil administrateur	Compte fonctionnel Profil administrateur	Compte fonctionnel Profil administrateur		Compte fonctionnel Profil administrateur
Maintenancier		Compte fonctionnel Profil administrateur	Compte fonctionnel Profil administrateur	Compte fonctionnel Profil utilisateur	Compte fonctionnel Profil administrateur

Le titulaire s'assure que tous les comptes (accès Windows et autres...) des intervenants dans le cadre de la prestation sont habilités selon le principe du moindre privilège

En l'absence de mots de passe conformes à cette exigence, le titulaire y répondra en se référant au BPU.

7.4 Exigences relatives aux annuaires

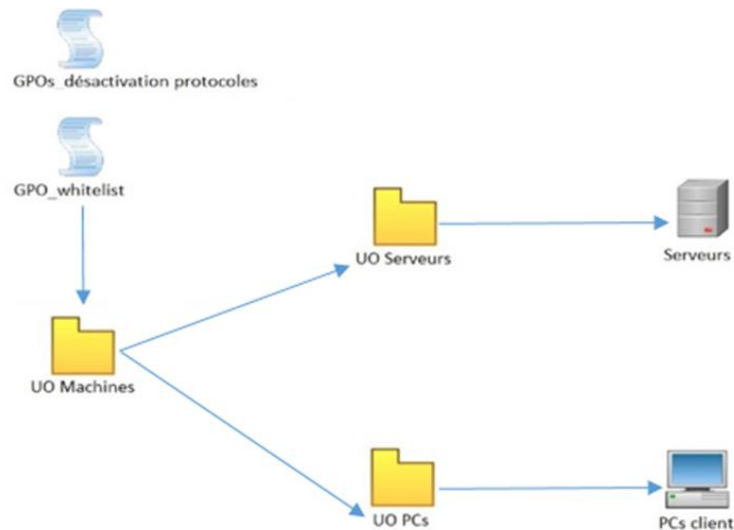
L'annuaire est une base de données centrale qui stocke des informations sur les utilisateurs, les ressources et les services. Il permet aux utilisateurs d'accéder aux ressources dont ils ont besoin pour travailler efficacement. Si l'annuaire n'est pas correctement sécurisé, il peut devenir une cible attrayante pour les attaquants qui cherchent à accéder à des informations sensibles ou à perturber les opérations de l'entreprise.

Les mesures à mettre en place sont :

- installer le service d'annuaire Active Directory (AD) sur un serveur dédié sans aucun autre logiciels métier ou service ;
- appliquer les mesures pour les postes et serveurs du SID définies ;
- limiter aux seuls administrateurs du domaine la connexion (en direct ou via le bureau à distance).

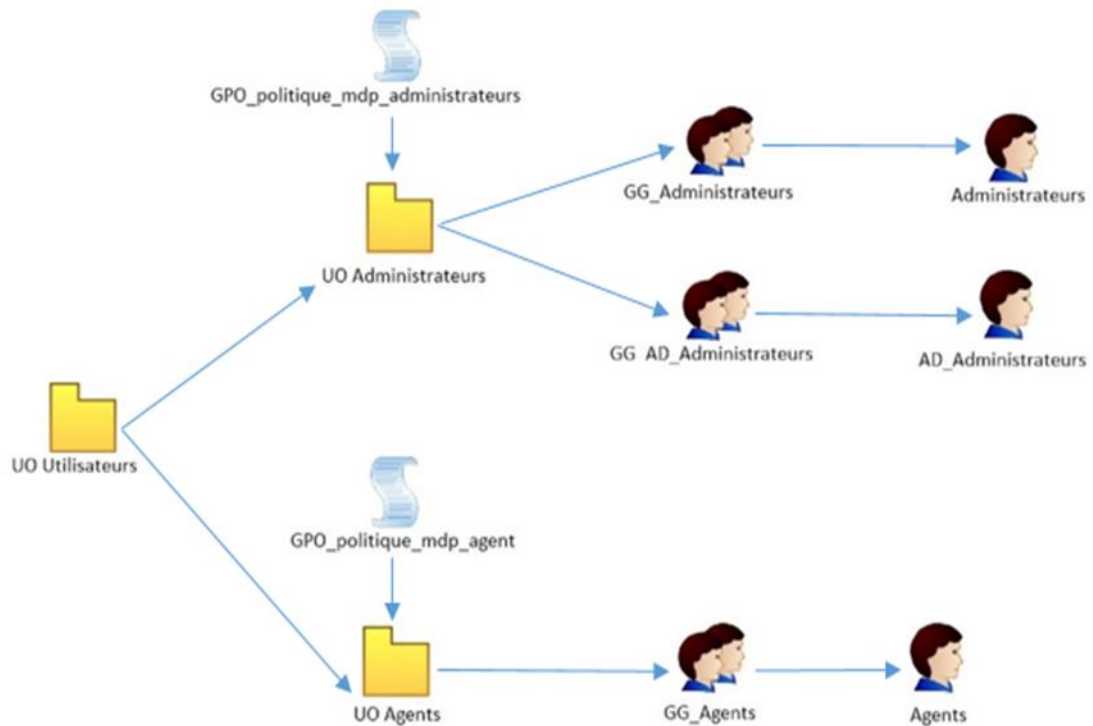
- limiter aux postes d'administration l'accès à distance ;
- proscrire les mots de passe en clair dans les partages par défauts « Netlogon » et « Sysvol » ;
- proscrire la modification de la stratégie de domaine par défaut et de la stratégie du contrôleur de domaine par défaut lors de la création des GPO⁷ sur un Active Directory.
- désactiver les protocoles NTLM, NetBIOS, LLMNR dans votre infrastructure ;
- les objets machines, groupes et utilisateurs seront créés selon les schémas ci-dessous.

Le schéma ci-dessous représente l'architecture des machines dans l'active-directory



Le schéma ci-dessous représente l'architecture des comptes et groupes utilisateurs dans l'active-directory

⁷ Group Policy Objects ou stratégie de groupe



Si l'annuaire n'est pas installé et en se référant au BPU, le titulaire du marché de maintenance réalisera cette exigence.

NB : Toutes les mesures de sécurisation pourront être réalisées via GPO, si elles le permettent.

7.5 Configuration de l'anti-virus

La mise en place de mesures de configuration d'un antivirus est essentielle pour assurer une protection efficace contre les menaces informatiques telles que les virus, les vers, les chevaux de Troie et les ransomwares.

Les paramétrages suivants sont à respecter pour les agents antivirus déployés :

- analyser tous les fichiers scannables⁸ ;
- programmer la planification de l'analyse hebdomadairement ; de préférence tous les dimanches à 12h ;
- configurer le niveau d'utilisation de l'UC à moyen, de manière à ne pas gêner l'utilisation du système ;
- analyser les fichiers compressés sur 3 couches ;
- analyser la zone d'amorçage ;
- activer l'IntelliTrap ou un outil similaire s'il existe ;
- activer l'antispyware/grayware ;
- exclure de l'analyse les répertoires d'installation de l'antivirus ;
- configurer les actions à réaliser dans le cadre d'une détection de programmes malveillants :
 - 1ère action : Nettoyer ;
 - 2ème action : Quarantaine ;
 - 3ème action : Supprimer ;

⁸ Option dans l'anti-virus.

- exclure les flux vidéos et les enregistrement vidéos de l'analyse en temps réel pour les serveurs vidéos.

Dans le cadre d'un marché de maintenance, le titulaire du marché, en se référant au BPU, appliquera cette exigence concernant l'antivirus :

- mise en place d'un antivirus si nécessaire en concertation avec le bureau cyber ;
- application de paramètres.

8 Pénalités

En fonction du SI déployé, le titulaire se doit de respecter les directives et les guides référents à la cybersécurité au sein du ministère. Tenu également de fournir dans le temps imparti les documents nécessaires à un maintien de sécurisation optimale, il peut se voir appliquer différents types de pénalités décrites dans le CCAP

9 Glossaire

ACID	Automate de Chiffrement des Informations de la Défense ACID est une solution logicielle cryptographique qui offre des services de chiffrement, de déchiffrement et de signature cryptographique. Elle permet de protéger des données sensibles
AH	Autorité d'Homologation Personne physique qui, après instruction du dossier d'homologation, prononce l'homologation de sécurité du SI, c'est-à-dire prend la décision d'accepter les risques résiduels identifiés sur le système. Elle est désignée à un niveau hiérarchique suffisant pour assumer les responsabilités qui lui incombent.
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information Elle décide des mesures que l'État met en œuvre pour répondre aux crises affectant ou menaçant la SSI des autorités publiques et des opérateurs d'importance vitale. Elle coordonne l'action gouvernementale en la matière
API	Automate Programmable Industriel Élément constitutif d'un système industriel Traduction anglaise : Programmable Logic Controller
BPU	Bordereau des prix unitaires
CCAP	Cahier des Clauses Administratives Particulières Document contractuel qui décrit les conditions administratives particulières d'exécution des marchés, notamment les conditions administratives et financières (avances, acomptes, conditions de livraison, pénalités, etc.).
CCTP	Cahier des Clauses Techniques Particulières Document contractuel qui décrit les conditions techniques particulières d'exécution des marchés, sous forme d'exigences minimales (approche fonctionnelle) ou de spécifications fonctionnelles techniques.
CPE	Common platform enumeration Système de nomenclature pour identifier les logiciels, les produits et les systèmes d'exploitation
CSSI	Correspondant SSI Lorsqu'il n'est pas possible, ou pas nécessaire, d'affecter un OSSI à temps plein, un correspondant SSI (CSSI) est désigné auprès du chef d'entité
Cyberdéfense	La cyberdéfense recouvre l'ensemble des activités permettant d'intervenir, militairement ou non, face à un événement cybernétique au travers de la posture permanente de détection et de réaction aux attaques et de la gestion de crise cybernétique.
Cybersécurité	État recherché pour un système d'information lui permettant de résister à des événements issus du cyberspace susceptible de compromettre la disponibilité, l'intégrité ou la confidentialité des données. La cybersécurité fait appel à la cyberprotection et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.
DR	Diffusion Restreinte Mention de protection pour des données sensibles
EAR	Élément actif de réseau Le cœur d'un réseau informatique est constitué d'éléments dits « actifs », comme les routeurs, les commutateurs et les switch.
IP	Internet Protocol Protocole de communication

MCS	Maintien en condition de sécurité Ensemble des mesures de nature organisationnelle et technique concourant à maintenir, tout au long de leur cycle de vie, le niveau de SSI accepté lors de son homologation de sécurité au travers d'une gestion maîtrisée et pérenne des risques. Le MCS a ainsi pour objectif de maintenir la validité de l'homologation.
MOOC	Massive Open Online Course Un MOOC est un cours en ligne ouvert et massif, accessible à tous et généralement gratuit. Il s'agit d'une formation en ligne qui permet aux apprenants de suivre des cours dispensés par des universités, des institutions académiques ou des experts dans un domaine spécifique.
NAS	Network Attached Storage Un NAS est un serveur de fichiers conçu pour être connecté à un réseau informatique et permettre le stockage, la sauvegarde et le partage de données entre plusieurs utilisateurs et appareils.
NIST	National Institute of Standards and Technology Agence fédérale américaine qui gère entre autres les CPE
OSSI	Officier de SSI OSSI est un terme général pour désigner un spécialiste SSI, employé à temps plein auprès d'une autorité (Représentant AQSSI, AH, chef d'organisme ou d'entité, etc.) pour le conseiller et l'aider à mettre en œuvre les processus opérationnels et supports qui lui incombent.
PAS	Plan d'assurance sécurité Document contractuel qui précise les dispositions prises par un futur prestataire pour répondre aux exigences de sécurité du donneur d'ordre pendant toute la durée du contrat, et cela dans le cadre de l'infogérance.
PDS	Plan de sécurité Document qui décrit les mesures qui répondent aux exigences de sécurité définies soit dans une FEROS, soit à l'issue d'une analyse de risques.
PES	Procédures d'exploitation de sécurité Document exposant les mesures de sécurité permettant de répondre aux objectifs de sécurité fixés par l'AH. Elles présentent les droits et les devoirs des accédants au système ainsi que les actions à réaliser dans le cadre de l'utilisation quotidienne du système.
RSSI	Responsable de Sécurité des Systèmes d'Information Un RSSI est, pour un SI donné, chargé de : - s'assurer de l'intégration de la SSI dans le SI à toutes les phases ; - s'assurer du MCS du SI ; - conduit la démarche d'homologation ainsi que des renouvellements d'homologation ; - conseiller les autorités d'homologation et d'emploi, recommander et proposer des règles spécifiques au SI et à son contexte d'utilisation ; - faire le lien avec la chaîne « défensive » ; - garantir la cohérence des mécanismes de sécurité, des procédures de sécurité et des conditions d'emploi du SI ; - informer les service utilisateurs des différentes mesures de protection physiques préalables à l'installation du SI.
RSSI-A	RSSI aval Désigné par l'autorité d'emploi pour assurer le suivi SSI du système en service (dont le MCS), jusqu'à son retrait, il est chargé d'instruire les renouvellements d'homologation.

RSSI-P	<p>RSSI projet</p> <p>Il pilote la démarche d'intégration de la SSI durant la phase projet ou programme incluant la phase de qualification, jusqu'à l'homologation initiale incluse</p>
SF	<p>Spécial France</p> <p>Mention complémentaire visant à restreindre la divulgation d'une information ou d'un support aux seuls ressortissants français. Une information ou un support portant cette mention ne peut être communiqué, en tout ou partie, à un État étranger ou à l'un de ses ressortissants, organisation internationale ou personne morale de droit étranger, même s'il existe un accord de sécurité, général ou spécifique, entre la France et l'État ou l'organisation internationale considérée.</p>
SI	<p>Système d'information</p> <p>Ensemble de moyens informatiques ayant pour finalité d'élaborer, de traiter, d'acheminer, de présenter ou de détruire de l'information, mais aussi d'un environnement organisationnel (incluant les procédures) et des informations qu'il traite</p>
SSI	<p>Sécurité des systèmes d'information</p> <p>Ensemble des actions techniques ou non techniques menées par le ministère visant à atteindre et maintenir l'état de cybersécurité des SI, i.e. l'état leur permettant de résister à des événements issus du cyberspace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. Elle est organisée autour de trois piliers : cyberprotection, cyberdéfense et résilience.</p>
S2I	<p>Système industriel d'infrastructure</p> <p>Un système industriel d'infrastructure est un système d'information particulier ayant pour finalité de contrôler ou de commander des installations ou équipements techniques, composés d'un ensemble de capteurs et/ou d'actionneurs. Il permet ainsi une interaction entre le monde numérique et le monde réel.</p>

Attestation de prise de connaissance de l'IM 2004

ETAT CIVIL ET EMPLOI :

Nom et prénoms :

Grade et emploi :

Service employeur :

Prise en compte de l'équipement –

Je, soussigné(e) Déclare :

- avoir pris connaissance de l'IM 2004 relative à la fonction d'administrateur de systèmes d'information et de communication au sein du ministère de la Défense du 14 décembre 2009 ;
- m'engage à respecter les termes de l'IM 2004.

à, le
(nom et signature de l'administrateur)

à, le
(nom, fonction et signature)
Atteste que l'intéressé(e) a été informé(e) de ses responsabilités
à l'égard de la fonction administrateur

INFORMATIONS

L'administrateur d'un système industriel d'infrastructure relevant du périmètre du SID Sud-Ouest doit prendre connaissance de l'IM 2004 et s'engager à la respecter. Il saisit son nom, son prénom, son emploi ou fonction, et l'entreprise qui l'emploie. L'attestation est imprimée recto-verso. Le RSSI-A du système atteste que l'administrateur a été informé de ses devoirs et conserve cette attestation comme preuve.

L'instruction ministérielle N° 2004/DEF/DGSIC relative à la fonction d'administrateur de systèmes d'information et de communication au sein du ministère de la défense est disponible sur le site de Légifrance.

<https://www.legifrance.gouv.fr/download/pdf/circ?id=30268>

Les règles principales concernant les devoirs de l'administrateur sont les suivantes.

✓ L'administrateur doit appliquer les politiques d'exploitation de sécurité (PES) attachées aux systèmes dont il a la charge de la mise en œuvre et rendre compte au RSSI-A de toute difficulté d'application.

Il est notamment interdit de modifier l'architecture du système, de l'interconnecter à un autre réseau (ex : internet) ou de modifier l'attribution des droits sans avoir eu l'accord du RSSI-A au préalable.

✓ Il est interdit à l'administrateur de faire usage de ces droits à d'autres fins que celle de sa mission.

✓ L'administrateur doit toujours agir dans le seul intérêt du maintien en condition opérationnelle - et en particulier du niveau de sécurité - du système géré et dans le strict respect de la confidentialité des informations qu'il est amené à connaître.

✓ L'administrateur a obligation de discrétion professionnelle pour protéger les informations de l'administration dont la divulgation pourrait nuire au bon fonctionnement de ses tâches.

✓ Dans le cas d'un système de vidéosurveillance, si un administrateur venait exceptionnellement à prendre connaissance du contenu des enregistrements d'images ou de conversation pour des motifs légitimes de maintien en condition de sécurité du système, il lui est interdit de divulguer les informations qu'il aurait été ainsi amené à connaître.

✓ L'administrateur peut constater des dysfonctionnements ou des incidents de sécurité touchant le système. Il doit faire cesser l'incident et en informe sans délai le RSSI-A. Avec son accord, il doit recouvrer le niveau de sécurité nominal et assurer la continuité du service en mode dégradé.

✓ Si l'administrateur découvre des crimes et délits, ils doivent être rapportés sans délais au RSSI-A qui contactera la gendarmerie ou les services de police.

Attestation Cybersécurité PC de maintenance

Ce certificat est obligatoire pour toute intervention sur un équipement du Ministère. L'intervenant doit pouvoir le présenter à tout instant. Il doit donc accompagner le PC.

Marché

Nom du marché : _____
 Numéro du marché : _____
 Nom de l'entreprise : _____

POC cyber entreprise

Nom Prénom : _____
 Téléphone : _____
 @mail : _____

Détenteur

Nom Prénom : _____
 Téléphone : _____
 @mail : _____
 Entreprise/unité : _____

Caractéristique du PC

Marque : _____
 Modèle : _____
 Num. de série : _____
 Adresse MAC : _____
 BIOS (Num. de version) : _____

Système d'exploitation

Nom OS : _____
 Version OS : _____
 Date MAJ : _____

Logiciels métiers

Nom	Version	Date MAJ
_____	_____	_____
_____	_____	_____
_____	_____	_____

Antivirus

Nom : _____
 Version moteur : _____
 Version signatures : _____
 Date MAJ Moteur : _____
 Date MAJ signatures : _____

Systèmes indus concernés

Nom

Nature des contrôles

Vérification de l'OS (MAJ) : _____
 Vérification de l'AV (MAJ) : _____
 Durcissement du PC (logiciels inutiles, BIOS...): _____
 Chiffrement du disque (CRYHOD/BitLocker) : _____
 Vérification des logiciels métiers (MAJ) : _____
 Scan antivirus complet : _____
 Sensibilisation par le RSSI-P ou A: _____
 Signature IM2004 : _____

Signature responsable

Date :

Cachet,
Signature :

Commentaires

