

 <p>Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE</p> <p>Premier ministre</p> <p>DIRECTION DE L'INFORMATION LÉGALE ET ADMINISTRATIVE</p>	<h2>Recueil des mesures de sécurité applicables au réseau industriel DILA</h2>	
<p><b>Date</b></p> <p>24/06/2016</p>	<p style="text-align: center;"><b>Statut</b></p> <div style="display: flex; justify-content: space-around;"> <span><input type="checkbox"/> Provisoire</span> <span><input checked="" type="checkbox"/> Validé</span> </div>	

Rédacteurs			
Nom	Fonction	Nom	Fonction
Lemainais	RSSI		
Valideur			
Nom	Fonction	Nom	Fonction

## 1. Introduction

Conformément à la circulaire du Premier ministre du 17 juillet 2014, tout système d'information DILA est soumis aux exigences de sécurité de la PSSIE ([http://www.ssi.gouv.fr/uploads/IMG/pdf/pssie\\_anssi.pdf](http://www.ssi.gouv.fr/uploads/IMG/pdf/pssie_anssi.pdf)).

Ce recueil a pour objectif de mettre en avant les principales exigences de sécurité (cf. Annexe 1) adaptées au contexte et au périmètre du réseau industriel<sup>1</sup> de la DILA. Ces éléments sont également à rapprocher de l'analyse des risques conduite sur ce même périmètre.

## 2. Exigences générales

Les principales règles de la PSSIE applicables au contexte du réseau industriel sont reprises en Annexe I. En particulier, la PSSIE demande d'utiliser, lorsqu'ils existent, des produits certifiés (<http://www.ssi.gouv.fr/entreprise/produits-certifies/produits-certifies-cspn/>) ou qualifiés (<http://www.ssi.gouv.fr/entreprise/qualifications/produits-qualifies-par-lanssi/les-produits/>).

Ces choix permettent d'être conforme de fait, avec les exigences de la PSSIE pour ce type de matériel ou logiciel.

<sup>1</sup> Ce recueil est donc applicable aux systèmes (serveur, machine, etc.) installés dans les plages d'adresse du réseau industriel DILA.

### 3. Cartographie

Le système est cartographié sur la base des documents suivants :

- Architecture matérielle et logicielle avec les versions des composants ;
- Topologie du réseau ;
- Matrice des flux ;
- Comptes (système, de service, de session ou applicatif), et procédures de changement de mot de passe associées ;
- Dossier des procédures d'exploitation et d'administration.

### 4. Gestion des correctifs de sécurité

Les contraintes ou limites en termes de maintien en conditions de sécurité doivent être identifiées et formalisées :

- Application ou non des correctifs de sécurité sur les systèmes et les composants applicatifs;
- Compatibilité ou non avec des solutions anti-virales.

Le fournisseur de la solution assure une veille sécurité sur ces matériels et logiciels. La DILA est destinataire de cette veille.

L'obsolescence des matériels et logiciels est traitée par cette fonction de veille et permet d'anticiper le remplacement des ressources concernées.

En cas d'obsolescence des logiciels, d'impossibilité d'appliquer des correctifs de sécurité ou autres protections antivirales, les systèmes doivent être durcis avec par exemple des solutions de scellements de l'OS.

### 5. Contrôle d'accès logique

#### 5.1. Politique des mots de passe

Les règles attachées aux mots de passe sont exprimées ci-dessous :

- Les mots de passe par défaut sont changés avant la mise en production ;
- Les mots de passe sont changés périodiquement ;
- Les mots de passe doivent être à minima sur 8 caractères (majuscules, minuscules, chiffres, caractères spéciaux)
- Des moyens de protection (temporisation vs blocage) ou d'alerte sont mis en place vis-à-vis des attaques par force brute des comptes à privilège (administrateur technique ou fonctionnel)
- Les mots de passe sont conservés de manière à assurer leur confidentialité et leur intégrité. Pour information la DILA utilise sur les postes Windows le logiciel libre Keepass qui est certifié par l'ANSSI ;
- Les procédures de réinitialisation ou de recouvrement de mot de passe sont formalisées ;
- Les flux réseau véhiculant les mots de passe sont chiffrés (exemple : https)

## 5.2. Gestion des comptes

Les règles attachées aux comptes sont exprimées ci-dessous :

- Les exigences de gestion des comptes s'appliquent à tous les utilisateurs ou administrateur titulaires de compte sur le système ;
- Les comptes sont nominatifs sauf exception dûment justifiée ;
- Une procédure de gestion des comptes doit intégrer le traitement des départs et des arrivées. Cette procédure formalise la création et la fermeture de comptes nominatifs. En cas d'utilisation incontournable de comptes génériques, les mots de passe sont changés en conséquence ;
- Les comptes sont ouverts selon le principe du moindre privilège ;
- Les comptes de service sont recensés et la procédure de mise à jour du mot de passe formalisée ;
- Une revue régulière des intervenants et de leurs comptes doit être effectuée, au minimum une fois par an. Cette revue s'appuie sur la production d'un état récapitulatif des habilitations en cours.

## 6. Contrôle d'accès physique

L'accès physique aux systèmes (ressources des VLAN du réseau industriel) est protégé et accessible qu'aux personnes habilitées (locaux, armoires fermés, etc.). La politique DILA d'accès aux locaux est applicable.

## 7. Maîtrise des configurations

La maîtrise des configurations assure à minima :

- La capacité à mettre en œuvre des mécanismes de scellement des OS, en cas de besoin fort de sécurité sur un système ;
- Le test périodique des sauvegardes et procédures de restauration. En particulier, avant la mise en production ;
- La sauvegarde des environnements après chaque changement de configuration ;
- La politique de sauvegarde est adaptée au système cible ;
- Les opérations de paramétrage ou modification du système sont authentifiées et traçables ;
- Seuls les services indispensables sont activés (exemple : service Apache)
- Seuls les logiciels et composants nécessaires sont installés sur le système (absence de compilateur, etc.)
- L'intégrité et l'authenticité des logiciels installés sont vérifiées ou garantie de source sûre ;
- En cas de nécessité et d'utilisation de média amovibles (clé USB, disques, etc.), ces média doivent être vérifiés en termes contre les codes malveillants. Il est recommandé d'utiliser des supports dédiés au réseau industriel ;
- Les comptes par défaut inutiles sont désactiver ou supprimer. Les mots de passe par défaut des comptes actifs sont personnalisés conformément à la politique ;
- Les ports USB ou autres interfaces Ethernet non utilisés sont désactivés ;
- L'usage de protocole non sécurisé (telnet, etc.) est proscrit ;
- L'usage de technologies sans fil autonome sur ce type d'équipement est proscrit.

## 8. Supervision

Les systèmes sont supervisés à minima sur le besoin de disponibilité.

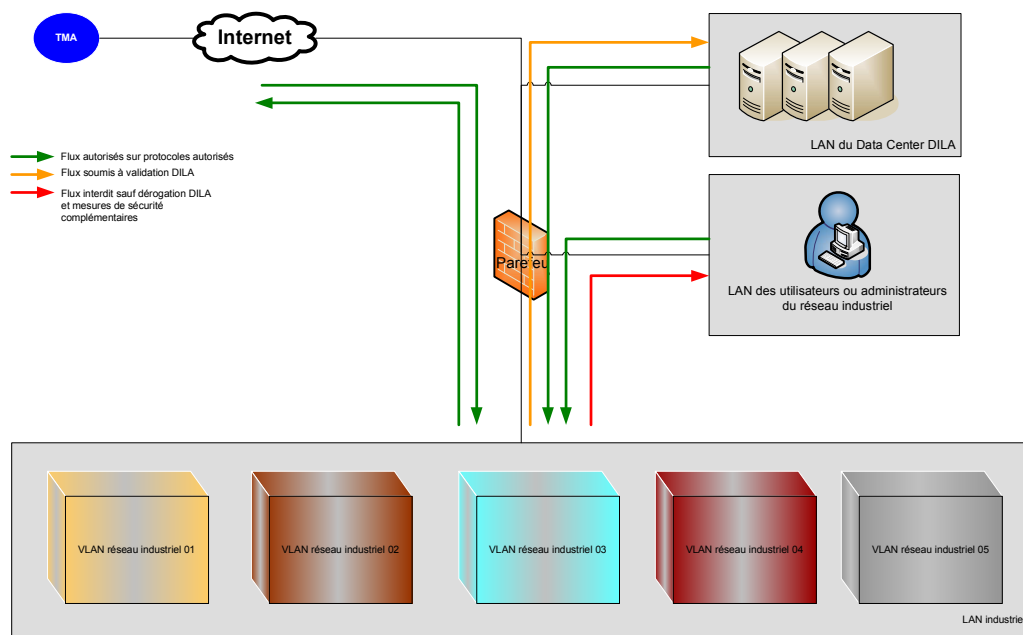
## 9. Cloisonnement

Le système industriel DILA est cloisonné physiquement des autres SI DILA. Ce cloisonnement est assuré par un pare-feu labellisé par l'ANSSI. Les flux entre les deux environnements sont limités au strict minimum. Le cloisonnement logique est mis en œuvre sur la base de VLAN en s'appuyant sur des équipements CISCO. L'attribution des plages d'adresses IP est sous le contrôle exclusif de la DILA.

Les règles applicables sont :

- Les flux sont refusés par défaut. Les flux nécessaires au fonctionnement du système industriel doivent s'appuyer sur des protocoles sécurisés (https, sftp, etc.)
- Les flux sortants du réseau industriel vers l'Internet sont filtrés par un proxy et autorisés que sur liste blanche (IP ou mécanisme d'authentification). Le système industriel doit être compatible avec ce mode de fonctionnement ;
- Les flux entrant d'Internet sur le réseau industriel sont limités aux opérations de télémaintenance ;
- Il est recommandé de cloisonner logiquement ou physiquement les flux d'administration du système (ssh, etc.) vis-à-vis des flux de production ;
- Il est recommandé que les postes d'administration dont ceux en télémaintenance ne soient pas connectés à Internet (hors sessions sécurisée VPN). A minima, pendant les opérations d'administration ;
- Les flux rejetés sont journalisés et analysables ;
- Tous les flux entrants ou sortants du système industriel doivent être journalisés. La période de rétention des données est précisée ;
- Il est recommandé de renforcer le contrôles des échanges sur la base d'identifiants source et destination lorsque nécessaire. Exemple : filtrage sur les adresses MAC dans le cas où un VLAN « DataCenter » est étendu sur une zone utilisateur sans contrôle d'accès physique aux locaux.

Le système industriel DILA est organisé en zones fonctionnelles ou techniques cohérentes. Ces zones sont cloisonnées entre elles, selon le **schéma suivant** :



## 10. Gestion des interventions tierces

Une procédure de gestion des interventions est mise en place. Toute intervention est validée par la DILA. Au cas où l'intervenant apporte ses propres outils (des outils de diagnostic, etc.), une procédure, même succincte, est mise en place pour vérifier que les équipements de l'intervenant ont un niveau de sécurité satisfaisant (correctifs de sécurité à jour, anti-virus actif et à jour).

Les prestataires intervenant sur les SI DILA sont sensibilisés à la cyber sécurité par leur organisme d'appartenance.

Les données confidentielles (exemple : dossier d'architecture technique) échangée entre la DILA et son prestataire doivent être chiffrées avec le logiciel Zed !.

## 11. Télémaintenance

La confidentialité, l'intégrité et l'authenticité des communications des systèmes distants sont assurés **en priorité** par la mise en œuvre de tunnel IPSEC ou VPN SSL avec authentification forte des intervenants. Ces opérations sont conduites à partir d'un poste de rebond hébergé à la DILA. Ce poste est localisé dans le sous-réseau concerné.

Les autres solutions sont soumises à une validation DILA. Exemples :

- Ouverture ponctuelle du flux sur un appel téléphonique du fournisseur ou principe du call-back ;
- Utilisation d'un intermédiaire type TeamViewer.

En toute situation :

- Les flux de télémaintenance sont gérés par un ou plusieurs pare-feu dont au moins un est labellisé par l'ANSSI ;
- Les opérations de télémaintenance sont tracées ;
- Les flux ouverts sont temporisés (time-out) et fermés en fin d'opération.

## ANNEXE I – LISTE DES DISPOSITION PSSIE APPLICABLES

Chacune des dispositions a été formalisée de manière à s'adapter au fonctionnement de la DILA. **Il convient donc d'en faire une lecture transposée au système d'information objet de ce marché.** A cette fin les mots clés ont été ci-dessous mis en évidence.

### 1. Gestion de biens

**GDB-INVENT** : **inventaire des ressources informatiques**. Chaque entité établit et maintient à jour un inventaire des ressources informatiques sous sa responsabilité, en s'appuyant sur un outillage adapté. Cet inventaire est tenu à disposition du RSSI, ainsi que du FSSI et de l'ANSSI en cas de besoin de coordination opérationnelle. Il comprend la liste des « briques » matérielles et logicielles utilisées, ainsi que leurs versions exactes. Il est constitué d'une base de données de configuration, maintenue à jour et tenue à disposition du RSSI.

*L'historique des attributions des biens inventoriés doit être conservé, dans le respect de la législation.*

**GDB-CARTO** : **cartographie**. La cartographie précise les centres informatiques, les architectures des réseaux (sur lesquelles sont identifiés les points névralgiques et la sensibilité des informations manipulées) et qualifie le niveau de sécurité attendu. Cette cartographie est maintenue à jour et tenue à disposition du RSSI, ainsi que du FSSI et de l'ANSSI en cas de besoin de coordination opérationnelle.

**GDB-QUALIF-SENSI** : **qualification des informations**. La sensibilité de toute information doit être évaluée. Le marquage systématique des documents, en fonction du niveau de sensibilité, est fortement recommandé.

**GDB-PROT-IS** : **protection des informations**. L'utilisateur doit protéger les informations qu'il est amené à manipuler dans le cadre de ses fonctions, selon leur sensibilité et tout au long de leur cycle de vie, depuis la création du brouillon jusqu'à son éventuelle destruction

### 2. Produits et services labellisés

**INT-AQ-PSL** : **acquisition de produits et services de confiance**. Lorsqu'ils sont disponibles, des produits ou des services de sécurité labellisés (certifiés, qualifiés) par l'ANSSI doivent être utilisés.

### 3. Sécurité des réseaux

**RES-MAITRISE** : **systèmes autorisés sur le réseau**. Seuls les équipements gérés et configurés par les **équipes informatiques habilitées** peuvent être connectés au réseau local d'une entité.

**RES-INTERCO** : **interconnexion avec des réseaux externes**. Toute interconnexion entre les réseaux locaux d'une entité et un réseau externe (réseau d'un tiers, Internet, etc.) doit être réalisée via les infrastructures nationales. Le terme infrastructure nationale adresse le réseau interministériel de l'état (RIE)

**RES-ENTSOR** : **mettre en place un filtrage réseau pour les flux sortants et entrants**. Dans l'optique de réduire les possibilités offertes à un attaquant, les connexions des machines du réseau interne vers l'extérieur doivent être filtrées.

**RES-PROT** : **protection des informations**. Les accès à Internet passent obligatoirement à travers les passerelles nationales. Dès lors que des informations sensibles doivent transiter sur des réseaux non maîtrisés, il convient de les protéger spécifiquement par chiffrement adapté.

Le terme passerelles nationales adresse celles du réseau interministériel de l'état (RIE)

#### 4. Sécurité des mécanismes de commutation et routage

RES-COUCHBAS : implanter des mécanismes de protection contre les attaques sur les couches basses. Une attention particulière doit être apportée à l'implantation des protocoles de couches basses, de façon à se prémunir des attaques usuelles par saturation ou empoisonnement de cache. Cela concerne, par exemple, le protocole ARP.

RES-ROUTDYN : surveiller les annonces de routage. Lorsque l'utilisation de protocoles de routage dynamiques est nécessaire, celle-ci doit s'accompagner de la mise en place d'une surveillance des annonces de routage, et de procédures permettant de réagir rapidement en cas d'incidents.

RES-ROUTDYN-IGP : configurer le protocole IGP de manière sécurisée. Le protocole de routage dynamique de type IGP doit être activé exclusivement sur les interfaces nécessaires à la construction de la topologie du réseau et désactivé sur le reste des interfaces. La configuration du protocole de routage dynamique doit systématiquement s'accompagner d'un mot de passe de type MESSAGE-DIGEST-KEY.

RES-ROUTDYN-EGP : sécuriser les sessions EGP. Lors de la mise en place d'une session EGP avec un pair extérieur sur un média partagé, cette session doit s'accompagner d'un mot de passe de type message-digest-key.

RES-SECRET : modifier systématiquement les éléments d'authentification par défaut des équipements et services. Les mots de passe par défaut doivent être impérativement modifiés, de même en ce qui concerne les certificats. Les dispositions nécessaires doivent être prises auprès des fournisseurs de façon à pouvoir modifier les certificats installés par défaut.

RES-DURCI : durcir les configurations des équipements de réseaux. Les équipements de réseaux (comme les routeurs) doivent faire l'objet d'un durcissement spécifique comprenant notamment, outre le changement des mots de passe et certificats, la désactivation des interfaces et services inutiles, ainsi que la mise en place de mécanismes de protection du plan de contrôle.

#### 5. Protection des données sensibles

EXP-PROT-INF : protection des informations sensibles en confidentialité et en intégrité. **Des mesures doivent être mises en œuvre afin de garantir la protection des informations sensibles en confidentialité et en intégrité.** A défaut d'utilisation d'un réseau homologué, ces informations doivent être chiffrées à l'aide d'un moyen de chiffrement labellisé.

#### 6. Sécurité des ressources informatiques

EXP-TRAC : traçabilité des interventions sur le système. **Les interventions de maintenance sur les ressources informatiques de l'entité doivent être tracées** par le service informatique, et ces traces doivent être accessibles au correspondant SSI local durant au moins un an.

EXP-CONFIG : configuration des ressources informatiques. Les systèmes d'exploitation et les logiciels doivent faire l'objet d'un durcissement. **Les configurations et mises à jour sont appliquées** dans le strict respect des guides ou procédures en vigueur dans l'entité ou, par défaut, en vigueur au niveau central.

EXP-DOC-CONFIG : documentation des configurations. **La configuration standard des ressources informatiques doit être documentée et mise à jour à chaque changement notable.**

## 7. Gestion des droits d'administration

EXP-SEQ-ADMIN : séquestre des authentifiants « administrateur ». **Les authentifiants permettant l'administration des ressources des SI doivent être placés sous séquestre et tenus à jour, dans un coffre ou une armoire fermée à clé.** L'authenticité doit être informé de l'existence de ces opérations de gestion, de leurs finalités et limites. **Tout accès d'administration à une ressource informatique doit pouvoir être tracé et permettre de remonter à la personne exerçant ce droit.** Les informations d'authentification bénéficiant d'un moyen de protection physique (notamment carte à puce) n'ont, par défaut, pas besoin d'être l'objet d'opérations de séquestre de la part d'autres personnels que l'authenticité lui-même.

EXP-POL-ADMIN : politique de mots de passe « administrateurs ». **Chaque administrateur doit disposer d'un mot de passe propre et destiné à l'administration.**

EXP-DEP-ADMIN : gestion du départ d'un administrateur des SI. **En cas de départ d'un administrateur disposant de privilèges sur des composants des SI, les comptes individuels dont il disposait doivent être immédiatement désactivés.** Les éventuels mots de passe d'administration dont il avait connaissance doivent être changés (exemples : mots de passe des comptes fonctionnels, comptes génériques ou comptes de service utilisés dans le cadre des fonctions de l'administrateur).

## 8. Lutte contre les codes malveillants

EXP-PROT-MALV : protection contre les codes malveillants. **Des logiciels de protection contre les codes malveillants, appelés communément antivirus, doivent être installés** sur l'ensemble des serveurs d'interconnexion, serveurs applicatifs et postes de travail de l'entité. Ces logiciels de protection doivent être distincts pour ces trois catégories au moins, et le dépouillement de leurs journaux doit être corrélé.

EXP-GES-ANTIVIR : gestion des événements de sécurité de l'antivirus. Les événements de sécurité de l'antivirus doivent être remontés sur un serveur national pour analyse statistique et gestion des problèmes a posteriori (exemples : serveur constamment infecté, virus détecté et non éradiqué par l'antivirus, etc.).

EXP-MAJ-ANTIVIR : mise à jour de la base de signatures. **Les mises à jour des bases antivirales et des moteurs d'antivirus doivent être déployées automatiquement sur les serveurs** et les postes de travail par un dispositif prescrit par les services centraux.

EXP-NAVIG : configuration du navigateur Internet. Le navigateur déployé par l'équipe locale chargée des SI sur l'ensemble des serveurs et des postes de travail nécessitant un accès Internet ou Intranet doit être configuré de manière sécurisée (désactivation des services inutiles, nettoyage du magasin de certificats, etc.).

## 9. Mise à jour des systèmes et des logiciels

EXP-POL-COR : définir et mettre en œuvre **une politique de suivi et d'application des correctifs de sécurité.** Le maintien dans le temps du niveau de sécurité d'un système d'information impose une gestion organisée et adaptée des mises à jour de sécurité. Un processus de gestion des correctifs propre à chaque système ou applicatif doit être défini, et adapté suivant les contraintes et le niveau d'exposition du système.

EXP-COR-SEC : **déploiement des correctifs de sécurité.** Les correctifs de sécurité des ressources informatiques locales doivent être déployés par l'équipe locale chargée des SI en s'appuyant sur les préconisations et outils proposés par les services centraux.

EXP-OBSOLETE : **assurer la migration des systèmes obsolètes.** L'ensemble des logiciels utilisés sur le système d'information doit être dans une version pour laquelle l'éditeur assure le support, et tenu à jour. En cas de défaillance du support, il convient d'en étudier l'impact et de prendre les mesures adaptées.