

 Direction de la sécurité et de la sûreté nucléaire	Nature du document : Instruction (Référentiel DSSN)	Page : 1 / 62
	Référence du document : RSSN-SSI-01-01	Indice : 9

Titre du document : PSSI CEA <i>Politique de sécurité des systèmes d'information</i>		
Pièces jointes éventuelles :		
N°	Titres	Nb de pages
Destinataires ou référence à une liste de diffusion : 		

2019

	Diffusion
Nom :	J-L. Vo Van Qui
Fonction :	DSSN – AQSSI CEA
Date & Visa :	

Direction de la sécurité et de la sûreté nucléaire / Service de sécurité des systèmes d'information
 Commissariat à l'énergie atomique et aux énergies alternatives
 Centre de Paris-Saclay – Établissement de Fontenay-aux-Roses – B.P. 6 – 92265 Fontenay-aux-Roses Cedex
 ✉ liste_dssn_s3i@cea.fr

Référence du document : RSSN-SSI-01-01	Page 2 / 62
Titre du document : PSSI CEA	Indice : 9

Historique des évolutions d'indice :

Indice	Date	Nature des modifications
8	20/02/2017	Première publication
9	15/03/2019	Nouvelle mise en page Nouvelle référence de document (ancienne : SPACI-SSI-REG-0324) Principales évolutions : – Périmètre de la PSSI – Périmètre et missions ASSI – définition plus précise et plus complète – Rôles et Responsabilités sur la cartographie et inventaires des moyens informatiques – Rôles, responsabilités, attendus pour la gestion des comptes utilisateurs – Gestion contractuelle – Offre Cloud – Évolution des contraintes liées à la sécurité réseau – Réseau SAN – Principe de « Blacklist » applications – Évolution de la politique mots de passe – Prise en compte INCA – Fédération Identité – Gestion des matériels en fin de vie / Généralisation du chiffrement de surface – Prise en compte des évolutions Mobi – Interdiction du multiboot / Assimilation des machines virtuelles, aux machines physiques – Plan de sauvegarde informatique (PCA, PRA et PPP) – Modification des documents annexes

Référence du document : RSSN-SSI-01-01	Page 3 / 62
Titre du document : PSSI CEA	Indice : 9

SOMMAIRE

1. Préambule.....	9
Définitions.....	9
2. Politique, organisation et gouvernance	10
2.1 Organisation de la SSI	10
2.1.1 Organisation SSI	10
2.1.2 Identification des acteurs SSI.....	10
2.1.3 Désignation du responsable SSI	11
2.1.4 Formalisation des responsabilités	11
Rôles et Missions des ASSI	11
2.1.5 Responsabilité vis-à-vis des tiers	14
2.1.6 Application des mesures de sécurité au sein de l'entité	14
2.1.7 Formalisation des documents d'application	14
3. Ressources humaines.....	15
3.1 Ressources humaines	15
3.1.1 Charte d'application SSI.....	15
3.1.2 Choix et sensibilisation des personnels SSI.	15
3.1.3 Personnel de confiance	15
3.1.4 Sensibilisation des utilisateurs des systèmes d'information	15
3.1.5 Gestion des arrivées, des mutations et des départs.....	15
3.1.6 Gestion du personnel non permanent.....	16
4. Intégration de la SSI dans le cycle de vie des Systèmes d'information	17
4.1 Cartographie des SI	17
4.1.1 Inventaire des ressources informatiques	17
4.1.2 Cartographie.....	17
4.2 Qualification et protection de l'information	18
4.2.1 Qualification des informations	18
4.2.2 Protection des informations.....	18
4.3 Gestion des risques et homologation de sécurité.....	18
4.3.1 Homologation de sécurité des systèmes d'information.....	18
4.4 Maintien en condition de sécurité	19
4.4.1 Intégration de la sécurité dans les projets.....	19
4.4.2 Mise en œuvre au quotidien de la SSI	19
4.4.3 Tableau de bord SSI	19
4.5 Produits et services qualifiés ou certifiés	20
4.5.1 Acquisition de produits et services de confiance	20
4.6 Maîtrise des prestations.....	20
4.6.1 Clauses de sécurité.....	20
4.6.2 Suivi et contrôle des prestations fournies	20
4.6.3 Analyse de risques	20
4.6.4 Hébergement et clauses de sécurité.....	21
5. Sécurité physique	22
5.1 Sécurité physique des locaux abritant les SI	22
5.1.1 Règles générales	22
5.1.2 Règles de sécurité des zones d'accueil du public	22
5.1.3 Protection des informations sensibles au sein des zones d'accueil	23

Référence du document : RSSN-SSI-01-01	Page 4 / 62
Titre du document : PSSI CEA	Indice : 9

5.1.4	Règles de sécurité des locaux techniques.....	23
5.1.5	Protection des câbles électriques et de télécommunication	23
5.1.6	Contrôles anti-piégeages	23
5.2	Sécurité physique des centres d'information	24
5.2.1	Règles générales	24
	Découpage des locaux en zones de sécurité	24
	Convention de service en cas d'hébergement tiers	24
5.2.2	Règles de sécurité aux zones internes	24
	Contrôle d'accès physique	24
	Délivrance des moyens d'accès physique	24
	Traçabilité des accès.....	24
5.2.3	Règles de sécurité des salles informatiques et locaux techniques.....	24
5.3	Sécurité du système d'information de sûreté	25
6.	Sécurité des réseaux	26
6.1	Usage sécurisé du réseau CEAnet.....	26
6.1.1	Systèmes autorisés sur le réseau	26
6.1.2	Interconnexion avec des réseaux externes	26
6.1.3	Filtrage réseau des flux sortants et entrants	26
6.1.4	Protection des informations.....	26
6.2	Usage sécurisé des réseaux locaux	27
6.2.1	Cloisonnement en sous-réseaux de sécurité homogènes	27
	Zones Réseaux	27
	Niveaux de sécurité.....	28
	Passerelle Internet	28
	Conditions d'emploi de la Zone Hébergement.....	29
6.2.2	Cloisonnement des ressources en cas de partage des locaux.....	29
6.3	Accès spécifiques	29
6.4	Usage des réseaux sans fil.....	29
6.4.1	Mise en place des réseaux sans fil	29
6.5	Sécurité des mécanismes de commutation et de routage.....	30
6.5.1	Protection contre les attaques en couches basses.....	30
6.5.2	Protection des annonces de routage	30
6.5.3	Configuration sécurisée du protocole IGP	30
6.5.4	Configuration sécurisée des sessions EGP	30
6.5.5	Conditions d'accès à l'administration	30
6.5.6	Durcissement des configurations des équipements réseau	30
6.6	Cartographie réseau	31
6.6.1	Documents d'architecture technique et fonctionnelle	31
7.	Architecture et exploitation des SI.....	32
7.1	Architecture sécurisée des centres informatiques.....	32
7.1.1	Principe d'architecture des centres informatiques	32
7.1.2	Architecture de stockage et de sauvegarde.....	32
	Réseau SAN de Stockage	32
7.2	Protection des informations sensibles	33
7.2.1	Protection des informations sensibles en confidentialité et en intégrité	33
7.3	Surveillance et configuration des ressources informatiques	33
7.3.1	Traçabilité des interventions sur le système	33
7.3.2	Configuration des ressources informatiques.....	33
7.3.3	Documentation des configurations	34

Référence du document : RSSN-SSI-01-01	Page 5 / 62
Titre du document : PSSI CEA	Indice : 9

7.4	Autorisation et contrôle d'accès	34
7.4.1	Contrôle des accès logiques	34
	Identification et contrôle d'accès logique	34
	Droits d'accès aux ressources	34
	Gestion des profils d'accès aux applications	34
7.4.2	Processus d'autorisation	35
	Autorisation d'accès des utilisateurs	35
	Revue des autorisations d'accès	35
7.4.3	Gestion des authentifiants	35
	Confidentialité des informations d'authentification	35
	Gestion des mots de passe	35
	Initialisation des mots de passe	35
	Gestion des certificats de chiffrement	36
	Cas particulier de la réinitialisation	36
	Politiques des mots de passe	36
	Utilisation des certificats électroniques	36
	Contrôle systématique de la qualité des mots de passe	36
	Fédération des Identités	37
7.4.4	Gestion des authentifiants d'administration	37
	Séquestre des authentifiants « Administrateur »	37
	Politique des mots de passe « Administrateur »	37
	Gestion des départs d'un « Administrateur »	37
7.4.5	Administration des systèmes	37
	Restriction des droits	37
	Protection des accès aux outils d'administration	38
	Habilitation des administrateurs	38
	Gestion des actions d'administration	38
	Sécurisation des flux d'administration	38
	Centraliser la gestion des systèmes d'information	38
	Sécurisation des outils de prise en main à distance	39
7.4.6	Administration des domaines	39
	Définir une politique de gestion des comptes du domaine	39
	Configurer la stratégie des mots de passe des domaines	39
	Définir et appliquer une nomenclature des comptes du domaine	39
	Restreindre au maximum l'appartenance aux groupe d'administration du domaine	39
	Maîtriser l'utilisation des comptes de service	40
	Limiter les droits des comptes de service	40
	Désactiver les comptes du domaine obsolètes	40
	Améliorer la gestion des comptes d'administrateurs locaux	40
7.5	Envoi en maintenance et mise au rebut	40
	Maintenance externe	40
	Mise au rebut	41
7.5.2	Lutte contre les codes malveillants	41
	Protection contre les codes malveillants	41
	Gestion des événements de sécurité de l'antivirus	41
	Mise à jour de la base de signatures	41
7.5.3	Mise à jour des systèmes et des logiciels	42
	Politique de suivi et d'applications des correctifs de sécurité	42
	Déploiement des correctifs de sécurité	42
	Assurer la migration des systèmes obsolètes	42
	Isoler les systèmes obsolètes	42
7.5.4	Journalisation	43
	Journalisation des alertes	43
	Politique de gestion et d'analyse des journaux	43
	Conservation des journaux	43
7.6	Défense des systèmes d'information	43
7.6.1	Gestion dynamique de la sécurité	43
7.6.2	Gestion des matériels fournis à l'utilisateur	43

Référence du document : RSSN-SSI-01-01	Page 6 / 62
Titre du document : PSSI CEA	Indice : 9

Maîtrise des matériels	43
Mesures de protections contre le vol et la perte	44
Déclarer les pertes et vols	44
Réaffectation de matériels informatiques	44
7.6.3 Nomadisme	44
Déclaration des équipements nomades aptes à traiter des informations sensibles	44
Accès à distance au système d'information CEA	45
7.6.4 Sécurité des imprimantes et copieurs multifonction	45
Impression des informations sensibles	45
Sécurité des imprimantes et des copieurs multifonctions	45
7.7 Exploitation sécurisée des centres informatiques	45
7.7.1 Sécurité des ressources informatiques	45
Système d'exploitation	45
Logiciel en tiers présentation	46
Logiciel en tiers application	46
Logiciel en tiers données	46
Passerelle d'échange de fichiers	46
Messagerie technique	46
Flux d'administration	46
Service de nom de domaine - DNS technique	47
Effacement de support	47
Destruction de support	47
Traçabilité / imputabilité	47
Supervision	47
Accès aux périphériques amovibles	47
Accès aux réseaux	47
Audit / Contrôle	48
8. Sécurité du poste de travail	49
8.1 Sécurisation des postes de travail	49
8.1.1 Mise à disposition du poste	49
Fourniture et gestion des postes de travail	49
Formalisation de la configuration des postes de travail	49
8.1.2 Sécurité physique des postes de travail	50
Verrouillage de l'unité centrale des postes fixes	50
Postes portables	50
Postes CEA en zones d'accueil du public ou en salles de réunion en accès libre	50
8.1.3 Réaffectation du poste et récupération d'informations	50
8.1.4 Gestion des privilèges sur les postes de travail	50
Privilèges des utilisateurs sur le poste de travail	50
Utilisation des privilèges d'accès "Administrateur"	51
Gestion du compte "Administrateur local"	51
8.1.5 Protection des informations	51
Stockage des informations	51
Sauvegarde / Synchronisation des données locales	51
Partage de fichiers ou de ressources	51
Suppression des données sur les postes partagés	52
Chiffrement des données sensibles	52
Protection des flux d'informations	52
Fourniture de supports de stockage amovible	52
8.1.6 Nomadisme	52
Accès à distance aux Systèmes d'Information de l'entité	52
Pare-feu local	53
Stockage local d'information sur les postes nomades	53
Filtre de confidentialité	53
Configuration des interfaces de connexion sans fil	53
Désactivation des interfaces de connexion sans fil	53
Utilisation des outils nomades dans le cadre du Télétravail	53

Référence du document : RSSN-SSI-01-01	Page 7 / 62
Titre du document : PSSI CEA	Indice : 9

8.2	Sécurisation des copieurs multifonctions.....	53
	Durcissement des imprimantes et copieurs multifonctions	53
	Sécurisation de la fonction numérisation	53
8.3	Sécurisation de la téléphonie.....	54
	Sécurisation de la téléphonie	54
	Sécuriser la configuration des autocommutateurs	54
	Codes d'accès téléphoniques	54
	DECT	54
8.4	Contrôles de la conformité des postes de travail.....	54
	Utiliser des outils de vérification automatique de la conformité	54
9.	Sécurité du développement des systèmes	56
9.1	Prise en compte de la sécurité dans le développement des SI.....	56
	Intégrer la sécurité dans les développements locaux	56
	Intégrer des clauses SSI dans les contrats de sous-traitance de développement informatique	56
9.2	Prise en compte de la sécurité dans le développement des logiciels	56
	Limiter les fuites d'information.....	56
	Réduire l'adhérence des applications à des produits ou technologies spécifiques	56
	Instaurer des critères de développement sécurisé	56
	Intégrer la sécurité dans le cycle de vie logiciel.....	57
	Améliorer la prise en compte de la sécurité dans les développements Web	57
	Calculer les empreintes de mots de passe de manière sécurisée	57
9.3	Sécurisation des applications à risques.....	57
	Mettre en œuvre des fonctionnalités de filtrage applicatif pour les applications à risque.....	57
10.	Traitement des incidents.....	58
10.1	Chaînes opérationnelles	58
10.1.1	Traitement des alertes de sécurité émises par l'ANSSI.....	58
	Chaînes opérationnelles SSI.....	58
	Mobilisation en cas d'alerte	58
10.1.2	Remontée des incidents de sécurité rencontrés.....	58
	Qualification et traitement des incidents	58
	Remontée des incidents.....	58
11.	Continuité d'activité.....	59
11.1	Gestion de la continuité d'activité	59
11.1.1	Mise en œuvre plan local de sécurité des Systèmes d'Information (PSI)	59
	Définition du plan local de sécurité des Systèmes d'Information (PSI)	59
	Plan de continuité d'activité – PCA des SI	59
	Plan de reprise d'activité – PRA des SI	59
	Plan de protection du patrimoine (protection des seules données) – PPP des SI	59
	Suivi de la mise en œuvre du plan de continuité d'activité local des Systèmes d'Information (PCA des SI)	59
	Mise en œuvre des dispositifs techniques et des procédures opérationnelles.....	60
	Protection de la disponibilité des sauvegardes.....	60
	Protection de la confidentialité des sauvegardes.....	60
11.1.2	Maintien en conditions opérationnelles du plan local de sécurité des SI (PSI)	60
	Exercice régulier du plan local de sécurité des Systèmes d'Information (PSI).....	60
	Mise à jour du plan local de sécurité des Systèmes d'Information (PSI).....	60
12.	Conformité, audit, inspection et contrôle.....	61
12.1	Contrôles réguliers.....	61
	Contrôles locaux.....	61
	Bilan Annuel	61

Référence du document : RSSN-SSI-01-01	Page 8 / 62
Titre du document : PSSI CEA	Indice : 9

13. Annexes	62
13.1 Documents de référence	62
13.2 Documents abrogés par la présente PSSI	62

Référence du document : RSSN-SSI-01-01	Page 9 / 62
Titre du document : PSSI CEA	Indice : 9

1. PRÉAMBULE

Ce document est la Politique de Sécurité des Systèmes d'Information du CEA [PSSI]. Il a pour objectif de définir les mesures techniques et organisationnelles mises en œuvre au CEA pour assurer la protection de son système d'information face aux cyber-menaces.

Le système d'information recouvre l'ensemble des moyens informatiques, les matériels, logiciels, applications, base de données, réseaux et fichiers numériques (moyens fixes ou mobiles, qu'ils soient locaux, ou accessibles à distance, placés sous la responsabilité des unités du CEA). Le système d'information est destiné à élaborer, traiter, stocker, échanger ou détruire les informations. Ces informations peuvent concerner tous les domaines d'activité du CEA : scientifique, technique, administratif, de gestion, bureautique, industriel et réseaux de télécommunication pouvant être mis à disposition par le CEA.

Chaque acteur de la PSSI est tenu d'appliquer les mesures et les directives de sécurité qu'elle définit et qui visent à assurer :

- la protection des informations dont le CEA est le propriétaire ou le dépositaire,
- la continuité et l'intégrité des services de traitement et de transport de l'information,
- la conformité avec la Politique de Sécurité des Systèmes d'Information de l'état [PSSI-E].

La présente PSSI s'applique à l'ensemble des systèmes d'informations relevant du périmètre de responsabilité du CEA, à l'exception des systèmes d'information relevant du contrôle gouvernemental d'intégrité des moyens de la dissuasion nucléaire¹.

Définitions

La présente PSSI définit la typologie de **matériels** :

- le poste de travail comme étant : L'ensemble des matériels correspondant à une notion de postes informatiques, i.e. ordinateur de bureau, ordinateur portable, téléphone connectés (Smartphone), tablette², station de travail, terminal passif, kiosque, machines virtuelles, ou équipements connectés,
- le serveur comme un fournisseur de ressources informatiques, à des services applicatifs, des services d'infrastructures, à des services techniques, à des services industriels et de commandes, à d'autres serveurs et in fine à des postes de travail,
- les équipements réseaux comme l'ensemble des éléments et composants mettant en relation deux postes de travail, deux serveurs, un serveur et un poste de travail, entre eux, avec un autre sous ensemble réseaux, ou internet,
- la téléphonie et le téléphone fixe (y compris DECT), comme étant les équipements de téléphonie commuté ou IP, avec ou sans fil, rattaché à une infrastructure propre à un bâtiment un ensemble de bâtiments, ou un site,
- un téléphone portable comme un terminal mobile de téléphonie limité en termes de fonction à l'envoi réception de sms et l'émission / la réception de communication vocale.³

¹ Code de la défense, article R*1411-7 à R*1411-11

Arrêté CD du Premier Ministre du 5 janvier 2016 relatif aux modalités d'exercice du contrôle gouvernemental de la dissuasion et aux moyens nécessaires à la mise en œuvre de la politique de dissuasion

Instruction Ministérielle n°26 du 24 janvier 2017 relative au contrôle gouvernemental de l'intégrité des moyens de la dissuasion nucléaire – réf. N°26/DEF/CAB/CM1/CD-SF

Directive d'Application du Contrôle Gouvernemental de l'Intégrité des Moyens de la dissuasion nucléaire applicable au sein des INID ne relevant pas du Ministre des Armées – CEA/DAM/DQSCG CD-SF 689/2018

Courrier n°167/ARM/CAB/CM2/CD-SF du 04/05/2018 portant approbation de la DACG

² Les tablettes Windows sont considérées comme des pc portable, les autres tablettes sous Android ou iOS sont à considérer comme des smartphones, les DECT sont considérés comme des téléphones fixes.

³ Les relais de téléphonie mobile ne sont pas inclus dans cette définition.

Référence du document : RSSN-SSI-01-01	Page 10 / 62
Titre du document : PSSI CEA	Indice : 9

2. POLITIQUE, ORGANISATION ET GOUVERNANCE

2.1 Organisation de la SSI

2.1.1 Organisation SSI

L'organisation de la Sécurité des Systèmes d'Information [SSI] se conforme à la NIG 613 sur l'organisation de la sécurité au CEA.

Le Directeur de la sécurité et de la sûreté nucléaire [DSSN] est l'Autorité Qualifiée de la Sécurité des Systèmes d'Information [AQSSI] du CEA. Il est nommé par le Haut Fonctionnaire de Défense et de Sécurité [HFDS] du Ministère de tutelle. Il est également Autorité d'Homologation pour l'ensemble du CEA à l'exception des systèmes d'information relevant du contrôle gouvernemental de l'intégrité des moyens de la dissuasion nucléaire.

2.1.2 Identification des acteurs SSI

Les utilisateurs des moyens informatiques du CEA sont responsables de leur utilisation du système d'information, de la protection des informations dont ils sont détenteurs et du bon usage des moyens mis à leur disposition par leur autorité hiérarchique.

La SSI du CEA s'appuie sur le réseau des Agents de Sécurité des Systèmes d'Information [ASSI] dont le missions sont détaillées au § 2.1.4.

Les Officiers de Sécurité [OS] travaillent conjointement avec les ASSI de leur périmètre respectif sur les aspects suivants :

- Identification et qualification des informations sensibles,
- Élaboration et maintien du des guides de classification,
- Processus d'habilitation des tiers, des intervenants et des personnes accédant aux systèmes d'information classifiés de défense,
- Suivi des marchés et des clauses contractuelles de sécurité vis-à-vis des tiers,
- Respect réglementaire de la protection physique des locaux et de la gestion des documents matérialisés.

Les Correspondants à la Protection des données (CPD) sont en charge de l'application de la politique interne CEA de mise en œuvre de la réglementation sur la protection des données à caractère personnel, sous l'autorité du Délégué à la protection des données (DPD).

La mise en œuvre et le maintien en condition de sécurité des systèmes d'informations sont confiés à la filière informatique pilotée par la Direction des Systèmes d'Information [DSI].

La DSI est responsable de l'animation de la filière informatique, de la mise en application de la PSSI et de la définition des configurations et de l'architecture du système d'information. Elle assure dans le cadre de ces missions, la mise à disposition des moyens d'inventaires et de cartographie globale du système d'information. Elle assure pilote et coordonne, l'ensemble des actions opérationnelles (inventaire, relevées, documentations) permettant la tenue et la mise à disposition d'une cartographie complète et détaillée du système d'information CEA associée à un inventaire exhaustif, précis et à jour de l'ensemble des équipements techniques y appartenant

Les Unités de services communs en informatique [USCI] sont responsables de l'exploitation et du maintien en condition de sécurité de l'infrastructure informatique du CEA, composée des réseaux, des télécommunications, des postes de travail et des systèmes de gestion et de partage des connaissances. Les USCI sont également responsables de la création et du maintien des inventaires et cartographie globale des éléments techniques d'infrastructures.

Les USCI sont également le point d'entrée des incidents de sécurité informatiques pour lesquels elles assurent un service d'astreinte en heures non ouvrables.

Chaque centre dispose d'une équipe d'exploitation locale en charge des systèmes d'information que l'on appellera [STIC] dans la PSSI. Le SIPS (Service Informatique Paris-Saclay) assure le rôle de STIC pour le centre de Paris-Saclay. Le STIC assure les missions de la filière informatique pour toutes les ressources sous

Référence du document : RSSN-SSI-01-01	Page 11 / 62
Titre du document : PSSI CEA	Indice : 9

la responsabilité du chef d'établissement. Les STIC alimentent et renseignent les outils d'inventaires et de cartographies globales du SI CEA.

Le Schéma Directeur du Système d'Information [SDSI] élaborée par la DSI sur les évolutions du système d'information, intègre la SSI dans ses évolutions.

2.1.3 Désignation du responsable SSI

Le Responsable SSI du CEA [RSSI] est nommé par l'AQSSI. Il est chargé de l'élaboration et des évolutions de la présente PSSI, de sa mise en œuvre au CEA, des relations avec les Fonctionnaires de Sécurité des Systèmes d'Information des ministères de tutelle [FSSI] et de l'Agence Nationale de Sécurité des Systèmes d'Information [ANSSI]. Il coordonne également le traitement des incidents SSI significatifs.

Le RSSI est membre permanent du Comité des Systèmes d'Information [CSI] auquel il rapporte des évolutions de la PSSI après validation par l'AQSSI.

Le RSSI s'appuie sur les compétences techniques du Service de sécurité des systèmes d'information (S³I) de la DSSN pour les audits techniques de sécurité, les aptitudes logiques dans le cadre de l'homologation, la détection d'incidents et les opérations techniques de remédiation.

2.1.4 Formalisation des responsabilités

Les missions et responsabilités des ASSI⁴ sont définies par la présente PSSI. Les ASSI de centre et de direction opérationnelle sont nommés par leur autorité hiérarchique après proposition au RSSI.

Les ASSI d'unité sont nommés par leur autorité hiérarchique (directeur d'institut, directeur fonctionnel ou chef de département) après validation par l'ASSI de centre qui vérifie leur appartenance à l'unité, leur niveau d'habilitation et leur niveau de formation à la SSI. L'ASSI de centre avise le RSSI des nominations d'ASSI d'unités de son centre.

Chaque ASSI est tenu de suivre une formation dans le domaine de la SSI, compléter d'une remise à niveau annuelle.

Le niveau d'habilitation des ASSI est Confidentiel Défense (à minima) et il doit s'agir de personnel CEA permanent.

Les ASSI en cours de mission sont référencés dans l'annuaire des ASSI mis en œuvre par le RSSI.

Les ASSI titulaires ont la possibilité de désigner un ou plusieurs ASSI suppléants. L'ASSI titulaire en informe l'ASSI de son centre ainsi que le RSSI pour que les ASSI suppléants puissent être référencés dans l'annuaire des ASSI en qualité de suppléant sur le périmètre concerné. Les conditions d'accès à la fonction de suppléance sont les mêmes que pour la fonction du titulaire. Les missions des ASSI suppléants sont définies par l'ASSI titulaire. Elles peuvent être équivalente à l'ASSI titulaire, ou restreintes à certaines activités. L'ASSI nommé conserve la responsabilité de la fonction.

Rôles et Missions des ASSI

Les ASSI sont les garants du respect de la PSSI, par les projets et les unités opérationnelles de leur périmètre, et agissent en tant que conseiller de leur direction (ou autorité) hiérarchique. À ce titre, ils sont en charge d'un certain nombre de missions transverses de SSI.

Missions	ASSI de Direction	ASSI de Centre	ASSI d'Unité
PSSI	Sont garant du respect de la PSSI, par les projets, activités et entités, relevant de son périmètre fonctionnel (y compris les unités mixtes)	Sont garant du respect de la PSSI, par les projets, activités et entités, relevant de son périmètre géographique (y compris les unités mixtes, et entités informatiques locales)	Sont garant du respect de la PSSI, par les projets, activités et entités, relevant de son périmètre fonctionnel (y compris les unités mixtes, et entités informatiques locales)

⁴ La PSSI ne distingue pas ASSI et ASSI adjoint

Référence du document : RSSN-SSI-01-01	Page 12 / 62
Titre du document : PSSI CEA	Indice : 9

Missions	ASSI de Direction	ASSI de Centre	ASSI d'Unité
Analyse des Risques	Sont en charge de l'analyse globale des risques SSI pour leur périmètre et des mesures de continuité d'activité à mettre en place ou à prioriser – en coordination avec l'ASSI de Centre Collaborent avec les ASSI des centres hébergeurs de leurs unités, à la consolidation d'une cartographie globale des systèmes et des risques SSI par direction	Veillent à l'application de la PSSI au niveau de la filière informatique de leur centre Sont en charge de l'analyse globale des risques SSI pour leur périmètre géographique et du suivi de la bonne adéquation aux besoins des mesures de continuité d'activité mise en place par les entités informatiques Est le référent Moyen de continuité de services pour les ASSI de Directions et d'Unité	Sont en charge de détaillée des risques SSI de chaque système, et de l'identification des systèmes critiques (en terme de valeur / Risques : activité) pour leur entité
Homologations des systèmes	Contribuent à l'identification des niveaux d'homologation des systèmes, adaptés au niveau d'exigences de sécurité des projets	Contribuent à l'identification des niveaux d'homologation des systèmes, adaptés au niveau d'exigences de sécurité des projets	Assistent le directeur d'institut, le directeur fonctionnel ou le chef de département dans les démarches d'homologation ou d'analyse de risque sur les systèmes d'information
Coordination ASSI / Animation Réseau ASSI	Assurent la coordination⁵ des ASSI de centre ou d'unité de leur direction	Assurent l'animation⁶ du réseau des ASSI d'unités présentes sur leur centre	
Gestion des incidents / Traitement des incidents SSI	Consolident les informations d'incidents de sécurité et déterminent au niveau de leurs périmètre les actions globales de sensibilisations nécessaires, et les actions de sécurisation de l'activité	Sont acteurs du traitement des incidents SSI majeurs ou sensibles	Assurent un rôle d'acteur dans la gestion des incidents SSI (levée de doute)
Pilotage des S2IV et systèmes sensibles	Consolident au niveau de leur périmètre une cartographie globale des systèmes, des systèmes sensibles et S2IV des centres d'hébergements de données, locaux informatiques techniques et d'exploitation, et les risques opérationnels liés aux risques SSI, quelle que soit l'unité d'appartenance de l'unité hébergée	Consolident au niveau de leur périmètre une cartographie globale des systèmes, des systèmes sensibles, des centres d'hébergements de données, locaux informatiques techniques et d'exploitation, et les risques opérationnels liés aux risques SSI, quelle que soit l'unité d'appartenance de l'unité hébergée	Assiste l'ASSI de centre direction dans le suivi des S2IV et systèmes sensibles

⁵ Coordination : Définition des objectifs, harmonisation des consignes, études de conformités

⁶ Animation : réunion régulière, prise en compte des contraintes fonctionnelles et locales, segmentation des activités, résolution des points de défaillances communs, prise en compte des contraintes SSI dans le cadre des réalisations informatiques ...

Missions	ASSI de Direction	ASSI de Centre	ASSI d'Unité
Cartographie Fonctionnelle (quels systèmes pour quelles fonctions)	Consolident au niveau de leur périmètre une cartographie globale des systèmes, des systèmes sensibles (S2IV), des droits d'accès, des silos de données et des risques opérationnels liés aux risques SSI	Consolident au niveau de leur périmètre une cartographie globale des systèmes, des systèmes sensibles (S2IV), des silos de données et des risques opérationnels liés aux risques SSI	Établissent et tiennent à jour une cartographie fonctionnelle ⁷ , des systèmes métiers ⁸ , moyens informatiques, droits d'accès et classifications des informations, pour leurs périmètres, ainsi que leurs localisations
Cartographie Technique / Cartographie Informatique (L'ensemble des moyens techniques et leurs localisation)		S'assurent de la conduite des actions de la réactualisation régulière et de la justesse (via audit) de la cartographie des moyens techniques réalisés par le STIC pour son périmètre géographique	S'assurent de la bonne tenue à jour de la cartographie des moyens techniques, mise à jour et entretenue par le STIC
Stratégie de Publication	Collaborent à la stratégie de publication du pôle de la direction avec l'Officier de Sécurité de la direction		
Classification de l'information	Se coordonnent avec les Officiers de Sécurité(OS), et les Correspondant Protection des Données (CPD) pour l'élaborer une politique de classifications et de mesures de la valeur de l'information, et en déduisent une politique de droits d'accès informatiques, (basée sur le droit « à en connaître ») et de droits de diffusions.		
Vérification de la gestion des droits d'accès	S'assure que les audits de droits des unités sont réalisés pour son périmètre. S'assure de la disponibilité et conformité des outils d'audit nécessaires aux vérifications	S'assure que les audits de droits des unités sont réalisés pour son périmètre. S'assure de la disponibilité et conformité des outils d'audit nécessaires aux vérifications	Vérifie la conformité des démarches d'autorisation d'accès pour les droits d'accès des utilisateurs (comptes, demandes d'autorisation, authentifiant et certificats). Vérifie régulièrement (via audit) la bonne tenue à jour et la pertinence des droits d'accès sur les ressources de données et applications du SI
Remontée d'Indicateur de SSI	Consolident la remontée des indicateurs SSI (issu de la supervision) pour sa direction	Consolident la remontée des indicateurs SSI (issu de la supervision) pour le centre	
Sensibilisation des nouveaux Arrivants et des personnels		Assurent de la sensibilisation des nouveaux arrivants	Assurent la sensibilisation des personnels CEA et non CEA de leur périmètre

⁷ Cartographie des fonctions, responsabilités, besoins métiers et attendus « métiers ». Identification des données critiques et des données de valeurs

⁸ Sous-éléments constitutif du système d'information, spécifique à une fonction un besoin ou un attendu métier, ou dédié à un objectif particulier

Référence du document : RSSN-SSI-01-01	Page 14 / 62
Titre du document : PSSI CEA	Indice : 9

Missions	ASSI de Direction	ASSI de Centre	ASSI d'Unité
Contrats et marchés	En collaboration avec l'OS, met en place les procédures et clauses type pour son périmètre	En collaboration avec l'OS, met en place les procédures et clauses type pour son périmètre	En collaboration avec le CS d'unité, s'assure que les clauses ou annexes de sécurité sont adaptées au besoin de sécurité. Valide le contenu des prestations demandées

2.1.5 Responsabilité vis-à-vis des tiers

Les clauses contractuelles liées à la réalisation de prestations de sécurité informatique ou de prestations informatiques sont validées par l'officier de sécurité. Ce dernier définit le type de marché et veille à l'intégration de la charte d'utilisation des moyens informatiques et de la PSSI dans les clauses opposables aux tiers intervenants.

La présente PSSI peut être communiquée en tant que de besoin dans le cadre d'une consultation ou pour la mise en œuvre d'une convention avec un organisme tiers.

Les ASSI valident le contenu des prestations demandées pour vérifier l'adéquation du cahier des charges avec les exigences de la PSSI.

2.1.6 Application des mesures de sécurité au sein de l'entité

Le RSSI est en charge de la planification des actions de mise en application de la PSSI. Il en contrôle le suivi et rend compte en CSI de l'application de la PSSI.

2.1.7 Formalisation des documents d'application

La PSSI et les documents d'application relatifs à sa mise en œuvre sont diffusés par le RSSI et mis à disposition sur le site intranet : <https://www-ssi.intra.cea.fr>

La PSSI est complétée :

- par des documents techniques plus détaillés applicables sur un contexte plus spécifique, les Instructions Techniques d'Emploi [ITE],
- par des guides d'application, plus didactiques, destinés aux maîtrises d'ouvrage et prennent en compte les aspects transverses de certains sujets. Ces guides sont mentionnés dans la présente PSSI.

Dans le contexte d'une homologation pour des systèmes traitant d'information classifié de défense, le système d'information homologué fait l'objet de procédures d'exploitation de sécurité [PES] qui décrivent les modalités complémentaires à la présente PSSI et les conditions spécifiques d'exploitation impactant la sécurité du SI homologué. La conformité entre les PES d'un système homologué classifié de défense et la PSSI fait partie intégrante du processus d'homologation, en particulier la non application de mesures de la présente PSSI est validée par l'autorité d'homologation et acceptée par l'autorité d'emploi.

Chaque centre a la possibilité d'élaborer des procédures d'exploitation plus détaillées, en cohérence avec les standards définis par la DSI. L'ASSI de centre veille à la conformité de ces procédures avec la PSSI. La non-application d'une mesure de la présente PSSI sur un système d'information est soumise à l'accord préalable du RSSI.

Référence du document : RSSN-SSI-01-01	Page 15 / 62
Titre du document : PSSI CEA	Indice : 9

3. RESSOURCES HUMAINES

3.1 Ressources humaines

3.1.1 Charte d'application SSI

La Charte d'utilisation des moyens informatiques du CEA [NIG 608], validée par l'administrateur général et présentée aux instances représentatives du personnel, est communiquée à l'ensemble des salariés. Elle est intégrée au règlement intérieur des centres avec l'appui de la Direction Juridique et Contentieux [DJC].

Tous les personnels non permanents (au sens du § 3.1.6) sont informés de la charte dès lors que leur activité requiert l'octroi d'un droit d'accès au système d'information du CEA. La charte est intégrée aux contrats ou aux conventions qui régissent la collaboration.

La charte est portée à la connaissance de tous les utilisateurs du système d'information et leur est opposable.

3.1.2 Choix et sensibilisation des personnels SSI.

La sensibilisation des utilisateurs des systèmes d'information est confiée aux ASSI des unités concernées et aux ASSI de centre pour les nouveaux arrivants. Les ASSI sont formés à la sécurité des systèmes d'information dans le cadre de la mission. La formation INSTN « Protection Informatique des Sites et des Installations » est la formation minimale des ASSI.

Les prestataires informatiques en charge des gestes d'administration ou de l'exploitation des moyens de sécurité, opèrent dans le cadre de marché dont la nature est validée par l'officier de sécurité du centre. Compte tenu du type de marché, l'officier de sécurité valide le niveau d'habilitation requis des intervenants extérieurs.

Conformément à la charte d'utilisation des moyens informatiques du CEA, les personnels en charge de l'exploitation ainsi que les ASSI, de par leur mission de contrôle, sont soumis à une obligation de confidentialité renforcée.

3.1.3 Personnel de confiance

Toutes les personnes ayant accès de par leurs fonctions à des informations sensibles doivent disposer du niveau d'habilitation requis. L'officier de sécurité du centre est en charge de ces contrôles.

3.1.4 Sensibilisation des utilisateurs des systèmes d'information

La sensibilisation des utilisateurs est assurée par l'ASSI d'unité. En complément, des campagnes de sensibilisation sont mises en œuvre régulièrement par les ASSI de centre pour tous les nouveaux arrivants.

Des campagnes de sensibilisation particulières sont également mises en œuvre sur l'Intranet en fonction de l'actualité par le RSSI.

3.1.5 Gestion des arrivées, des mutations et des départs

On entend par :

- Arrivée : tout nouvel arrivé au sein du CEA, quel que soit le centre ;
- Départ : tout départ du CEA, quel que soit le centre ;
- Mutation : changement d'unité.

La gestion des droits d'accès informatiques associée aux arrivées, départs et aux mutations de personnel est sous la responsabilité du responsable hiérarchique de l'utilisateur concerné qui valide la demande.

Le responsable hiérarchique valide les autorisations d'accès. Il a pour responsabilité de révoquer ou faire révoquer l'ensemble des droits d'accès informatiques, des personnels quittant l'unité dont il a la charge, et ce dès la date du départ ou de la mutation effective.

Les révocations de droits d'accès suite à un départ ou une mutation (avec changement d'unité) ne nécessitent aucune validation et peuvent être réalisées automatiquement.

L'ASSI d'unité supervise, consolide et vérifie mensuellement :

Référence du document : RSSN-SSI-01-01	Page 16 / 62
Titre du document : PSSI CEA	Indice : 9

- toutes les autorisations d'accès, validées par le responsable hiérarchique ou un responsable de la ressource désigné par le responsable hiérarchique ;
- toutes les opérations de révocation liées aux droits d'accès suite à un départ ou une mutation (avec changement d'unité).

L'ASSI d'unité procède :

- aux opérations de révocations de droits, liées à une situation de non-conformité ;
- à l'audit mensuel de la liste des droits d'accès des utilisateurs dépendant de son périmètre et mène les actions correctives en cas d'anomalie constatée.

L'ASSI d'unité valide

- si nécessaire, les autorisations d'accès aux applications dotées d'un droit d'accès spécifique.

L'Officier de sécurité valide :

- le processus et le niveau d'habilitation des personnels ;
- le droit d'accès, du personnel, en fonction des obligations de missions, aux locaux identifiés dans la protection du patrimoine scientifique et technique et dans la protection du secret de la défense nationale.

La filière informatique gère :

- l'inventaire, l'affectation et la réforme des matériels informatiques professionnels confiés à un utilisateur sous le contrôle du chef d'unité.

En cas de mutation (avec changement d'unité), la réaffectation du même compte informatique est tolérée s'il s'accompagne d'un processus garantissant la révocation automatique de l'ensemble des droits. En l'absence d'un processus garantissant la révocation des droits, la destruction du compte historique et la création d'un nouveau compte est exigée. Une période ne pouvant excéder 3 mois est tolérée pour la cohabitation des comptes ou des accès historiques et actuels de l'utilisateur pour favoriser la transition sans interruption de service.

3.1.6 Gestion du personnel non permanent

Est considéré comme personnel non permanent, toute personne devant accéder au système d'information du CEA et dont le CEA n'est pas employeur.

Le personnel non permanent est de type « travailleur » lorsque sa relation avec le CEA est régie par un contrat (prestation, collaboration scientifique ou autre) qui indique que la charte d'utilisation des moyens informatique et la présente PSSI lui sont applicables. Ce personnel peut en tant que de besoin disposer d'un compte informatique, à condition d'être préalablement titulaire d'un avis de sécurité favorable suite à une procédure d'enquête administrative (l'obtention de cet avis s'effectue suivant les modalités prescrites par l'officier de sécurité). Le compte informatique respecte la présente PSSI (compte nominatif et personnel, durée de validité limitée à la durée de la collaboration...).

En cas d'avis défavorable des officiers de sécurité, aucun compte ne peut être octroyé à un personnel non permanent, et tout compte qui lui aurait été affecté préalablement à l'avis défavorable serait immédiatement suspendu.

Les autres personnels non permanents sont de type « visiteur » (exemple : rencontre commerciale, visite scientifique d'une installation...) et ne disposent pas d'accès aux systèmes d'information CEA, à l'exception des ressources explicitement prévues à l'accueil des visiteurs (comme le Wifi destiné aux visiteurs).

Référence du document : RSSN-SSI-01-01	Page 17 / 62
Titre du document : PSSI CEA	Indice : 9

4. INTÉGRATION DE LA SSI DANS LE CYCLE DE VIE DES SYSTÈMES D'INFORMATION

4.1 Cartographie des SI

4.1.1 Inventaire des ressources informatiques

L'ensemble des ressources informatiques est inventorié par le STIC du centre. L'ASSI de centre veille à l'application stricte de cette mesure. Le STIC soumet périodiquement cet inventaire à l'ASSI d'unité pour qu'il en vérifie la justesse et puisse faire procéder aux mises jours nécessaires.

Cet inventaire doit tendre à être exhaustif, avec une mise à jour mensuelle puis à terme hebdomadaire, et comprend l'ensemble des ressources informatiques (systèmes gérés par l'unité, physiques ou virtuels, systèmes industriels, systèmes bureautiques ou scientifiques, systèmes de communication ou de sécurité, systèmes physiques et virtuels, éléments d'infrastructures, liaisons, réseaux, ...) quelle que soit leur appartenance (CEA ou autres entités hébergées, prestataires extérieurs, etc.)

L'inventaire comprend :

- l'identification unique des matériels (dont la typologie est définie en préambule),
- les caractéristiques en termes de connectivité réseau,
- les caractéristiques matérielles (Marque, modèle et constructeur),
- la configuration logicielle (Système d'exploitation et applicatifs),
- l'attribution : géographique (localisation) et personnel/unité.

L'inventaire est tenu à jour pour être exact sur une période mensuelle.

Tous les postes de travail et les serveurs doivent être référencés dans un inventaire national pour chaque zone de sécurité, sauf exception motivée uniquement pour des raisons de sécurité ou d'homologation (cas des réseaux isolés classifiés de défense ou des systèmes industriels critiques dont l'inventaire demeure interne au périmètre de l'homologation mais demeure consultable par l'ASSI de centre et par le RSSI sur simple demande).

Les éléments d'architecture réseau et de sécurité en charge de la protection du CEA avec les réseaux opérés par des tiers (réseaux publics, Renater...) font l'objet d'un inventaire particulier détenu par la DSI et mis à jour par les USCI.

L'inventaire des moyens informatiques gouvernementaux (ISIS, THEOREM, ...) et des articles contrôlés de la sécurité des systèmes d'information [ACSSI] est assuré par l'OCSSI désigné par l'AQSSI, comme gestionnaire ACSSI.

4.1.2 Cartographie

La cartographie précise pour chaque centre, les centres de données⁹, les architectures réseaux, les points névralgiques et la sensibilité des informations manipulées. Cette cartographie s'appuie sur les inventaires des ressources informatiques mais apporte les informations sur les objectifs des systèmes hébergés et sur les interfaces entre les différents systèmes.

La cartographie est créée et maintenue par les STIC de chaque centre, et validée par les ASSI de centre qui en vérifient la pertinence. Elle est mise à jour à chaque évolution notable du système d'information du centre. Elle est consolidée au niveau des USCI et de la DSI

Elle est tenue à jour et à disposition permanente du RSSI pour une consolidation nationale.

⁹ Datacenter

Référence du document : RSSN-SSI-01-01	Page 18 / 62
Titre du document : PSSI CEA	Indice : 9

4.2 Qualification et protection de l'information

4.2.1 Qualification des informations

Toutes les informations et tous les systèmes d'information font l'objet d'une évaluation de la confidentialité des informations traitées. Cette évaluation est désignée sous le terme générique de « qualification des informations ».

La qualification des informations est confiée à l'Officier de sécurité. L'ASSI vérifie l'adéquation des mesures de protection mises en œuvre conformément au niveau de qualification de l'information identifiée.

La qualification des informations repose sur la grille de classification suivante :

- SECRET DEFENSE :
Informations relevant de la défense nationale, au sens du code de la défense.
- CONFIDENTIEL DEFENSE :
Informations relevant de la défense nationale, au sens du code de la défense.
- CONFIDENTIEL CEA :
Informations stratégiques et très confidentielles, au sens de la NIG 312.
- DIFFUSION RESTREINTE :
Informations sensibles dont le CEA entend restreindre la diffusion, au sens de l'IGI 1300.
- DIFFUSION ORDINAIRE :
Informations destinées à un usage interne, au sens commun.
- DIFFUSION PUBLIQUE :
Informations validées par l'autorité de publication pour diffusion, au sens de la NIG Publication de travaux à caractère scientifique et technique [NIG 660].

Une information, propriété du CEA, est en l'absence de marquage particulier, considérée comme « diffusion ordinaire ». Cette qualification « diffusion ordinaire » doit être explicitement indiquée sur les documents par une mention type : « *Ce document est la propriété du CEA et ne peut être utilisé, reproduit ou communiqué en dehors du CEA sans l'accord de son émetteur.* »

4.2.2 Protection des informations

L'utilisateur est responsable de la protection des informations qu'il manipule ou qu'il consulte dans le cadre de ses fonctions, selon leur niveau de sensibilité et tout au long de leur cycle de vie, depuis la création du brouillon jusqu'à son éventuelle destruction.

Les usages du système d'information conformes au niveau de protection de l'information font l'objet d'un « *Guide Pratique SSI – Protection des informations* ».

La conformité RGPD fait l'objet d'un document de politique interne qui s'applique pour la partie concernant la sécurité informatique des données personnelles.

4.3 Gestion des risques et homologation de sécurité

4.3.1 Homologation de sécurité des systèmes d'information

Compte tenu de la qualification des informations, les systèmes d'information doivent faire l'objet d'une homologation formelle suivant un processus validé par le DSSN – Autorité d'homologation.

Les modalités d'obtention de l'homologation sont définies par le RSSI dans le processus d'homologation.

Le processus d'homologation est décrit dans le « *Guide – Homologation* ».

Référence du document : RSSN-SSI-01-01	Page 19 / 62
Titre du document : PSSI CEA	Indice : 9

4.4 Maintien en condition de sécurité

4.4.1 Intégration de la sécurité dans les projets

L'intégration de la sécurité informatique dans les projets (informatiques et métiers) doit être effectuée le plus en amont possible. Il est de la responsabilité du responsable hiérarchique ou du chef de projet de prendre en charge l'analyse de risque avec l'assistance de l'ASSI d'unité.

Le rôle de l'ASSI d'unité est d'identifier la nature du projet, de prendre en compte le niveau de sensibilité des informations traitées défini par l'officier de sécurité, les intervenants et les interfaces avec des systèmes d'information existants. Les documents « Étude d'impact » sont mis en œuvre pour aider dans l'élaboration de ce processus.

Le processus d'analyse de risque est décrit dans le « *Guide – Homologation* »

L'ASSI d'unité vérifie l'adéquation des moyens informatiques mis en œuvre avec les objectifs de sécurité (Confidentialité, Intégrité, Disponibilité, Traçabilité). Si les moyens informatiques font déjà l'objet d'un profil de sécurité, les moyens de protection mis en œuvre sont décrits dans un dossier d'exploitation (sous la responsabilité des STIC). Ils doivent être en conformité avec les objectifs de sécurité du projet spécifiés dans l'étude d'impact. La qualification des moyens de protection est définie par le RSSI dans le cadre de profils de sécurité qui définissent les spécifications nécessaires et suffisantes pour qu'un système d'information puisse héberger un type de service (Site collaboratif interne, site de publication internet, site collaboratif extérieur).

Ce processus donne lieu à une vérification préalable par l'ASSI de l'unité.

Ce processus donne lieu à une autorisation formelle de l'AQSSI pour les systèmes d'informations :

- relevant d'une homologation classifiée de défense.

Ce processus donne lieu à une autorisation formelle du RSSI pour les systèmes d'informations :

- relevant d'une homologation Confidentiel CEA ou Diffusion Restreinte,
- pour les hébergements externalisés,
- lorsque les moyens mis en œuvre nécessitent de déroger à la présente PSSI.

Les projets nationaux présentés en CSI font l'objet d'une prise en compte de la SSI dans les études d'opportunités réalisées avant la prise de décision (Analyse de la valeur – Thématique – Maîtrise des risques).

4.4.2 Mise en œuvre au quotidien de la SSI

La présente PSSI vise à obtenir une couverture exhaustive de la protection du système d'information¹⁰. En particulier,

- durant les phases de conception, par le biais des analyses de risques et de l'identification des objectifs de sécurité par l'ASSI d'unité,
- durant les phases d'exploitation, par le rôle actif de la filière informatique dans le maintien en condition de sécurité et par celui de la chaîne fonctionnel sécurité pour le traitement des incidents et des non conformités,
- durant les phases de retrait, par les procédures de mise au rebut spécifiées dans la présente PSSI.

4.4.3 Tableau de bord SSI

Le RSSI est responsable de l'élaboration du pilotage de la SSI au CEA. Il définit les indicateurs SSI retenus pour l'élaboration des tableaux de bord. Ces indicateurs sont réactualisés de manière mensuelle et sont tenus à la disposition de l'AQSSI et des ASSI de centre pour leur périmètre.

Le RSSI présente également le tableau de bord SSI en CSI.

¹⁰ Y compris des codes de développement ou codes de calcul

Référence du document : RSSN-SSI-01-01	Page 20 / 62
Titre du document : PSSI CEA	Indice : 9

4.5 Produits et services qualifiés ou certifiés

4.5.1 Acquisition de produits et services de confiance

Toutes les prestations externes d'audit de sécurité des systèmes d'information sont soumises à la validation du RSSI. Les prestataires extérieurs d'audit de la sécurité des systèmes d'information [PASSI] doivent faire l'objet d'une qualification PASSI auprès de l'ANSSI.

La mise en place de système de supervision traitant des informations nominatives est soumise à l'accord préalable de l'AQSSI.

Dans le processus de passation des marchés concernant l'acquisition de matériels de sécurité (garde-barrière, VPN, outil de chiffrement, terminaux sécurisés...) des clauses particulières doivent être intégrées pour favoriser l'acquisition des produits labellisés par l'ANSSI¹¹. Il en est de même pour toutes les prestations d'assistance à la mise en œuvre de ces outils de sécurité qui doivent mettre en avant la labellisation des prestataires par l'ANSSI.

L'acquisition de produits et de services de sécurité non labellisés doit faire l'objet d'une dérogation formelle du RSSI, elle ne peut être justifiée que par l'absence de produits labellisés répondant au cahier des charges.

4.6 Maîtrise des prestations

4.6.1 Clauses de sécurité

Toute prestation dans le domaine des systèmes d'information doit faire l'objet d'une évaluation du niveau de sensibilité du marché sous la responsabilité de l'officier de sécurité.

Toute prestation dans le domaine des systèmes d'information doit intégrer contractuellement le respect de la présente PSSI, à minima, dans le cadre de la prestation réalisée.

La mise en œuvre d'un système externalisé est soumise au préalable au RSSI pour accord suite à une analyse de risque (cf. § 4.4.1).

La prise en compte de la présente PSSI doit être matérialisée par la rédaction et la validation contractuelle d'une annexe de sécurité conformément aux exigences de l'IGI 1300.

4.6.2 Suivi et contrôle des prestations fournies

Outre le contrôle de la réalisation du marché et la conformité des prestations avec le cahier des charges, bien que cela ne relève pas de sa responsabilité, l'ASSI a pleine autorité pour réaliser des opérations de contrôle sur les prestations fournies pour réaliser des opérations de contrôles sur le respect des exigences de la PSSI lorsque les prestations sont réalisées sur des ressources CEA ou sur le respect du plan d'assurance sécurité lorsque celui-ci a été élaboré.

4.6.3 Analyse de risques

Toute prestation dans le domaine de la sécurité des systèmes d'information réalisée sur site CEA relève de la présente PSSI qui en définit les modalités d'exécution.

Tout usage d'un système externalisé, doit faire l'objet d'une analyse de risque et d'un processus d'homologation et doit être formalisée par un plan d'assurance sécurité (PAS).

Les prestations (commerciales ou à titre gracieux) réalisées sur des ressources informatiques externalisées et ne bénéficiant pas de la protection du système d'information CEA doivent faire l'objet d'une analyse préalable par l'officier de sécurité pour la protection des informations, le correspondant à la protection des données en cas de traitement de données personnelles et par l'ASSI pour les adhésions éventuelles avec le système d'information CEA (procédures d'échanges automatisées, mises en œuvre de référentiel d'authentification commun et supervision de l'activité du système externalisé).

¹¹ Comme le guide « Achat de produits de sécurité et de services de confiance » <http://www.ssi.gouv.fr>

Référence du document : RSSN-SSI-01-01	Page 21 / 62
Titre du document : PSSI CEA	Indice : 9

4.6.4 Hébergement et clauses de sécurité

Les informations de niveau « Diffusion Restreinte » traitées dans le cadre de la prestation doivent être traitées sur des systèmes homologués et hébergées sur le territoire national et en conformité avec l'instruction interministérielle 901.

Les informations de niveau « Confidentiel CEA » ou classifiées de défense doivent être traitées sur des systèmes homologués après l'établissement d'un marché de nature à définir formellement les conditions d'exécutions du marché par le biais d'une annexe de sécurité. Ce type de marché est soumis à l'accord préalable de l'officier de sécurité.

Pour l'ensemble des autres niveaux d'information (diffusion ordinaire ou diffusion publique) :

L'hébergement externalisé¹² de données CEA pour traitement, doit faire l'objet :

- d'une homologation DSSN,
- d'un plan d'assurance sécurité définissant les exigences de sécurité du titulaire pendant toute l'exécution du marché, et d'une homologation,
- d'un contrat au titre d'une passation de marché (y compris UGAP).

Le Plan Assurance sécurité réalisé¹³ sous la responsabilité par l'ASSI d'unité, prend en compte les spécificités de l'externalisation comme :

- le risque lié à la perte de maîtrise du système,
- le risque lié à la localisation des données,
- le risque lié aux données confidentielles,
- le risque lié aux données à caractère personnel,
- le risque inhérent aux interventions distantes,
- le risque lié à l'hébergement mutualisé.

En l'absence de passation de marché formalisée (souscription d'une offre commerciale cloud), l'usage d'un système externalisé¹⁴ est toutefois soumis à l'accord, du RSSI, et des services juridiques du centre, en charge de l'analyse des conditions générales d'utilisation (CGU) pour vérifier au préalable la conformité avec le traitement d'informations professionnelles. L'Officier de sécurité et l'ASSI sont sollicités pour vérifier l'adéquation entre le niveau de sensibilité des informations et le niveau de sécurité du système externalisé.

Dans les autres cas, une analyse préalable des conditions d'usage, par l'ASSI de direction, pour vérifier au préalable la conformité avec le traitement d'informations professionnelles devra être intégrée au processus d'homologation.

¹² Se référer au guide « Externalisation et sécurité des systèmes d'information » <http://www.ssi.gouv.fr>

¹³ Peut-être sous-traité, comme livrable du projet / contrat

¹⁴ Exemple : offre de type Cloud grand public ou professionnel

5. SÉCURITÉ PHYSIQUE

5.1 Sécurité physique des locaux abritant les SI

5.1.1 Règles générales

Les systèmes d'information du CEA sont hébergés dans des locaux dont le niveau de sécurité physique respecte un principe de zonage. Le zonage définit une emprise géographique dont les moyens de protection sont proportionnés à la menace.

On distingue les niveaux suivants :

Protection physique	Enquête administrative	Règlement Intérieur	Contrôle d'accès	Gardiennage
Niveau 0	Aucune	Non	Aucun	Aucun
Niveau 1	Aucune ou selon termes du contrat	CEA	Spécifique Opéré par un tiers sous contrat	Opéré par un tiers sous contrat
Niveau 2	Oui	CEA	CEA Mode : Liste noire	FLS
Niveau 3	Oui	CEA	CEA Mode : Liste blanche	FLS

- Niveau 0 : sans protection ou d'accueil du public ou dont la responsabilité n'incombe pas au CEA,
- Niveau 1 : Type plateforme extérieure, sous politique CEA mais dont les dispositifs de contrôle et de gardiennage sont opérés par un tiers sous contrat ou régi par une convention.
- Niveau 2 : Type centre, sous politique CEA et dont l'accès des personnels est soumis à une enquête administrative préalable. Tous les personnels titulaires d'un badge CEA sont potentiellement autorisés à pénétrer dans cette zone sauf contre-indication (liste noire des personnels non autorisés). Tout personnel CEA non interdit est autorisé à pénétrer dans la zone (mode liste noire ou implicite).
- Niveau 3 : Type installation, seuls les personnels dûment autorisés de manière nominative peuvent pénétrer dans la zone. Il est possible de fournir la liste exhaustive des personnels autorisés à pénétrer dans la zone. Tout personnel CEA non autorisé est interdit à pénétrer dans la zone (mode liste blanche ou explicite).

De manière générale, ces zones définissent le niveau de protection des « bureaux » ou locaux affectés aux postes de travail des utilisateurs concernés, cependant au sein de ces zones, certains locaux peuvent bénéficier d'un régime particulier et sont tenus de respecter des exigences spécifiques, il s'agit des :

- locaux techniques,
- salles de réunion,
- locaux de travail des personnels en charge de l'exploitation et de l'administration du système d'information,
- centres informatiques.

5.1.2 Règles de sécurité des zones d'accueil du public

Les prises réseaux et équipements (routeurs, switches, armoire de brassage, ...) desservant les réseaux du CEA sont proscrits dans les zones de niveau 0 (sans protection ou d'accueil du public) en dehors des prises et équipements prévus pour la Zone Hébergement. Les systèmes d'information utilisés dans ces zones sont considérés au même titre que les équipements nomades du CEA et doivent avoir été traités en tant que tel.

Référence du document : RSSN-SSI-01-01	Page 23 / 62
Titre du document : PSSI CEA	Indice : 9

5.1.3 Protection des informations sensibles au sein des zones d'accueil

Le traitement d'information sensible à partir du niveau « Diffusion Restreinte » est proscrit dans les zones d'accueil.

Les matériels doivent être équipés de dispositifs antivol limitant les risques d'enlèvement ou d'arrachage (câbles, ...).

Les ports USB non utilisés doivent être neutralisés et rendus inopérants, ou physiquement rendus inaccessibles aux visiteurs.

Les unités centrales des postes informatiques doivent être scellées avec des étiquettes de sécurité permettant de détecter toute ouverture. Ces unités respectent les mesures de protection applicables au matériel nomade.

5.1.4 Règles de sécurité des locaux techniques

De manière générale, quel que soit le niveau de protection du bâtiment, les locaux techniques doivent être verrouillés et ne permettre l'accès qu'aux seuls personnels en charge de l'exploitation. Les locaux de travail des personnels en charge de l'exploitation et de l'administration sont placés sous la responsabilité de ces personnels en leur présence et doivent être verrouillés en leur absence.

Lorsque le local technique est mutualisé avec d'autres organismes que le CEA, les équipements CEA doivent être isolés dans des armoires verrouillées assurant que seul le personnel autorisé peut y avoir accès.

5.1.5 Protection des câbles électriques et de télécommunication

La protection des câbles électriques est de la responsabilité des services techniques du centre. Dans le cadre de l'homologation d'un système, l'ASSI peut être amené à contrôler la qualité du câblage en commanditant des mesures vis-à-vis des rayonnements compromettants.

Le plan de câblage des réseaux et plus généralement des courants faibles doit être tenu à jour par le STIC ainsi que la localisation des locaux techniques de desserte. Dans le contexte d'une homologation, il est de la responsabilité de l'autorité d'emploi d'assurer la protection de ces câbles conformément au dossier d'homologation.

5.1.6 Contrôles anti-piégeages

Les locaux aptes à traiter des informations à partir du niveau « Confidentiel CEA ou CONFIDENTIEL DEFENSE » doivent faire l'objet de campagnes de sécurisation contre les dispositifs d'écoute et d'interception (recherche de micro espion, d'émetteur caché...). L'ASSI de centre tient à jour l'inventaire de ces locaux (bureaux, salles de réunion, salles serveurs...) et rend compte au RSSI pour l'élaboration d'une planification périodique de ces opérations (Certaines opérations pouvant être réalisées par DSSN/SPPS). Ces locaux doivent bénéficier d'un contrôle d'accès adapté pour garantir leur intégrité entre deux campagnes de vérification (la fréquence des campagnes est à minima la même que celle du processus de ré-homologation).

Les locaux aptes à traiter des informations classifiées de défense doivent faire l'objet de campagnes de mesures contre les rayonnements compromettants (TEMPEST) mises en œuvre par les services compétents de l'état sur demande auprès du DSSN.

Référence du document : RSSN-SSI-01-01	Page 24 / 62
Titre du document : PSSI CEA	Indice : 9

5.2 Sécurité physique des centres d'information

5.2.1 Règles générales

Découpage des locaux en zones de sécurité

Les centres d'information, communément appelés salles informatiques ou salles serveurs, hébergent les ressources informatiques (traitement, stockage et communication) mutualisées pour un ensemble d'utilisateurs. Tous les centres d'information doivent bénéficier d'une protection physique de niveau 3.

Les autorisations d'accès pour accéder à ces centres d'information sont délivrées suivant les conditions définies par l'Officier de sécurité en fonction de la nature des activités hébergées.

Convention de service en cas d'hébergement tiers

Lorsqu'un tiers gère tout ou partie des locaux du centre informatique, une convention de service doit être établie avec le CEA afin de spécifier les responsabilités mutuelles en matière de sécurité. Les centres informatiques dont tout ou partie des locaux sont gérés par un tiers sont de niveau maximum 1, ils ne peuvent héberger l'Intranet CEA en dehors du processus d'homologation des locaux pour accueillir l'Intranet CEA spécifié par DSSN/SPPS.

5.2.2 Règles de sécurité aux zones internes

Contrôle d'accès physique

L'accès aux centres d'information repose sur un dispositif de contrôle d'accès qui limite la population aux seuls personnels autorisés en charge de l'exploitation et des visiteurs accompagnés par ce personnel.

Délivrance des moyens d'accès physique

Le contrôle d'accès des centres informatiques s'appuie sur le processus de délivrance du badge CEA. Seules les personnes titulaires d'un badge CEA nominatif et en cours de validité peuvent accéder au centre informatique. Lorsqu'il est fait usage d'un autre badge, un processus d'échange avec le badge CEA doit être mis en œuvre pour bénéficier d'un processus de délivrance équivalent. Lorsqu'il est fait usage d'un autre dispositif (clé), un processus formel doit être mis en œuvre qui assure la traçabilité et la gestion des personnels autorisés (ajout et retrait).

Les personnels disposant d'un badge visiteur doivent être accompagnés pour accéder aux centres d'information (exemple : cas d'une intervention de maintenance ponctuelle).

Traçabilité des accès

Tous les dispositifs de contrôle d'accès des centres informatiques doivent journaliser et conserver sur une période minimale d'un an, les accès au centre d'information. Ces journaux conservent l'identification du dispositif ou badge CEA utilisé, la date et l'heure d'entrée dans le centre d'information. Ces journaux sont tenus à la disposition de l'officier de sécurité du centre et du chef d'installation.

5.2.3 Règles de sécurité des salles informatiques et locaux techniques

Le chef d'installation assisté par les services techniques du centre doit mettre en œuvre et maintenir en condition opérationnelle les dispositifs support du centre d'information, en particulier :

- les moyens mis en œuvre pour garantir l'alimentation électrique des centres d'information,
- les dispositifs de climatisation nécessaires pour prévenir toute surchauffe des équipements,
- les dispositifs de lutte contre l'incendie avec les procédures de réaction en cas d'incendie, validées par la FLS du centre,
- les dispositifs de lutte contre les voies d'eau, une étude de risque doit être réalisée pour évaluer le risque de dégâts des eaux dans les centres d'information.

Référence du document : RSSN-SSI-01-01	Page 25 / 62
Titre du document : PSSI CEA	Indice : 9

5.3 Sécurité du système d'information de sûreté

La sécurité des systèmes industriels intervenant dans les missions vitales du CEA fait l'objet de mesures spécifiques détaillées dans le document PSSI-S2IV.

Les Systèmes d'Information d'Importance Vitale [S2IV] bénéficient de politiques d'emploi de sécurité complémentaires définies réglementairement par décrets et déclinées dans le cadre de leur processus d'homologation.

Les systèmes industriels sont soumis à l'Instruction technique d'emploi (ITE), qui précise les conditions dans lesquelles un système industriel peut être raccordé au système d'information du CEA.

À défaut d'appliquer cette ITE, un système industriel est considéré comme isolé et n'admet aucune télémaintenance.

Chaque centre doit mettre en œuvre les plateformes d'accueil (Réseau, Serveurs de maintenance, centre de supervision, Postes d'administration...) spécifiques et dédiées à l'intégration des systèmes industriels.

Référence du document : RSSN-SSI-01-01	Page 26 / 62
Titre du document : PSSI CEA	Indice : 9

6. SÉCURITÉ DES RÉSEAUX

6.1 Usage sécurisé du réseau CEAnet

On désigne par réseau CEAnet, l'ensemble des réseaux placés sous la responsabilité du CEA à l'exception des réseaux faisant l'objet d'une homologation classifiée de défense. CEAnet désigne en particulier les espaces d'adressage IP alloués à l'organisme par les opérateurs de l'internet et par voie de conséquence, dont l'usage engage la responsabilité du CEA.

6.1.1 Systèmes autorisés sur le réseau

Seuls les équipements gérés et configurés conformément aux règles de la PSSI, et respectant les normes définies par la DSI et mises en œuvre par les STICs sont autorisés à être connectés sur le réseau CEAnet.

Les équipements appartenant à des tiers et/ou qui ne peuvent se conformer à ces prescriptions techniques, dans le cadre d'une collaboration ou d'une prestation, doivent être connectés en Zone Hébergement.

6.1.2 Interconnexion avec des réseaux externes

L'interconnexion du réseau CEAnet avec des réseaux externes (Internet ou autres réseaux publics ou qui n'est pas sous la maîtrise d'ouvrage du CEA) est exclusivement réalisée au travers des points d'accès opérés par les USCI, sous le contrôle de la DSI.

Le raccordement physique quel qu'il soit (modem, carte 3/4G/5G, liaison spécifique) ou logique (établissement d'un tunnel de type VPN à travers le réseau CEAnet pour se raccorder au réseau d'une entité extérieure) est une violation de la présente PSSI, sauf dérogation formelle du RSSI.

6.1.3 Filtrage réseau des flux sortants et entrants

Tous les flux de communication entrants et sortants du réseau CEAnet, et les flux interzones (voir § 6.2.1), sont supervisés et filtrés pour être limités aux usages sécurisés et conformes à la protection du réseau CEAnet, ils sont également analysés en profondeur et journalisés pour détecter les violations à la PSSI et les attaques de compromission ou d'exfiltration de données éventuelles.

La politique de filtrage est établie par la DSI et mise en œuvre par les USCI après validation par le RSSI.

Les flux de communication peuvent être stoppés sans préavis pour des raisons de sécurité dans le cadre de la gestion d'incidents par les équipes en charge de la résolution de l'incident.

Sur décision du CSI, du CCC ou sur décision du RSSI dans le cadre du traitement des incidents de sécurité, ou de leur remédiation, des périodes de filtrage restrictives seront mises en œuvre, pour adapter la protection du réseau CEAnet à l'actualité de la cyber menace, ou bien pour réduire la surface potentielle d'attaque lorsque l'exploitation DSI/USCI/STIC est en équipe réduite (période de fermeture collective par exemple).

6.1.4 Protection des informations

Les informations doivent être protégées en confidentialité et en intégrité par du chiffrement.

Le niveau de robustesse et de confiance des outils mis en œuvre repose sur le schéma de qualification de l'ANSSI¹⁵.

Qualifié renforcé :

- Classifié de défense
- Confidentiel CEA

Qualifié Standard

- Diffusion Restreinte

La qualification élémentaire est recommandée pour le niveau Diffusion ordinaire, mais ne permet pas à elle seule de traiter les éléments de niveau supérieur.

¹⁵ <http://www.ssi.gouv.fr/entreprise/qualifications/>

6.2 Usage sécurisé des réseaux locaux

6.2.1 Cloisonnement en sous-réseaux de sécurité homogènes

Zones Réseaux

Pour garantir la protection de l'information traitée sur le réseau CEAnet, celui-ci est cloisonné en différentes zones. Chaque zone constitue une partie du réseau CEA sur laquelle les moyens techniques mis en œuvre pour assurer la protection de l'information sont identiques, définissant ainsi un profil de protection homogène et appliqué à toutes les ressources hébergées dans une même zone. Les caractéristiques d'une zone sont principalement le niveau maximum de confidentialité qu'elle est habilitée à traiter et la population pouvant y accéder.

Les réseaux CEAnet sont cloisonnés suivant les zones suivantes (de la plus exposée à la plus sécurisée) :

- Zone Hébergement : pas de protection d'intégrité, de disponibilité ou de confidentialité,
- Zone Extranet : pas de protection de confidentialité,
- Zone Partenaires : informations sensibles (max DR) pour des partenaires identifiés,
- Zone Intranet : informations sensibles (max DR) réservées à des titulaires d'un badge CEA (hors visiteur),
- Réseaux classifiés : réseaux sans aucune interconnexion physique, ou isolés via diode.

Toutes les communications interzones :

- passent exclusivement par les passerelles nationales maîtrisées par l'USCI ;
- et donnent lieu à une supervision exhaustive des flux de communication traversant ces passerelles.

Zone CEAnet	Réseaux classifiés	INTRANET	PARTENAIRES	EXTRANET	HEBERGEMENT
Confidentialité maximale	Dépend du niveau d'homologation SD, CD ou CCEA	Diffusion Restreinte	Diffusion Restreinte	Diffusion Ordinaire	Non CEA
Interconnexion internet	Interdit	En sortie vers internet et les autres zones.	En entrée depuis internet	En entrée et sortie avec internet	En sortie vers internet.
Objectifs SSI majeurs	Confidentialité Authentification	Confidentialité Authentification	Confidentialité, Authentification Contrôle d'accès des collaborateurs extérieurs	Intégrité	Aucun
Cas d'usage les plus fréquents	Protection des activités classifiées de défense	Protection des infrastructures internes CEA Protection du Patrimoine	Collaboration sensible et protection du patrimoine	Communautés ouvertes, Services de publication	Wifi, Accueil des visiteurs et des organismes extérieurs

Une ressource informatique hébergée sur CEAnet n'appartient qu'à une seule et unique zone. Aucun système ou équipement informatique ne peut interconnecter ces différentes zones, à l'exception des ressources nationales opérées par les USCI et dédiées au transport et la sécurité de ces zones entre les différents sites du CEA et internet.

Les locaux pouvant héberger des ressources informatiques (locaux techniques, bureaux, salles de réunions, etc.) peuvent proposer des raccordements aux différentes zones, à condition que ces raccordements soient mutuellement exclusifs, et que les règles d'accès à la zone la plus sécurisée s'appliquent à l'ensemble des personnes pouvant accéder au local.

Référence du document : RSSN-SSI-01-01	Page 28 / 62
Titre du document : PSSI CEA	Indice : 9

Les communications entre zones font l'objet d'un contrôle d'accès et contrôle de flux générique et homogène dont les principes sont : la réduction des flux au strict minimum nécessaire, la protection de l'information en transit conformément au niveau de confidentialité maximum traitée et la restriction d'accès aux seuls personnels autorisés. Seuls sont autorisés les flux initiés depuis la zone la plus sécurisée vers la zone la plus exposée.

Les seules dérogations admises à cette règle sont, les flux :

- de supervision,
- de remontée des journaux,
- de sauvegarde,
- de données unidirectionnels nécessaires au maintien en condition de sécurité de la zone la plus sécurisée, et traversant une diode.

Au sein de ces zones de sécurité réseaux, des profils plus restrictifs sont mis en œuvre pour renforcer la protection des ressources qu'ils hébergent (ces profils ne peuvent en aucun cas être une condition d'assouplissement du contrôle d'accès générique appliqué à la zone). Il s'agit de « bulles » mises en œuvre au sein d'une zone notamment pour assurer la protection :

- d'une unité nécessitant des besoins de protection renforcés,
- des serveurs et des éléments d'infrastructures techniques,
- des systèmes et processus industriels,
- des postes et ressources utilisés pour l'administration et l'exploitation,
- du reste de la zone lorsque les ressources souffrent d'une vulnérabilité spécifique (systèmes d'exploitation obsolètes, ressources incompatibles avec des protections génériques).

Niveaux de sécurité

Pour assurer le maintien de la sécurité de ces zones, chaque zone dispose de bulles spécifiques pour :

- La protection des postes d'administration déclinée suivant la criticité des rôles d'administration :
 - o Rouge, pour lesquels une atteinte conduit à un détriment pour toute la zone (les services d'infrastructures et de sécurité nationaux),
 - o Jaune, pour lesquels une atteinte conduirait à un détriment pour l'ensemble du centre (les serveurs d'infrastructure du centre, les dispositifs de protection réseau du centre),
 - o Vert, pour lesquels une atteinte conduirait à un détriment pour les utilisateurs du centre (les administrateurs en charge du support utilisateurs et de la gestion des postes de travail).
- La protection des serveurs informatiques :
 - o Rouge : serveurs d'infrastructure et de sécurité nationaux,
 - o Jaune : serveurs d'infrastructure du centre,
 - o Vert : postes de travail et serveurs destinés au maintien en condition de sécurité de ces postes.
- L'isolation des postes non conformes à la politique de la zone.

Chaque « Bulle » est dédiée à un seul type d'usage à la fois (poste d'administration, serveurs, poste utilisateurs, téléphonie, ...) et ne relève que d'un seul niveau de sécurité (Blanc, Vert, Jaune ou Rouge).

Par convention, on considère comme poste blanc, l'ensemble des ressources de la zone qui ne justifient pas de bulle de protection particulière (typiquement les postes de travail des utilisateurs de la zone).

En dehors d'un contexte d'homologation spécifique, les réseaux isolés sont considérés comme appartenant à la zone Intranet et dans une bulle « isolée ».

Passerelle Internet

Toutes les communications entrantes et sortantes de CEAnet vers Internet passent exclusivement par les passerelles nationales maîtrisées par l'USCI.

Ces passerelles sont constituées d'éléments de confiance et assurent :

Référence du document : RSSN-SSI-01-01	Page 29 / 62
Titre du document : PSSI CEA	Indice : 9

- la mise en œuvre de la politique de protection de CEAnet,
- la supervision exhaustive des flux de communication à travers ces passerelles,
- la détection et le blocage éventuel de toutes signatures d'attaques connues ou de violation de conformité par rapport à la présente PSSI,
- la mise en œuvre ponctuelle d'opérations de « mise en quarantaine » sur incident ou sur risque potentiel de cyber menace.

Ces passerelles mettent en œuvre de manière préférentielle des outils labellisés ANSSI si ceux-ci sont disponibles et adaptés aux besoins techniques et fonctionnels.

Conditions d'emploi de la Zone Hébergement

La Zone Hébergement est destinée à l'accueil des ressources informatiques n'appartenant pas au CEA, telles que les postes des visiteurs, le matériel personnel des salariés ou les réseaux des entreprises hébergées sur des sites CEA.

Cet hébergement fait l'objet d'une convention formelle et/ou de conditions d'usages indiquant les limites d'utilisation de cet accès et les responsabilités des parties.

Les seules ressources informatiques du CEA admises en Zone Hébergement sont :

- les équipements sans-fils, tels que bornes Wifi, tablettes et smartphones, outils de déport d'écran, poste nomade, etc. (cf. § 6.4) ;
- les équipements ouverts ponctuellement sur internet pour en permettre la maintenance ;
- et les ressources nécessaires à la gestion et l'administration de ces équipements.

L'ouverture ponctuelle d'équipements sur internet dans le but de leur maintenance n'est possible que dans le cadre strict de « l'ITE Systèmes industriels ». En particulier, ces équipements ne doivent jamais être en service nominal dans cette zone et sont regroupés au sein de bulles « Maintenance » dédiées à cet usage. Les USCI/STIC doivent détecter et bloquer tout raccordement dont la durée serait jugée excessive par rapport aux besoins de maintenance.

6.2.2 Cloisonnement des ressources en cas de partage des locaux

Le partage des locaux de type bureaux avec des entités extérieures doit faire l'objet de mesure de cloisonnement pour maintenir la protection des actifs et des prises réseaux CEA. Ces mécanismes de partage doivent être évités au profit d'une maîtrise complète par le CEA de la protection de ses ressources. S'il s'avère nécessaire de les mettre en œuvre, la protection physique doit être évaluée par DSSN/SPPS. Cette évaluation donne lieu à un procès-verbal d'aptitude, préalable au déploiement du réseau CEAnet.

6.3 Accès spécifiques

Les raccordements spécifiques (carte 3G, liaison satellite, modem ou liaison spécifique, tunnel VPN, technique d'anonymisation comme TOR) sont proscrits sauf autorisation formelle du RSSI. De manière générale, toute technologie permettant de mettre en œuvre un canal de communication non maîtrisé et susceptible de contourner les dispositifs de protection réseau mis en œuvre est proscrite et constitue une violation de la présente PSSI.

6.4 Usage des réseaux sans fil

6.4.1 Mise en place des réseaux sans fil

L'usage des réseaux sans fil (bornes d'accès wifi CEA) est proscrit en dehors de la Zone Hébergement. Aucune ressource raccordée au réseau CEAnet par une interface filaire ne doit faire l'objet d'un raccordement simultané à des réseaux sans fil lorsqu'elle bénéficie de ce raccordement filaire.

De manière générale, tous Les périphériques disposant d'une interface sans fil de type Wifi activée ne doivent pas être raccordés au réseau CEAnet (Vidéo projecteur, Imprimante, Périphérique d'acquisition, déport d'affichage de type « Click'n Share », etc.). Les terminaux disposant d'une interface sans fil active de type 3G ou 4G ne doivent pas être raccordés au réseau CEAnet à l'exception de la Zone Hébergement.

Référence du document : RSSN-SSI-01-01	Page 30 / 62
Titre du document : PSSI CEA	Indice : 9

6.5 Sécurité des mécanismes de commutation et de routage

6.5.1 Protection contre les attaques en couches basses

La configuration des équipements réseau est de la responsabilité du STIC pour le centre et des USCI pour les infrastructures nationales. Les équipements sont configurés pour éviter les attaques usuelles par saturation ou empoisonnement de cache, et font l'objet d'une surveillance pour détecter et intervenir en cas de tentative d'attaque.

6.5.2 Protection des annonces de routage

La configuration et la protection des annonces de routage des espaces d'adressage internet alloués au CEA est de la responsabilité des USCI qui mettent en place une surveillance des annonces de routage, et des procédures permettant de réagir rapidement en cas d'incident.

6.5.3 Configuration sécurisée du protocole IGP

Les USCI sont responsables de la configuration du protocole IGP. Le protocole dynamique IGP n'est activé que sur les interfaces nécessaires à la construction de la topologie du réseau et est désactivé sur le reste des interfaces. La configuration du protocole s'accompagne systématiquement d'un mot de passe de type message-digest-key.

6.5.4 Configuration sécurisée des sessions EGP

Lors de la mise en place d'une session EGP avec un pair extérieur sur un média partagé, les USCI s'assurent que la session s'accompagne d'un mot de passe de type message-digest-key.

6.5.5 Conditions d'accès à l'administration

Les équipements réseaux et de sécurité du réseau CEAnet sont considérés comme des serveurs jaunes. À ce titre, ils ne sont exploitables que depuis des postes d'administration jaunes de l'Intranet. Ils sont opérés par les USCI.

Les équipements réseaux et de sécurité locaux du réseau CEAnet d'un centre sont considérés comme des serveurs jaunes. À ce titre, ils ne sont exploitables que depuis des postes d'administration jaunes de l'Intranet. Ils sont opérés par le STIC.

Les équipements réseaux et de sécurité restreints à une unité sont considérés comme des serveurs verts. À ce titre, ils sont exploitables depuis des postes d'administration verts ou des serveurs relais accessible depuis les postes blancs.

Les pare-feu sont toujours administrés depuis l'intérieur, à partir d'un profil de protection à minima identique aux ressources protégées par l'équipement (interface bénéficiant de la protection du firewall par rapport aux réseaux les plus exposés). Par dérogation, lorsque la mise en place de ressources d'administration dédiées ne se justifie pas, le pare-feu peut être administré depuis des postes d'administration jaunes extérieurs aux bulles protégées par le pare-feu, mais situés dans la même zone.

Les couches physiques des réseaux d'un centre peuvent être mutualisées par le biais de la virtualisation. Lorsque la mutualisation est mise en œuvre, les conditions d'accès à l'administration des VLANs doivent respecter les contraintes de sécurité les plus élevées des systèmes d'information concernés.

Un cas d'usage fréquent est la mise en œuvre d'un cloisonnement par VLAN de l'intranet, de plateforme d'accueil des systèmes industriels ou de la téléphonie sur IP.

La mutualisation des couches physiques par VLAN est proscrite entre les zones de CEAnet.

6.5.6 Durcissement des configurations des équipements réseau

La configuration des équipements réseau est de la responsabilité du STIC pour le centre et des USCI pour les infrastructures nationales. Ils s'assurent, chacun pour son périmètre, de la gestion des mots de passe et des certificats, de la désactivation des interfaces et des services inutiles.

Référence du document : RSSN-SSI-01-01	Page 31 / 62
Titre du document : PSSI CEA	Indice : 9

Ils modifient impérativement les mots de passe par défaut (y-compris les certificats par défaut ou auto-signés) présents dans les équipements livrés par le fournisseur.

6.6 Cartographie réseau

6.6.1 Documents d'architecture technique et fonctionnelle

La DSI est responsable de l'élaboration des documents d'architectures technique et fonctionnelle qui constitue CEAnet dans ses interfaces avec les accès extérieurs et de raccordements des différents sites CEA. Elle peut déléguer aux USCI tout ou partie de cette charge (identification des passerelles de sécurité et des équipements de routage, localisation des points de rattachement sur les différents centres, allocation des adresses CEAnet aux différents centres). L'ensemble de ces documents sont validés et contrôlés par la DSI.

Le STIC du centre est responsable de l'élaboration et de la mise à jour de tous les documents d'architectures technique et fonctionnelle sur son périmètre (identification des bâtiments, localisation des locaux techniques de distribution, plan de câblage sur le périmètre du centre, répartition des adresses réseaux sur les périmètres de ses unités).

Le STIC du centre est responsable de l'inventaire de ses ressources informatiques, notamment des serveurs :

- Identification du type de serveur,
- Évaluation de la sensibilité du serveur,
- Identification des flux techniques nécessaires vers les réseaux non maîtrisés,
- Protection et identification des postes d'administration,
- Interfaces avec les autres services (sauvegarde, supervision, inventaire, stockage...).

L'ASSI de centre veille à l'application stricte de ces actions.

L'inventaire est tenu à jour pour être exact sur une période de 8 jours ouvrés.

Référence du document : RSSN-SSI-01-01	Page 32 / 62
Titre du document : PSSI CEA	Indice : 9

7. ARCHITECTURE ET EXPLOITATION DES SI

7.1 Architecture sécurisée des centres informatiques

7.1.1 Principe d'architecture des centres informatiques

Les centres informatiques sont placés sous la pleine et entière responsabilité du directeur de centre. Ils sont à minima physiquement hébergés dans des locaux bénéficiant d'une protection physique de Niveau 3, lorsqu'il s'agit de l'INTRANET.

Les centres informatiques ont la capacité d'héberger des ressources de niveaux différents en respectant les règles de séparation inhérentes à leur sensibilité ou leur fonction :

- des serveurs ou ressources de système d'information homologués, des zones INTRANET, PARTENAIRES, EXTRANET ou HEBERGEMENT,
- des serveurs d'une même zone mais de différents niveaux de sécurité (serveurs jaunes, rouges et verts),
- des ressources utilisateurs,
- des ressources dédiées à l'administration et l'exploitation,
- des ressources dédiées à la conservation et au traitement des journaux d'activité.

7.1.2 Architecture de stockage et de sauvegarde

L'utilisation de ressources de stockage ou d'archivage externalisées est proscrite (en dehors du contexte de l'homologation pour un système d'information autorisé).

Pour chaque centre, les ressources dédiées au stockage ou à l'archivage sont réparties à minima sur deux bâtiments distincts mais de niveaux de protection physique équivalents, suffisamment éloignés pour éviter un sinistre conjoint et reliées par un réseau de type SAN dédié et physiquement séparé du réseau d'usage de ces ressources. Ces deux sites de stockage peuvent fonctionner en « sites chauds » avec répartition de charge ou en « site chaud – site froid » fonctionnement de type maître et secours. Chacun des deux sites peut permettre un maintien de l'activité dégradée.

Un troisième local sécurisé distinct doit être mis en œuvre sur le centre ou sur un centre déporté pour assurer le stockage longue durée des informations dont la préservation doit être garantie. Ce troisième site de stockage considéré comme « site mort » ne permet pas d'assurer le service aux utilisateurs mais assure la préservation du patrimoine CEA. À cet effet il dispose d'un jeu de données inerte réactualisé de manière mensuelle en cas de sinistre majeur sur l'établissement.

Réseau SAN de Stockage

Le Réseau SAN est un réseau technique de stockage de données, mutualisable entre les zones CEAnet (Hébergement, Partenaires, Extranet et Intranet) à condition d'avoir fait l'objet d'un dossier de sécurité présentant une analyse des risques spécifiques au SAN, les mesures de prises pour les limiter¹⁶, et le modèle d'administration mis en place.

Le réseau SAN met à disposition son stockage via les LUN (ou point d'accès au réseau SAN). Chaque LUN appartient à une seule et unique zone, et à un seul niveau de sécurité (Jaune, Vert, Blanc). De même, chaque zone SAN doit rester exclusive à une zone CEAnet. Les zones SAN ne doivent pas être mutualisées [pour des hôtes ayant des besoins de sécurité hétérogène](#).

Le réseau SAN est considéré comme sensible, isolé et absent de toute interface de communication directe avec le réseau CEAnet (en dehors des flux d'administration).

Lorsque le réseau SAN fournit du stockage à la zone Intranet, il est considéré de niveau Jaune et son administration se fait depuis des postes d'administration de l'Intranet (cf. § 6.2.1).

¹⁶ Typiquement, au niveau FABRIC, utilisation du zoning appliqué directement sur les ports des switches, ou à défaut par WWN et avec du LUN Masking au niveau de la baie (notion d'iGroup où sont associées le WWN de la carte HBA avec le WWN du LUN). Désactivation des ports des switches Brocade non utilisés. Supervision de l'infrastructure avec remontée centralisée des journaux.

Référence du document : RSSN-SSI-01-01	Page 33 / 62
Titre du document : PSSI CEA	Indice : 9

Le réseau SAN ne peut pas être utilisé pour le stockage ou la sauvegarde des systèmes Intranet de niveau Rouge.

7.2 Protection des informations sensibles

7.2.1 Protection des informations sensibles en confidentialité et en intégrité

Toutes les informations sensibles en transit ou en stockage doivent être protégées soit par une infrastructure d'hébergement homologuée (stockage et réseau), soit par un outil de chiffrement qualifié par ANSSI au niveau adapté.

	Classifié de défense	Confidentiel CEA	Diffusion Restreinte	Diffusion Ordinaire
Chiffrement	Agréé Qualifié niveau renforcé	Qualifié niveau renforcé	Qualifié niveau standard	Commercial

Toutes les informations sensibles en cours de traitement par l'utilisateur (donc accessibles en clair) doivent être protégées par le niveau d'homologation du terminal utilisé et par le respect des conditions d'usage spécifiées dans l'homologation par l'utilisateur. Les risques liés à la rémanence des informations sur le terminal et les interfaces (réseaux, supports amovibles ou impression) sont pris en compte dans le cadre de l'homologation.

7.3 Surveillance et configuration des ressources informatiques

7.3.1 Traçabilité des interventions sur le système

Toutes les interventions de maintenance sur les ressources informatiques (membre des USCI, STIC, sous-traitants, administrateurs fonctionnels des serveurs) doivent faire l'objet d'une traçabilité par le STIC et doivent être accessibles durant au moins un an. Le STIC doit mettre en œuvre des outils de gestion de tickets d'intervention pour assurer cette traçabilité. Cette traçabilité doit permettre d'identifier :

- la nature et la date de l'intervention,
- la ressource informatique impactée (serveur ou poste de travail),
- les personnels étant intervenus pour réaliser l'opération,
- les actions conduites,
- les conséquences constatées de l'intervention.

Les journaux d'activité relatifs à ces interventions doivent demeurer la pleine et entière propriété du CEA.

Une visibilité en lecture de l'ensemble des tickets et des journaux d'interventions doit être octroyée à l'ASSI de Centre.

7.3.2 Configuration des ressources informatiques

Les configurations déployées sur les ressources informatiques du CEA sont spécifiées pour les postes de travail par la DSI. Ces configurations sont tenues à jour et spécifient :

- les systèmes d'exploitation en vigueur (sous licence et sous maintenance),
- les paramétrages, y compris de sécurité, imposés sur ces systèmes,
- le socle de base des logiciels installés sur ces systèmes,
- les « dépôts de confiance » à utiliser pour récupérer les sources et les configurations de ces postes.

Le STIC est responsable de l'application et la réactualisation de ces configurations sur l'ensemble des terminaux de son périmètre.

Des configurations spécifiques peuvent être mises en œuvre, en particulier pour les serveurs, mais elles doivent être limitées au strict nécessaire et bénéficier de l'analyse de risque des configurations nationales.

Conformément à la charte informatique, certains outils peuvent être spécifiquement interdits par le RSSI.

Référence du document : RSSN-SSI-01-01	Page 34 / 62
Titre du document : PSSI CEA	Indice : 9

7.3.3 Documentation des configurations

Chaque STIC doit tenir à jour les dossiers techniques des systèmes d'information de son périmètre. Ces dossiers techniques détaillent notamment :

- la finalité du système,
- les ressources concernées et leur identification,
- les systèmes d'exploitation et leur paramétrage de sécurité,
- le profil de sécurité du service (niveau d'administration, filtrage réseau, modèle de délégation RBAC),
- son plan d'adressage réseau.

Ces dossiers techniques sont tenus à la disposition permanente de l'ASSI de Centre et du RSSI.

Ces dossiers doivent faire l'objet d'une revue générale et d'une réactualisation annuelle.

La réactualisation et la mise à jour de ces dossiers est une étape indispensable du processus de renouvellement de personnel en charge de l'administration.

7.4 Autorisation et contrôle d'accès

7.4.1 Contrôle des accès logiques

Identification et contrôle d'accès logique

Tous les utilisateurs du système d'information doivent disposer d'un compte personnel respectant les conventions de nommage spécifiés par la DSI. Ce compte personnel assure l'identification et l'imputabilité des actions sans équivoque. Il doit être utilisé y-compris pour l'accès aux postes de travail partagés (postes en libre-service, salles de réunion, etc.).

Droits d'accès aux ressources

Chaque utilisateur dispose d'un profil générique défini par son unité (accès aux ressources communes de l'unité), son domaine d'appartenance (domaine Active Directory de référence) et ses fonctions (accès aux données du service, accès aux ressources projet).

L'octroi de droits d'accès aux ressources ou données ne relevant pas de ce profil générique de l'utilisateur est soumis à l'accord préalable du propriétaire ou gestionnaire de la ressource à minima.

Droits sur	CD/SD	CCEA	Diffusion Restreinte	Diffusion Ordinaire
Autorisation	Accord de l'ASSI et OS	Accord de l'ASSI et OS	Accord du propriétaire pour l'INTRANET Accord de l'OS (hors INTRANET pour analyse des nationalités concernées)	Accord du propriétaire ou gestionnaire

Gestion des profils d'accès aux applications

Les applications faisant l'objet d'une homologation, doivent faire l'objet d'une description formelle de leur modèle d'administration. En particulier, ce modèle (RBAC – Role Based Access Control) doit définir :

- les différents profils et leurs niveaux de criticité (Rouge, Jaune, Vert ou Blanc),
- les modèles de délégation entre les différents profils,
- les administrateurs fonctionnels de l'application,
- les moyens techniques pour accéder à ces profils (postes, réseaux, protocoles et logiciels),
- les prérequis organisationnels (niveau d'habilitation en particulier) pour l'obtention de ces profils.

Ces éléments font partie intégrante du dossier d'homologation du serveur. Ils sont contrôlés avant la mise en service de la ressource et ponctuellement dans le cadre d'audit. Le périmètre de l'homologation se limite aux

Référence du document : RSSN-SSI-01-01	Page 35 / 62
Titre du document : PSSI CEA	Indice : 9

droits d'accès d'administration et d'exploitation des ressources applicatives, la définition des différents profils fonctionnels et la vérification de leur aptitude est de la responsabilité de la maîtrise d'ouvrage de l'application.

7.4.2 Processus d'autorisation

Autorisation d'accès des utilisateurs

L'octroi d'un compte informatique est soumis à l'autorisation préalable du responsable hiérarchique tel que spécifié dans la charte d'usage des moyens informatiques, et à la vérification que le personnel concerné dispose de tous les niveaux d'habilitation, ou des garanties de sécurité nécessaires, auprès de l'officier de sécurité en fonction de l'unité et de son domaine d'appartenance.

L'ASSI est informé systématiquement de toute nouvelle ouverture de compte.

L'ASSI procède régulièrement à une revue des comptes et droits d'accès pour son périmètre, et s'assure de l'adéquation des niveaux d'habilitation requis par rapports à la sensibilité des données, et à l'évolution de cette sensibilité dans le temps. Les moyens nécessaires à ces revues de comptes et de droits sont à la charge des STIC.

Revue des autorisations d'accès

Les autorisations d'accès à une ressource de données¹⁷ doivent être validées par le responsable/propriétaire de la ressource, par défaut l'ASSI de l'unité est considéré comme responsable de la ressource.

Les autorisations d'accès donnant droit à des privilèges d'administration techniques ou fonctionnelles doivent être justifiées et préalablement validées par l'ASSI de centre.

Toutes les autorisations d'accès doivent faire l'objet de revue périodique par l'ASSI d'unité, par le biais des outils mis en place par le STIC. Cette revue périodique porte sur la légitimité d'un compte vis-à-vis de ses groupes d'appartenance dans les annuaires de sécurité, enrichie par des relevés de configuration automatisés pour des ressources de type serveur.

Les revues des droits des comptes d'administration jaunes et verts doivent être réalisées de manière trimestrielle par l'ASSI du centre concerné.

La revue des droits des comptes d'administration de portée nationale – i.e. comptes rouges ou jaunes – doivent être réalisés par l'ASSI de centre et les ASSI de référence pour la DSI et les USCI.

7.4.3 Gestion des authentifiants

Confidentialité des informations d'authentification

Les mots de passe et autres informations d'authentification sont des informations sensibles qui doivent être traitées comme des informations confidentielles. Ils sont la propriété de leur détenteur et ne doivent être cédés sous aucun prétexte. Les utilisateurs sont avisés que la fourniture de leur mot de passe à un tiers y compris de l'exploitation ne se justifie pas en dehors des opérations de séquestre visées par l'ASSI lorsqu'il est fait usage de moyens de chiffrement.

Tous les mots de passe doivent être considérés comme des informations de niveau « Diffusion Restreinte » (à l'exception des mots de passe d'initialisation) et doivent être protégés comme tels.

Gestion des mots de passe

Aucune application ne doit faire transiter les mots de passe des utilisateurs en clair sur le réseau CEAnet. Aucun mot de passe utilisateur ne peut être stocké sous une forme réversible ou en clair, sans bénéficier de la protection d'un outil de chiffrement de niveau « Diffusion Restreinte ».

Initialisation des mots de passe

Les mots de passe d'initialisation sont aléatoires et à usage unique. La réutilisation d'un même mot de passe d'initialisation est proscrite. L'utilisateur est forcé de changer ce mot de passe aléatoire dès la première utilisation et en cas de non initialisation du compte, au-delà de 30 jours, le compte est désactivé par le STIC ou par l'exploitant concerné.

¹⁷ espaces de données, applications, sites collaboratifs, sites de publications, partage de données, moyens techniques, etc....

Référence du document : RSSN-SSI-01-01	Page 36 / 62
Titre du document : PSSI CEA	Indice : 9

Les mots de passe initiaux sont transmis à l'utilisateur selon des procédures permettant de s'assurer de son identité (i.e. en contact facial) ou envoyés comme un document de nature « Diffusion Restreinte » à un tiers de confiance parmi l'ASSI d'unité, le chef d'unité ou à un tiers lorsque celui-ci est dûment identifié par l'ASSI d'unité.

Gestion des certificats de chiffrement

La gestion des clés de chiffrement privées et publiques, permettant les échanges confidentiels, repose sur l'infrastructure INCA.

L'utilisation de clés ou certificats de chiffrements CEA non stockés, sur le badge sécurisé INCA est proscrite pour le niveau Diffusion Restreinte.

Cas particulier de la réinitialisation

La fourniture d'un mot de passe de réinitialisation est soumis aux mêmes contraintes que celles du premier mot de passe, il est cependant admis que celui-ci soit fourni directement à l'utilisateur par le biais d'un contact téléphonique dès lors que l'opérateur s'assure de l'identité de son interlocuteur (l'opérateur doit rappeler son interlocuteur en utilisant le numéro professionnel référencé dans l'annuaire CEA).

L'utilisation d'outil d'auto-dépannage de type « question / réponse » est proscrite sur les systèmes d'information CEA. L'auto-dépannage peut être mis en œuvre lorsqu'il repose sur l'authentification par badge INCA.

Politiques des mots de passe

Les systèmes d'authentification CEA doivent mettre en œuvre les politiques de mot de passe suivantes :

- Longueur minimale du mot de passe : 12 caractères (14 caractères pour les comptes de service)
- Longueur maximale du mot de passe : aucune
- 4 jeux de caractères différents doivent être utilisés : Minuscule, Majuscule, Chiffre et Ponctuation
- Durée minimale du mot de passe : 24h
- Durée maximale du mot de passe : 1 an (pour les comptes interactifs et pour les comptes de service)
- Historique des mots de passe : 6 minimum (interdiction de reprendre un mot de passe parmi les 6 derniers utilisés).

Pour anticiper l'abandon de l'authentification par mot de passe sur le domaine Intra, et compte tenu des analyses de risques actuelles, la durée maximale du mot de passe des comptes utilisateurs sur le domaine Intra peut être illimitée.

Utilisation des certificats électroniques

Chaque utilisateur doit disposer de certificats de l'AC Utilisateur Badge CEA obtenus auprès de l'infrastructure de gestion de clé [IGC] CEA. L'attribution automatique ainsi que la publication des certificats lors de la création du compte utilisateur doivent être mis en œuvre pour garantir la cohérence de l'annuaire.

Les clés privées associées à ces certificats sont stockées et mis en œuvre sur le badge CEA INCA de l'utilisateur.

Contrôle systématique de la qualité des mots de passe

La conformité avec la politique de mots de passe est de la responsabilité du maître d'ouvrage de toute nouvelle application. Elle peut être contrôlée et donner lieu à l'arrêt d'un service non conforme. L'utilisation des annuaires d'authentification communs Active Directory est exigée sauf dérogation dûment motivée pour des raisons de sécurité et validée par l'ASSI du centre.

Des audits de vérification peuvent être diligentés sur la qualité des mots de passe d'un système en production. Ils sont soumis à l'accord préalable du RSSI qui valide les acteurs, les outils mis en œuvre et le respect de la confidentialité des informations collectées.

Référence du document : RSSN-SSI-01-01	Page 37 / 62
Titre du document : PSSI CEA	Indice : 9

Fédération des Identités

Les logiciels et services SAAS dont l'usage nécessite un abonnement lié à une identification sur une plateforme externe (exemple : Logiciels Adobe) ne peuvent être mis en œuvre que dans le cadre d'une fédération d'identités.

Les fournisseurs d'identités exposés à internet bénéficient des mêmes services de protection que les services nomades, c.à.d. utilisation d'un dispositif OTP.

7.4.4 Gestion des authentifiants d'administration

Séquestre des authentifiants « Administrateur »

Le CEA doit conserver un authentifiant d'administration en séquestre pour des raisons de sécurité, à fortiori lorsque l'administration des systèmes est confiée à un prestataire extérieur.

Cet authentifiant est conservé au coffre et confié à l'ASSI de centre sous forme papier dans une enveloppe scellée ou sous la forme d'un support amovible chiffré par un outil qualifié standard à minima.

Un séquestre de secours, si nécessaire pour des contraintes d'exploitation, est réalisé par le STIC du site via un support chiffré par un outil qualifié standard à minima.

Il est de la responsabilité de l'exploitant de fournir à l'ASSI de centre, les mots de passe de séquestre à chaque renouvellement.

Il est recommandé de créer des comptes d'administration spécifiques pour le séquestre, dont la moindre activité doit faire l'objet d'une alerte de sécurité.

Politique des mots de passe « Administrateur »

Les mots de passe administrateur sont soumis à minima aux mêmes règles que les mots de passe des utilisateurs. Il est de la responsabilité de l'administrateur responsable de son compte privilégié de ne pas réutiliser le même mot de passe sur ses différents comptes d'administration.

Gestion des départs d'un « Administrateur »

Le départ ou le changement de périmètre d'un administrateur donne lieu à la révocation immédiate de ses authentifiants et à la désactivation de ses comptes d'administration.

En cas de fin de mission pour des motifs d'incident de sécurité, l'ensemble des mots de passe d'administration et de services portés à la connaissance de l'administrateur défaillant sont modifiés suivant le même procédé que celui mis en œuvre pour le renouvellement automatique.

7.4.5 Administration des systèmes

Restriction des droits

Les administrateurs ne peuvent disposer de droits d'administration de serveurs avec leur compte utilisateur.

Les mots de passe des comptes d'administration sont obligatoirement diversifiés pour limiter les impacts d'une compromission. À titre dérogatoire et après l'accord de l'ASSI de centre, les utilisateurs peuvent se voir confier un compte d'administration local de leur poste de travail, si ce poste leur est nominativement affecté. Ce compte d'administration local dispose de prérogatives limitées au poste de travail et l'autorisation doit être renouvelée tous les deux ans.

Les administrateurs peuvent disposer de différents comptes d'administration en fonction du périmètre accédé :

	Admin Rouge	Admin Jaune	Admin Vert	Admin Blanc	Admin Locale
Périmètre	Admin Domaine	Admin serveurs Jaunes Admin postes Jaunes	Support utilisateurs Admin serveurs verts Admin Postes Verts	Prise en main sur un poste utilisateur Admin Postes Blancs	Gestion d'un poste dédié unique Courrier et navigation internet

Référence du document : RSSN-SSI-01-01	Page 38 / 62
Titre du document : PSSI CEA	Indice : 9

Impact	Global CEA	Global Centre	Limité Centre	Limité STIC Exception pour les administrateurs fonctionnels	Limité utilisateur
---------------	------------	---------------	---------------	--	--------------------

Protection des accès aux outils d'administration

L'accès à distance aux outils et interfaces d'administration est limité aux personnes habilitées depuis des ressources identifiées comme dédiées à l'administration.

	Admin d'une ressource Rouge	Admin d'une ressource Jaune	Admin d'une ressource Verte	Admin d'un poste utilisateur
Compte	Compte Rouge	Compte Jaune	Compte Vert	Compte Blanc
Provenance	LAN Admin Rouge	LAN Admin Jaune	LAN Admin Vert	LAN Admin Vert

L'ensemble des comptes et mot de passe d'administration par défaut de tous matériels informatiques doivent être systématiquement révoqués, modifiés ou inactivés et remplacés par les comptes d'administration CEA, avant la mise en service de ces équipements.

Ces mesures de protection concernent également :

- les cartes d'administration « bas niveau » (exemples : BMC, DRAC ou ILO),
- les interfaces d'administration des équipements de sécurité et réseaux.

Habilitation des administrateurs

Les administrateurs sont des personnels CEA ou des prestataires de confiance. Ils sont réputés loyaux et compétents. En fonction du périmètre, ils doivent disposer d'un niveau d'habilitation minimum.

	Système homologué	Admin Rouge	Admin Jaune	Admin Vert
Habilitation	Habilitation équivalente	Habilitation CD	Habilitation CD	Badge CEA

Gestion des actions d'administration

Les opérations d'administration des systèmes doivent être systématiquement journalisées. Les politiques de journalisation sont mises en œuvre pour tracer toutes les opérations d'administration avec l'imputabilité du compte et le périmètre de l'action. La centralisation de ces journaux doit être privilégiée sur les systèmes étendus, elle est exigée sur les réseaux Intranet, Extranet, Hébergement (wifi CEA) et Partenaires.

Sécurisation des flux d'administration

Les flux d'administration sont exclusivement autorisés depuis les postes et réseaux d'administration d'un niveau équivalent à la ressource administrée (Par exemple, les serveurs rouges d'une zone ne sont administrés que depuis la bulle d'administration rouge). Les postes utilisateurs ne sont accessibles à distance que depuis les réseaux d'administration de niveau vert.

Centraliser la gestion des systèmes d'information

Les journaux d'activité liés aux traces d'administration sont collectés de manière globale sur des équipements dédiés sous la responsabilité du RSSI. Seuls les administrateurs autorisés par l'ASSI de centre peuvent disposer d'un accès au centre de supervision.

Le centre de supervision fait l'objet d'une déclaration spécifique dans le registre des application DPD (Délégué à la protection des données) – pour être en conformité avec le Règlement général de Protection des données (RGPD).

Le centre de supervision est placé sous la responsabilité du RSSI.

Référence du document : RSSN-SSI-01-01	Page 39 / 62
Titre du document : PSSI CEA	Indice : 9

Sécurisation des outils de prise en main à distance

La prise en main à distance sur un poste utilisateur n'est autorisée que par les administrateurs du STIC provenant du réseau d'administration de niveau vert. Ces derniers utilisent pour effectuer ces opérations des outils approuvés et robustes à des attaques d'interception réseau, depuis des postes d'administration verts. Ils utilisent leur compte blanc (celui associé à leur profil utilisateur) pour se connecter à distance sur le poste d'un utilisateur pour éviter de compromettre leur mot de passe d'administration sur un poste utilisateur.

La prise en main à distance depuis des réseaux de sécurité moindre, à fortiori internet ou d'autres réseaux publics, est proscrite.

Lorsqu'une opération de prise en main à distance sur un poste de travail est réalisée alors que l'utilisateur est en session, ce dernier doit être alerté préalablement à toute opération et il lui est laissé le temps de fermer ses documents.

7.4.6 Administration des domaines

Chaque zone CEAnet (Intranet, Partenaires et Extranet) dispose d'un domaine Active Directory de référence qui lui est propre. Cet annuaire de sécurité assure l'inventaire des utilisateurs et des ressources, ainsi que les mesures de cloisonnement de sécurité.

D'autres domaines peuvent être mis en œuvre sur les réseaux homologués, mais leurs spécifications de sécurité ne seront pas traitées dans la PSSI, mais dans leur dossier d'homologation. Chacun de ces domaines disposent de spécificités, mais ils respectent les caractéristiques communes de la PSSI.

La protection des domaines Active Directory fait l'objet d'un « *Guide – Protection de l'AD* ».

L'administration des domaines se fait obligatoirement via un compte d'administration rouge, un poste d'administration rouge, et un VLAN d'administration rouge dédié à ce type d'usage

Définir une politique de gestion des comptes du domaine

Chaque utilisateur du système d'information CEA doit disposer d'un compte dans un des domaines relatifs à son périmètre après l'accord du chef d'unité et de son ASSI d'unité. Ce compte dit utilisateur est un compte individuel et nominatif associé à une adresse de messagerie cea.fr et donne lieu à un espace de stockage individuel.

Les comptes sont créés par le STIC du centre de rattachement.

Les comptes d'administration nécessitent des processus d'autorisation plus restrictifs.

	Admin Rouge	Admin Jaune	Admin Vert	Admin local	Utilisateur
Compte	Accord USCI et DSI	Accord STIC	Accord STIC	Accord ASSI	Chef de laboratoire ASSI Unité
Exemple	AR-XX123456	AJ-XX123456	A-XX123456	ADMIN-LOCAL	XX123456

Configurer la stratégie des mots de passe des domaines

La stratégie des mots de passe décrite précédemment dans la PSSI est configurée dans la « politique par défaut du domaine ». La mise en conformité et le maintien de la politique du domaine est sous la responsabilité des administrateurs rouges.

Définir et appliquer une nomenclature des comptes du domaine

La nomenclature des comptes du domaine est définie par la DSI dans sa spécification de nommage des comptes du domaine. Cette spécification fournit les normes sur les conventions de nommages utilisées sur les domaines.

Restreindre au maximum l'appartenance aux groupe d'administration du domaine

Les comptes d'administration du domaine sont des comptes rouges. Ils doivent être limités au strict nécessaire et ne doivent pas excéder 2 comptes pour 1000 utilisateurs.

Référence du document : RSSN-SSI-01-01	Page 40 / 62
Titre du document : PSSI CEA	Indice : 9

Maîtriser l'utilisation des comptes de service

L'octroi d'un compte de service est soumis au processus d'autorisation des comptes d'administration qui dépend du niveau de sensibilité des tâches d'administration. Ces comptes sont proscrits de tout usage interactif sur le domaine. Les comptes sont placés sous la responsabilité d'une unité identifiée, à défaut du STIC du centre.

Limiter les droits des comptes de service

Les comptes de services ne doivent pas être utilisables de manière interactive.

Les comptes génériques doivent être évités et s'ils sont mis en œuvre, ils doivent être restreints à l'usage du terminal concerné sans aucun droit d'administration et d'utilisation d'outils de chiffrement. Leur création doit être validée par l'ASSI de centre, qui veille à limiter les droits au strict minimum.

Comme les comptes d'administration, les comptes de services rouges et jaunes sont contraints par politique de groupe à leur périmètre d'exploitation.

Désactiver les comptes du domaine obsolètes

Les comptes du domaine sont désactivés dès le départ ou la fin de mission du détenteur concerné. Après un délai de désactivation de 6 mois, ces comptes sont détruits définitivement.

Améliorer la gestion des comptes d'administrateurs locaux

Les comptes d'administrateur locaux sur les serveurs sont limités au strict nécessaire en cas d'impossibilité d'utiliser les comptes du domaine pour des raisons d'isolation réseau. Ils ne sont pas utilisés dans l'exploitation courante mais uniquement en accès console en dernier recours.

Tous les comptes d'administration locaux des serveurs ont des mots de passe diversifiés et respectant la politique de mot de passe du domaine. Leurs mots de passe doivent être changés tous les ans au même titre que les comptes de service. Les processus techniques de renouvellement des mots de passe locaux doivent utiliser des procédés cryptographiques pour s'assurer que le mot de passe ne peut être recouvré par une simple lecture de script ou découverte du procédé.

Les comptes d'administration locaux des postes de travail sont interdits d'accès depuis le réseau par une politique du domaine appliquée sur tous les postes. Cette protection est mise en œuvre par les STIC.

7.5 Envoi en maintenance et mise au rebut

Maintenance externe

Les opérations de maintenance externe, pour lesquelles des supports de données rémanentes seraient amenés à sortir d'un établissement CEA, doivent s'affranchir du risque de fuite d'informations sur ces supports. Les mesures conservatoires sur les supports de données (disques, cartouches ou autres supports) dépendent du niveau de confidentialité.

	CD/SD	CCEA	Diffusion Restreinte	Diffusion Ordinaire
Maintenance externe	Interdit	Interdit	Si données chiffrées par produit qualifié (effacement simple) Sinon, interdit	Si données chiffrées (effacement simple) Sinon, effacement sécurisé avec réécriture

Il est de la responsabilité des STIC de mettre en œuvre et de spécifier des options « No Disk Return » dans les marchés liés au stockage et à l'archivage. Les mécanismes de type RAID ne sont pas jugés suffisants pour garantir l'absence de rémanence sur les disques.

En cas d'impossibilité de mener à bien les opérations d'effacement sécurisé du support (support défectueux), le support n'est pas autorisé à sortir d'un établissement CEA. En cas d'impossibilité d'extraire le support physiquement pour conservation sur site, l'ensemble du terminal n'est pas autorisé à sortir d'un établissement CEA (cas des équipements type tablette avec support de données indissociable du terminal).

Référence du document : RSSN-SSI-01-01	Page 41 / 62
Titre du document : PSSI CEA	Indice : 9

Lors du retour de matériel à l'issue d'une opération de maintenance, le STIC veille à l'innocuité des supports rendus (présence de maliciels ou de virus) en procédant à un effacement simple si ces derniers ne sont pas restitués vierges.

Mise au rebut

Les opérations de mise à la réforme doivent garantir l'absence de fuite d'informations sur les supports de données rémanentes. Les mesures de réformes dépendent du niveau de confidentialité.

	CD/SD	CCEA	Diffusion Restreinte	Diffusion Ordinaire
Réforme	Destruction physique	Destruction physique	Si données chiffrées par produit qualifié (effacement simple,) Sinon, destruction physique	Si support intégralement chiffré, (effacement simple) Sinon, effacement sécurisé avec réécriture ou destruction physique

En cas de doute sur la nature des informations traitées, les supports de données rémanentes doivent être détruits.

Ces dispositions doivent être prévues dans les contrats liés à ces interventions.

L'ensemble des matériels informatiques doit s'inscrire dans un processus de revalorisation et de recyclage.

7.5.2 Lutte contre les codes malveillants

Protection contre les codes malveillants

Tous les terminaux utilisateurs CEA sont équipés d'un antivirus national spécifié par la DSI. Cet antivirus « Poste de travail » est complété par les antivirus suivants :

- Antivirus sur les passerelles de messagerie,
- Antivirus sur les serveurs de messagerie.

Ces trois dispositifs Antivirus doivent être issus de fournisseurs différents et validés par le RSSI.

Les sites internet appartenant à la catégorie « Sites connus pour héberger des codes malveillants » ou non conformes à la charte CEA sont bloqués par la passerelle internet de CEAnet.

Il est rappelé que l'utilisation de supports amovibles non CEA est interdite sauf autorisation préalable du chef d'unité, à ce titre des services dédiés d'analyse de sécurité des supports amovibles, doivent être mis en œuvre. Ils peuvent être également utilisés pour vérifier l'innocuité des supports amovibles CEA.

L'utilisation de services externalisés d'analyse de malware, nécessitant l'envoi de fichiers de données du CEA, est proscrite.

Gestion des évènements de sécurité de l'antivirus

Tous les journaux antivirus des postes de travail sont collectés et archivés pour un an dans le centre de supervision nationale.

Mise à jour de la base de signatures

La mise à jour du logiciel antivirus fait partie du maintien en condition de sécurité et est pilotée par le STIC du centre sur l'ensemble des terminaux de son périmètre. La mise à jour des bases virales est automatisée et pilotée par les serveurs Antivirus Nationaux à partir de la politique nationale antivirus définie par la DSI et mise en œuvre par l'USCI.

Certains incidents peuvent donner lieu à des diffusions rapides de signatures de manière forcée et non plus automatique par l'USCI.

Référence du document : RSSN-SSI-01-01	Page 42 / 62
Titre du document : PSSI CEA	Indice : 9

7.5.3 Mise à jour des systèmes et des logiciels

Politique de suivi et d'applications des correctifs de sécurité

Les applications déployées sur les postes et serveurs sont placées sous la pleine et entière responsabilité du STIC dans le respect des standards nationaux définis par la DSI. Ces applications font l'objet d'un processus de mise à jour pour lutter contre l'obsolescence et d'une publication des correctifs de sécurité validée par la DSI.

Les applications obsolètes ou non maîtrisées par le STIC sont proscrites et peuvent être désinstallées pour motif de sécurité, pour des motifs de violation de licence ou pour non-conformité avec la présente PSSI. Le STIC est également garant de la rationalisation des applications mises en œuvre sur son périmètre pour limiter la surface d'exposition pour un même besoin fonctionnel.

Déploiement des correctifs de sécurité

La DSI publie les correctifs de sécurité de confiance et de manière fiable et sécurisée. À compter de la date de publication de ces correctifs par la DSI, les correctifs doivent être déployés :

Pour les postes de travail :

- sous 5 jours ouvrés en régime normal,
- sous 24h en régime incident signalé par la DSI.

Pour les serveurs :

- sous 30 jours ouvrés en régime normal,
- en régime incident, spécifique - à définir par la DSI.

En cas d'impossibilité de respecter ces délais (problème d'incompatibilité), le STIC signale à la DSI son incapacité à déployer le correctif, propose une date de résolution et l'informe des démarches entreprises pour limiter l'impact de la vulnérabilité sur la sécurité des systèmes concernés.

Assurer la migration des systèmes obsolètes

Un système est considéré comme obsolète lorsqu'il ne dispose plus d'un support en capacité de fournir des correctifs de sécurité (quelque que soit la validité de sa certification¹⁸ ou de ses services rendus).

La DSI informe les STIC de l'obsolescence d'un système ou logiciel dès qu'elle en est avisée. À compter de cette date, les STIC disposent d'un délai d'une année pour se placer en conformité en migrant les systèmes obsolètes vers les plateformes en cours de validité ou en arrêtant le système obsolète.

Les mesures conservatoires sont spécifiées par le RSSI pour prendre en compte la période transitoire entre l'obsolescence du système et sa migration.

Isoler les systèmes obsolètes

Chaque STIC dispose d'une bulle « Postes non conformes ». Ce profil réseau particulier assure un premier niveau de protection contre des systèmes vulnérables (absence de navigation internet, absence de messagerie...). Il est de la responsabilité de chaque STIC de déplacer les systèmes obsolètes sur ce VLAN pour garantir l'intégrité du système d'information, et de procéder à leur mise en conformité dans les meilleurs délais. Cette bulle « Postes non conformes » n'a pas à vocation à conserver de manière pérenne des systèmes obsolètes et vulnérables.

¹⁸ Certains systèmes disposent d'une certification fonctionnelle par un organisme externe, liée à une version spécifique d'un logiciel ou d'un système (ensemble de versions spécifiques d'équipements, associé à des versions spécifiques de logiciels).

Référence du document : RSSN-SSI-01-01	Page 43 / 62
Titre du document : PSSI CEA	Indice : 9

7.5.4 Journalisation

Journalisation des alertes

Chaque système (serveur et poste de travail) applique la politique de journalisation définie par le RSSI. Cette politique est appliquée par le STIC sur les ressources de son périmètre.

Politique de gestion et d'analyse des journaux

Les journaux d'activité sont analysés par les STICs et par les USCI pour assurer le contrôle de sécurité de premier niveau. Certains systèmes identifiés par le RSSI sont collectés et consolidés sur le centre de supervision de sécurité pour un contrôle de deuxième niveau.

Les journaux sont accessibles en lecture à l'ensemble des exploitants et ASSI validés par l'ASSI du centre concerné. L'ASSI du centre vérifie la bonne diffusion de la charte d'utilisation de la supervision aux différents acteurs de son périmètre, étant entendu que toutes ces personnes sont soumises à un devoir de confidentialité renforcée.

Le centre de supervision de sécurité est sous la maîtrise d'ouvrage du RSSI.

Conservation des journaux

Les journaux d'activité sont conservés sur une période d'une année glissante. Chaque STIC veille à la destruction des journaux au-delà de cette période de rétention.

Le RSSI est responsable de la destruction des journaux sur le centre de supervision au-delà de cette période de rétention.

7.6 Défense des systèmes d'information

7.6.1 Gestion dynamique de la sécurité

La gestion de la sécurité est confiée en contrôle de premier niveau au STIC et USCI, en deuxième niveau au RSSI à travers le centre de supervision de sécurité. Le RSSI est en charge de l'analyse des journaux à la recherche des signaux faibles et des corrélations avec la veille sécurité de la cyber menace. Le STIC est en charge de l'analyse des journaux pour traiter les alertes détectées et les non-conformités de son parc logiciel et matériel avec les configurations attendues. Une attention particulière est portée sur les interfaces de communication entrantes et sortantes avec l'extérieur du CEA (réseaux, messagerie et supports amovibles).

7.6.2 Gestion des matériels fournis à l'utilisateur

Maîtrise des matériels

Les matériels informatiques sont affectés à l'utilisateur après leur approvisionnement, leur identification dans l'inventaire et leur mise en conformité vis-à-vis des configurations autorisées par le STIC. L'utilisation de moyens personnels est proscrite pour traiter des informations professionnelles à l'exception de l'offre MOBI-Standard.

L'ensemble des matériels reste propriété du CEA, et doit être restitué au STIC, dès fin d'usage, remplacement ou fin de mission.

Le STIC conserve un accès administrateur sur l'ensemble des matériels affectés.

La connexion d'équipements non CEA qu'il n'est pas possible d'inventorier ou maîtriser par le STIC est proscrite sur les réseaux du CEA à l'exception de la Zone Hébergement. Les matériels propriétés CEA n'ont pas vocation à être raccordés en Zone Hébergement. Les matériels provenant d'organismes extérieurs doivent être soumis à l'accord du chef d'unité avant leur raccordement et respecter les conditions d'usage et de raccordement définis par l'ASSI de centre suivant la nature des besoins et des ressources accédées.

Les procédures d'entrées / sorties de matériels sont définies par l'Officier de sécurité du centre propriétaire du matériel.

Référence du document : RSSN-SSI-01-01	Page 44 / 62
Titre du document : PSSI CEA	Indice : 9

Mesures de protections contre le vol et la perte

Tous les terminaux doivent disposer d'un chiffrement de surface de l'ensemble du disque. Pour les terminaux nomades, ce chiffrement doit être protégé par une authentification au démarrage (authentification pré-boot). Cette mesure limite les capacités d'extraction de données par lecture directe du disque dur.

Tous les supports amovibles utilisés sur l'Intranet doivent bénéficier d'un chiffrement de données au niveau qualifié standard sous la forme d'une archive ou d'une zone chiffrée.

Des supports qualifiés au niveau renforcé peuvent être autorisés, dans le cadre d'une homologation, à conserver de l'information classifiée. L'utilisateur est alors contraint de respecter la politique d'emploi définie dans le cadre de l'homologation, en particulier l'interdiction d'utiliser ces supports sur des postes non homologués au moins au même niveau.

Déclarer les pertes et vols

Les pertes et vols de matériels ou de ressources informatiques sont à déclarer à l'Officier de Sécurité du Centre concerné qui tient à jour le registre de ces incidents avec en particulier l'identité du personnel détenteur, l'identification du matériel et le niveau de sensibilité des informations traitées.

Ces incidents sont signalés sans délai par l'officier de sécurité du centre au STIC concerné pour la mise en œuvre de mesures conservatoires (changement des mots de passe de l'utilisateur, effacement à distance lorsque les dispositifs le permettent).

Réaffectation de matériels informatiques

Les matériels informatiques sont restitués à l'unité après la fin de mission de l'utilisateur, le STIC prend en charge sa réattribution. Les matériels qui seront réaffectés à un même niveau de sensibilité ou supérieur doivent faire l'objet d'un effacement sécurisé du disque, si les données étaient en clair ou d'un effacement simple si les données étaient chiffrées.

En fonction de la qualification des informations traitées, la réaffectation à un niveau inférieur doit être assimilée à une mise au rebut pour le traitement des données rémanentes (cf. § 7.5).

7.6.3 Nomadisme

On considère comme « nomadisme » le fait pour un utilisateur des moyens informatiques du CEA d'exercer son activité professionnelle dans des locaux qui ne sont pas sous la responsabilité du CEA (les utilisateurs travaillant sur un autre centre que leur centre habituel avec des ressources fournis par le centre d'accueil ne sont pas considérés comme nomades).

Déclaration des équipements nomades aptes à traiter des informations sensibles

Tous les services et tous les terminaux ne sont pas aptes à traiter des informations sensibles en situation de nomadisme.

Seuls les services MOBI-Standard sont autorisés depuis des postes non maîtrisés par le CEA, ces services offrent :

- l'accès à la messagerie d'entreprise sans capacité de lire les courriels chiffrés,
- l'accès à certains sites intranet spécifiquement autorisés.

Toutes les autres offres de services de nomadismes (MOBI-Étendu ou MOBI-Push) sont exclusivement réservées à des terminaux professionnels propriété du CEA, conformes aux règles de sécurité définies dans la PSSI.

Seul le service MOBI-Étendu est apte à traiter de l'information Diffusion-Restreinte.

Les autres services ne sont pas aptes à traiter de l'information d'un niveau équivalent au « Diffusion Restreinte ».

Référence du document : RSSN-SSI-01-01	Page 45 / 62
Titre du document : PSSI CEA	Indice : 9

Accès à distance au système d'information CEA

L'accès à distance au système d'information CEA est dénommé offre MOBI (cf. § 8.1.6). Elle est soumise à une authentification forte¹⁹ et personnelle de l'utilisateur sous la forme d'un dispositif nomade validé par le RSSI communément appelé MOBI-Pass.

Un mécanisme d'authentification par mot de passe dit de secours peut être mis en œuvre sur dérogation dans deux cas d'usage seulement :

- l'utilisateur bénéficie d'une authentification par son mot de passe de domaine qu'il doit changer dès qu'il récupère son nouveau MOBI-Pass. Avant de mettre en place ce processus vulnérable de dépannage, le STIC doit s'assurer de l'identité de l'utilisateur en le rappelant sur son numéro de téléphone professionnel référencé dans l'annuaire CEA.
- sur dérogation de l'ASSI de centre pour le personnel malvoyant.

7.6.4 Sécurité des imprimantes et copieurs multifonction

Impression des informations sensibles

Les copieurs multifonction sont sélectionnés dans le cadre d'un accord national après validation du cahier des charges intégrant les spécifications de sécurité fournies par le RSSI. Ces copieurs assurent également la fonction d'impression en réseau.

Le copieur bénéficie du niveau de classification de son contexte d'homologation, les restrictions d'usage sont définies et affichés à proximité du copieur pour éviter les erreurs de la part de l'utilisateur. L'officier de sécurité veille à la mise en œuvre de l'affichage des restrictions d'usage à proximité du copieur.

Les impressions en réseau sont soumises à l'authentification de l'utilisateur pour récupérer ses sorties papier en sa présence. Les fonctions de numérisation sont également autorisées vers une ressource de stockage en réseau (ressource en accès restreinte), vers une boîte aux lettres limitée au domaine cea.fr ou à l'annuaire de messagerie CEA ou vers un support USB sous la responsabilité de l'utilisateur.

Sécurité des imprimantes et des copieurs multifonctions

Les équipements de type imprimantes réseau et copieurs multifonctions doivent être raccordés au réseau dans des VLAN spécifiques qui protègent leurs interfaces d'administration réseau en ne les exposant qu'aux VLAN d'administration vert. Seuls les serveurs d'impression, les serveurs de stockage, les serveurs de messagerie et les postes d'admin sont autorisés à communiquer via le réseau avec ces équipements. Aucune communication directe depuis les postes de travail ou vers internet n'est autorisée.

Les journaux d'activité d'impression doivent être conservés au niveau de chaque centre pour une durée de 1 an maximum.

7.7 Exploitation sécurisée des centres informatiques

7.7.1 Sécurité des ressources informatiques

Système d'exploitation

Les systèmes d'exploitation déployés sur le système d'information CEA sont spécifiés par la DSI qui est responsable de l'acquisition des licences commerciales pour le CEA.

Tous les systèmes d'exploitation font l'objet d'un support de la part de l'éditeur ou d'un prestataire de service. Pour les logiciels communautaires, le support et les mises à jour sont mises en œuvre par le STIC sur la base des serveurs communautaires internet prévus à cet effet. Le STIC met en œuvre des sites miroirs internes pour la distribution et la mise à jour des logiciels communautaires.

Chaque machine physique ne peut disposer que d'un seul système d'exploitation : le multiboot est interdit

¹⁹ basée sur un double facteur

Référence du document : RSSN-SSI-01-01	Page 46 / 62
Titre du document : PSSI CEA	Indice : 9

Logiciel en tiers présentation

Tous les services exposés à internet sont soumis à une analyse de risque préalable, à une configuration durcie et à un processus d'autorisation technique avant leur mise en production.

Les services de la zone Partenaires mettent en œuvre exclusivement des protocoles sécurisés (chiffrés) et assurent l'authentification de l'utilisateur.

Les services de la zone Extranet ne sont pas éligibles à traiter des informations confidentielles. Ils doivent cependant mettre en œuvre les mécanismes visant à garantir l'intégrité et la disponibilité des informations traitées.

Logiciel en tiers application

Tous les services en tiers application doivent prendre en charge l'autorisation de l'utilisateur, la journalisation et les restrictions d'accès en fonction du réseau de provenance de la requête. Sur les services mis en œuvre en zone Partenaires, l'authentification doit être réalisée le plus en amont possible et doit être mise en œuvre par le « Tiers » présentation.

Les services traitant des informations sensibles bénéficient tous d'une homologation, soit parce qu'ils sont hébergés sur des infrastructures homologuées auquel cas ils se conforment aux instructions prévues dans l'homologation, soit ils sont homologués individuellement en prenant en compte les menaces inhérentes à l'infrastructure d'hébergement.

Logiciel en tiers données

Tous les services hébergeant la donnée mettent en œuvre des restrictions d'accès pour limiter les connexions directes aux équipes en charge de l'exploitation (maintenance, sauvegarde et supervision). Les accès directs par l'utilisateur doivent être proscrits. Les accès au tiers données doivent être restreints aux équipements réseau en charge de l'exploitation et au tiers applicatif.

Les accès, au tiers données, sont proscrits en provenance de l'internet.

Passerelle d'échange de fichiers

Les échanges de fichiers sont autorisés entre les différents réseaux dans la mesure où :

- le protocole utilisé est sécurisé (chiffrement et authentification),
- les flux sont limités et pris en charge dans les fiches bulles ou compatibles avec le filtrage interzone,
- l'établissement de la session d'échange est toujours à l'initiative de la ressource la plus sécurisée.

À titre dérogatoire, des échanges de données initiés depuis une ressource moins sécurisée vers une ressource homologuée doivent utiliser des passerelles de type diode labellisées et autorisées dans le contexte de l'homologation.

Messagerie technique

Il n'y a pas de messagerie SMTP dédiée au flux technique d'administration. La messagerie CEA peut être utilisée pour véhiculer des informations techniques, mais aucun compte d'administration n'est associé à ce moyen de communication, les administrateurs utilisent leur compte blanc pour accéder à la messagerie. Filtrage des flux applicatifs

Toutes les ressources informatiques hébergeant des services aux utilisateurs ou exposées à internet doivent être placées dans des bulles serveurs prévues à cet effet. Les services informatiques hébergés dans des bulles utilisateurs ne sont pas autorisés à traiter ou à héberger des informations ou des services.

Les bulles serveurs font l'objet de filtrage réseau pour limiter les services exposés au strict nécessaire et ne peuvent communiquer avec internet qu'à travers une « liste blanche » de services internet (toute ressource internet qui n'est pas explicitement autorisée est interdite).

Flux d'administration

Les flux d'administration ne sont autorisés en entrée des bulles serveurs que depuis les bulles d'administration prévues à cet effet.

Les flux d'administration des serveurs depuis les bulles utilisateurs et à fortiori depuis internet ou des zones de moindre sécurité sont proscrits.

Référence du document : RSSN-SSI-01-01	Page 47 / 62
Titre du document : PSSI CEA	Indice : 9

Lorsqu'il n'est pas possible de distinguer les flux d'administration des flux d'usage, le contrôle des flux d'administration doit être mis en œuvre au niveau du service (restriction par adressage IP de l'accès aux profils d'administration, restriction des postes à l'origine des flux d'administration).

Service de nom de domaine - DNS technique

Les conventions de nommage DNS sont définies par la DSI.

Il n'y a pas de service DNS technique, les services DNS sont communs aux utilisateurs et aux services. Le maintien en condition de sécurité de l'infrastructure DNS est confié aux USCI, l'administration des enregistrements DNS est déléguée aux STIC du centre depuis les bulles d'administration vertes.

Effacement de support

Suivant les spécifications du § 7.5, pour procéder à l'effacement des supports de données rémanentes, le STIC met en œuvre les outils validés par le RSSI suivant les modalités suivantes :

- si le support ne contient que des données chiffrées, un effacement simple sans surcharge après destruction de la clé de chiffrement est admis,
- si le support contient des données non chiffrées, un effacement avec surcharge (réécriture de l'ensemble du support) est mis en œuvre.

Destruction de support

Suivant les spécifications du § 7.5, pour procéder à la destruction des supports de données rémanentes, le STIC est en charge de la collecte des supports et de leur stockage dans un local adapté au niveau de qualification des données. L'officier de sécurité du centre, organise des campagnes de destruction par le biais de marché avec des prestataires qualifiés.

Traçabilité / imputabilité

Tous les services mis en œuvre par le STIC (serveurs, équipements réseau et équipements de sécurité) emploient la référence de temps fournie par le domaine Active Directory de rattachement ou, si inapplicable, par leur routeur par défaut, qui est lui-même synchronisé avec la référence CEA opérée par l'USCI (time.cea.fr).

Supervision

Les flux de supervision mis en place sur les différents services sont configurés pour assurer l'alimentation du centre de supervision directement ou par le biais de collecteurs dédiés. Ces flux peuvent être autorisés depuis des zones Hébergement, Partenaires, Extranet vers Intranet.

Le centre de supervision est hébergé dans la zone Intranet pour les réseaux non homologués.

Dans le contexte d'une homologation, un centre de supervision doit être mis en œuvre et opéré dans le périmètre de l'homologation si l'usage des ressources Intranet est proscrit.

Accès aux périphériques amovibles

L'accès aux supports amovibles de type USB est proscrit sur les postes d'administration rouges et jaunes, ainsi qu'à tous postes d'administration ou serveurs assurant des fonctions critiques, à l'exception du processus d'initialisation qui ne peut se faire qu'à partir des supports de confiance issus de la chaîne de masterisation. Les supports de type USB peuvent être utilisés depuis des postes blancs ou verts pour déposer le contenu sur des serveurs de stockage sécurisés accessibles depuis les postes d'administration.

L'accès aux périphériques amovibles de type CD/DVD est autorisé sur les postes d'administration.

L'exécution automatique, déclenchée par l'insertion d'un support amovible, est proscrite.

Accès aux réseaux

Les équipements actifs réseau (commutateurs d'étage) qui desservent les prises réseaux des postes d'administration doivent bénéficier du même niveau de protection que celui du centre informatique. Il est de la responsabilité du STIC de vérifier l'adressage et la distribution des points d'accès aux réseaux d'administration aux seuls locaux autorisés.

Référence du document : RSSN-SSI-01-01	Page 48 / 62
Titre du document : PSSI CEA	Indice : 9

L'adressage logique (affectation des plages d'adresse et mise en place du filtrage) des bulles réseaux d'administration et des bulles serveurs est de la responsabilité de la DSI qui en délègue la réalisation aux USCI.

Audit / Contrôle

Le contrôle de conformité des prestations informatiques est assuré par le STIC.

L'ASSI du centre assure le contrôle de premier niveau des règles d'exploitation des centres informatiques et de leur respect de la présente PSSI. Il se coordonne avec l'officier de sécurité du centre sur les habilitations des personnels, les clauses de sécurité des marchés en cas de prestation extérieures et la protection physique des centres informatiques.

Le RSSI assure le contrôle de deuxième niveau sur le respect des règles d'exploitation de la présente PSSI, ainsi que sur l'exploitation des systèmes homologués.

L'audit des activités du RSSI et de la filière SSI est assuré dans le cadre des missions de l'Inspection Générale.

Référence du document : RSSN-SSI-01-01	Page 49 / 62
Titre du document : PSSI CEA	Indice : 9

8. SÉCURITÉ DU POSTE DE TRAVAIL

8.1 Sécurisation des postes de travail

La sécurité du poste de travail est un élément primordial de la sécurité des systèmes d'information dans la mesure où il s'agit le plus souvent du premier point d'exposition à la menace. La protection des postes de travail repose sur les mécanismes suivants²⁰ :

- raccordement de la ressource à un annuaire d'authentification centralisé,
- inventaire du matériel auprès du STIC,
- configuration et sécurisation maîtrisées par le STIC (OS, socle logiciel, masterisation),
- relevé de configuration automatique et centralisé des postes,
- mise à jour logiciel et correctifs de sécurité,
- journalisation des activités du poste et collecte centralisée,
- antivirus avec pilotage de la politique par le STIC,
- outil de chiffrement de surface pour les portables avec authentification pré-boot contre le vol et les attaques bas niveau,
- outil de chiffrement de surface pour les postes fixes contre le vol et les attaques bas niveau,
- outil de chiffrement « patrimoine » pour la protection des données contenues sur le poste,
- navigateur durci pour naviguer sur internet,
- droits d'administration locaux en tant que de besoin et distincts du profil utilisateur courant,
- restriction d'accès à distance par firewall local, aucune communication entrante à l'exception des postes administrateurs du STIC affectés au support.

Ces mesures sont déclinées dans la suite de ce chapitre.

8.1.1 Mise à disposition du poste

Fourniture et gestion des postes de travail

Les postes de travail doivent être fournis à l'utilisateur exclusivement par le STIC après accord du chef de service, approvisionnement du poste, mise en conformité, inventaire et attribution. Les postes de travail doivent être étiquetés avec leur numéro d'inventaire unique attribué par le STIC.

Il est interdit de traiter des données professionnelles sur des équipements personnels.

Par défaut, les postes de travail d'utilisateurs extérieurs non CEA sont proscrits en dehors de la zone d'hébergement. Une autorisation locale d'emploi d'une durée d'un trimestre, peut être accordé sur la base d'une analyse exhaustive de risque et d'une mise en conformité du matériel, par la STIC, avec la présente PSSI.

Le processus de réforme doit s'appliquer à ces matériels – notamment destruction systématique des supports de données non préalablement chiffrés à l'entrée sur le site.

Formalisation de la configuration des postes de travail

Les configurations des postes de travail doivent être formalisées par le STIC sur la base des accords nationaux pour les matériels, des spécifications validées par la DSI et des services mis en œuvre par le centre.

²⁰ s'applique à l'ensemble des postes dit conformes. Tout poste ne respectant un seule de ces conditions est qualifié de non conforme et doit être isolé, ou est traité selon un régime dérogatoire

Référence du document : RSSN-SSI-01-01	Page 50 / 62
Titre du document : PSSI CEA	Indice : 9

8.1.2 Sécurité physique des postes de travail

Verrouillage de l'unité centrale des postes fixes

Tous les postes doivent faire l'objet d'un chiffrement de surface et d'une maîtrise par le STIC du BIOS (cf. § 7.6.2).

Postes portables

Tous les postes portables doivent faire l'objet d'un chiffrement de surface antivol avec authentification au démarrage de la station (pré boot).

Les postes de travail portable doivent être remis à l'utilisateur avec :

- un filtre de confidentialité (obligatoire),
- un câble de sécurité antivol (facultatif).

Les utilisateurs doivent également être sensibilisés par l'Officier de sécurité :

- pour des déplacements hors UE sur le risque d'interception, et sur la nécessité d'utiliser des portables spécifiques et blanchis (c.-à-d. sans aucune données) pour ce type de déplacement, matériel éventuellement mis en commun au niveau de l'unité,
- à l'usage des enveloppes scellées pour les appareils laissés en consigne (facultatif),
- à l'usage d'un filtre de confidentialité (obligatoire),
- à l'usage d'un câble de sécurité antivol (facultatif).

Postes CEA en zones d'accueil du public ou en salles de réunion en accès libre

Dans les zones d'accueil au public ou les salles de réunion en accès libre, les postes informatiques doivent disposer :

- de protections antivols,
- de scellés de sécurité pour détecter les ouvertures de châssis matériel ou la manipulation des câbles des périphériques (clavier, souris, connectique écran, connectique réseau, etc.),
- de la neutralisation des ports USB et connectiques non utilisées par des dispositifs adéquats.

L'intégrité physique du matériel doit être contrôlée périodiquement et toute anomalie doit être signalée sans délai à l'ASSI du Centre.

8.1.3 Réaffectation du poste et récupération d'informations

En cas de cessation d'activité ou de changement de matériel, un poste de travail peut être réaffecté au même niveau de sensibilité après l'effacement de ce dernier (cf. § 7.6.2).

Lorsqu'un utilisateur est amené à cesser son activité, à l'exception de sa boîte aux lettres de messagerie individuelle qui ne peut être transférée, l'ensemble des données de l'utilisateur peut être transféré par le STIC sur demande de l'ASSI de l'unité, ces données étant réputées professionnelles.

Conformément à la charte informatique, l'utilisateur en est informé et est invité à extraire ses éventuelles données à caractère privé préalablement à sa cessation d'activité.

À défaut, en cas de cessation d'activité, le STIC procède à l'archivage des données utilisateurs pour une période de six mois avant destruction définitive en l'absence d'avis contraire.

8.1.4 Gestion des privilèges sur les postes de travail

Privilèges des utilisateurs sur le poste de travail

Les utilisateurs ne disposent pas des droits d'administration sur leur poste de travail avec leur compte du domaine.

Référence du document : RSSN-SSI-01-01	Page 51 / 62
Titre du document : PSSI CEA	Indice : 9

Utilisation des privilèges d'accès "Administrateur"

Les accès administrateur à distance sur un poste de travail sont réservés aux STIC et aux administrateurs affectés au support en provenance des réseaux d'administration de niveau vert.

L'accès à distance en tant qu'administrateur à un poste de travail est proscrit pour les comptes d'administration affectés également à des serveurs (administrateurs rouges, administrateurs jaunes et verts). Les personnels en charge de l'administration utilisent leur compte blanc ou un compte spécifique sans aucune prérogative d'administration sur des services, pour effectuer les opérations de prise en main à distance sur les postes utilisateurs. Pour rappel, cette mesure est la seule protégeant le périmètre d'administration en cas d'intervention à distance sur un poste compromis.

Gestion du compte "Administrateur local"

Sur autorisation de l'ASSI centre, un utilisateur qui doit disposer des droits d'administration local, se voit octroyer un compte d'administration distinct de son compte utilisateur du domaine. Les mécanismes d'élévation ponctuels des privilèges doivent être mis en œuvre (UAC, sudo) pour limiter l'exposition des privilèges au strict minimum.

L'ASSI de centre peut prononcer des dérogations sur des environnements scientifiques très spécifiques liés au développement système par exemple. Les mesures dérogatoires doivent s'accompagner d'un placement de ces postes dans la bulle « Postes non conformes ».

8.1.5 Protection des informations

Stockage des informations

Les informations professionnelles doivent être stockées sur les ressources de stockage mutualisé du centre. Le STIC est responsable de la planification des besoins en termes de capacité de stockage vis-à-vis des unités implantées sur son centre.

Le stockage sur le poste de travail, sur support amovible ou sur stockage local, doit bénéficier des mêmes niveaux de protection en termes de confidentialité et d'intégrité (chiffrement pour les données Diffusion restreinte à l'aide d'un outil qualifié standard) mais ne peut se prévaloir des mêmes capacités de disponibilité ou de préservation.

Lorsque les activités du service dépendent de la disponibilité des données, l'ASSI d'unité doit valider les solutions de stockage retenues pour vérifier leur adéquation en cas de sinistre, et leur conformité au PCA.

Pour protéger l'accès aux informations en l'absence de l'utilisateur, la mise en place d'un système de verrouillage de session inactive au-delà de 15 minutes d'inactivité doit être mise en œuvre par défaut.

En cas de stockage local, l'utilisateur est tenu de s'assurer de la préservation des données en cas de sinistre.

Sauvegarde / Synchronisation des données locales

Le stockage d'information sur la machine (stockage local) doit relever d'une dérogation pour besoin de service justifiée par le chef d'unité et après validation de l'ASSI.

Lorsque l'ASSI d'unité valide des capacités de stockage sur poste ou sur des ressources locales, il doit s'assurer des capacités de synchronisation avec les espaces de stockage du centre pour sauvegarde et archivage.

En l'absence de mécanisme de synchronisation mis en œuvre par le STIC, la préservation des données locale n'est pas garantie. Le stockage local ne peut alors être utilisé que pour des documents temporaires ou de travail dont la perte ou la destruction est admissible.

Pour rappel, l'utilisation de service externalisé (ex. Dropbox, Google Drive, OneDrive ...) pour le stockage des informations professionnelles est proscrite, sans autorisation préalable dans le contexte d'une homologation CEA.

Partage de fichiers ou de ressources

Le partage de fichiers ou la mise à disposition de ressources de stockage depuis un poste de travail vers d'autres postes est proscrit. Seules les ressources de type serveur peuvent assurer la fonction de partage de fichiers.

Référence du document : RSSN-SSI-01-01	Page 52 / 62
Titre du document : PSSI CEA	Indice : 9

Les échanges directs, le partage de ressources entre postes de travail sont proscrits (ceci inclut les suites logicielles de partage de ressources mutualisés entre plusieurs postes).

Suppression des données sur les postes partagés

Les postes partagés, qui ne sont pas affectés à l'usage exclusif d'un utilisateur, doivent faire l'objet d'un traitement particulier contre la rémanence des informations dès lors qu'ils ne sont pas utilisés par des utilisateurs ayant le même besoin d'en connaître.

En particulier :

- les postes mis à disposition dans les salles de réunion,
- les postes nomades dédiés aux déplacements à l'étranger,
- les postes en libre-service.

Il est recommandé de déployer des techniques de virtualisation (mode kiosque) ou des terminaux passifs déportés sans rémanence pour ce type d'usage.

Chiffrement des données sensibles

À l'exception des postes en zone Extranet et en zone Hébergement (non éligibles au traitement d'informations sensibles), tous les postes de travail doivent disposer d'un outil de chiffrement qualifié standard, validé par le RSSI et mis en œuvre conformément aux spécifications d'exploitation de la DSI.

Cet outil de chiffrement est exigé pour permettre le traitement, le stockage et la transmission éventuelle d'information « Diffusion Restreinte » et est utilisable pour la transmission du Diffusion Ordinaire sur des supports vulnérables (USB, mails externes, partages Internet...).

Les niveaux de classification supérieurs font l'objet d'un chiffrement évalué dans le contexte de leur homologation.

Protection des flux d'informations

L'information en transit est en partie protégée par les protocoles réseaux mis en œuvre. Ces protocoles doivent intégrer un chiffrement à l'état de l'art.

Les outils en charge de ces flux doivent faire l'objet d'une validation DSI et ne pas être interdit par DSSN.

Fourniture de supports de stockage amovible

Les supports de stockage amovibles sont approvisionnés par le STIC dans le cadre des accords nationaux. Les supports proposant des fonctions de chiffrement embarqués sont proscrits en dehors des dispositifs labellisés ANSSI utilisés conformément à une politique d'emploi validée par le RSSI.

8.1.6 Nomadisme

Accès à distance aux Systèmes d'Information de l'entité

Les postes en situation de nomadisme (cf. § 7.6.3) peuvent sur autorisation du chef d'unité pour les besoins d'un utilisateur (qui se traduit par l'obtention d'un MOBI-Pass) disposer de 3 services nomades :

- MOBI-Standard : Authentification forte, services limités, usage admis depuis des terminaux non maîtrisés - accès à certaines applications sélectionnées et validée au travers d'un portail de publication spécifique
- MOBI-Étendu : Authentification forte, services non limités, usage exclusif depuis des terminaux maîtrisés et conformes à la PSSI, usage de la messagerie sécurisée autorisée - accès à l'ensemble des ressources informatiques du CEA (domaine Intra)
- MOBI-Push : Authentification faible, service limité à la messagerie, usage exclusif depuis des terminaux maîtrisés et conformes à la PSSI, interdiction d'usage de la messagerie sécurisée (aucune clé privée sur les terminaux n'est autorisée) - accès réservé uniquement à la messagerie (hors messagerie sécurisée)

Référence du document : RSSN-SSI-01-01	Page 53 / 62
Titre du document : PSSI CEA	Indice : 9

Pare-feu local

Tous les postes nomades disposent d'un antivirus local qui assure la fonction pare-feu en situation de nomadisme. La politique pare-feu « NO-INBOUND²¹ » est mise en œuvre de manière automatique pour les postes en situation de nomadisme. Le STIC est en charge de la mise en œuvre de cette politique sur l'ensemble des postes de travail des utilisateurs.

Stockage local d'information sur les postes nomades

Le stockage local d'information sur les postes nomades doit être limité au strict nécessaire. Il est considéré comme temporaire et doit être limité au besoin de la mission au profit des échanges à travers les offres MOBI qui assurent la protection des données stockées.

Tous les postes nomades doivent disposer d'un outil de chiffrement qualifié standard s'il est nécessaire de traiter des informations de niveau « Diffusion restreinte ».

Les services MOBI-Standard autorisés sur des terminaux non maîtrisés doivent assurer l'absence de stockage local des informations sur le poste ou leur destruction à la fin de la session.

Filtre de confidentialité

Tous les postes nomades doivent disposer d'un filtre de confidentialité fournis lors de l'attribution du poste à l'utilisateur.

Configuration des interfaces de connexion sans fil

Les interfaces de connexion sans fil ne sont activées, sur les matériels nomades, que lorsqu'elles sont utilisées. L'usage des technologies sans fil pour l'utilisateur en situation de nomadisme est placé sous sa responsabilité.

L'utilisateur est formé à l'utilisation des offres MOBI-Étendu préalablement à l'utilisation de son poste. L'ASSI d'unité à en charge la sensibilisation des utilisateurs quant à l'utilisation de l'offre MOBI-Étendu en particulier l'ouverture de session VPN préalable à l'utilisation du poste (option « VPN before login »).

Désactivation des interfaces de connexion sans fil

L'utilisateur est sensibilisé à la désactivation de ses interfaces de connexion sans fil, communément appelée « Mode avion ».

Utilisation des outils nomades dans le cadre du Télétravail

Le télétravail requiert obligatoirement une autorisation d'accès à l'offre MOBI-Étendu.

8.2 Sécurisation des copieurs multifonctions

Durcissement des imprimantes et copieurs multifonctions

Les imprimantes et les copieurs multifonctions font partie d'un marché national dont le cahier des charges intègre les spécifications nationales SSI validées par le RSSI. Seuls les matériels issus de ce marché national sont autorisés. Le STIC a la responsabilité de mettre en œuvre les mécanismes de protection sur les équipements déployés suivant les directives nationales.

Sécurisation de la fonction numérisation

Les seules fonctions de numérisation autorisées sont :

- la numérisation des documents vers la messagerie limitée aux adresses internes CEA,
- la numérisation des documents à destination des ressources de stockage prévues à cet effet sur le centre,
- la numérisation des documents à destination d'un support amovible sous la responsabilité de l'utilisateur.

²¹ Fermeture de l'ensemble des ports de communications entrants, sauf depuis les réseaux d'administration

Référence du document : RSSN-SSI-01-01	Page 54 / 62
Titre du document : PSSI CEA	Indice : 9

8.3 Sécurisation de la téléphonie

Les smartphones sont considérés comme des postes de travail nomades et ne sont pas traités dans ce chapitre.

Sécurisation de la téléphonie

La téléphonie (fixe et mobile) n'est pas considérée comme un moyen de communication sécurisé et ne peut pas traiter des informations autres que Diffusion Ordinaire.

Les outils de communication mis à disposition sur les postes (Audio et Vidéo Conférence) qui bénéficient de la protection du réseau de transport dans le cadre de leur homologation sont privilégiés pour les échanges de données sensibles.

Sécuriser la configuration des autocommutateurs

Les autocommutateurs et les services de téléphonie accessibles depuis les réseaux opérateurs sont filtrés vis-à-vis du réseau de données CEAnet. Ces règles s'appliquent aux équipements raccordés directement au réseau opérateurs (exemple : visioconférence, fax, ...).

Ils sont déployés sur des ressources propres qui sont filtrées vis-à-vis des réseaux bureautiques et scientifiques pour éviter qu'une compromission de ces équipements puisse occasionner une perte d'intégrité sur le réseau de données. L'ouverture des services est limitée et soumise à l'accord préalable de l'ASSI du centre concerné après validation par le RSSI.

Codes d'accès téléphoniques

Les codes d'accès téléphoniques ne doivent être utilisés que si les services associés sont demandés par l'utilisateur. Les services de type « boîte vocale » doivent être invalidés par défaut.

Lorsque ces services sont mis en œuvre à la demande de l'unité, le STIC doit veiller à la mise en œuvre de code d'accès de 6 chiffres minimum et l'utilisateur du service doit être formé au changement de ce code personnel.

DECT

L'usage du protocole DECT²² est limité aux communications courantes et est proscrit pour l'échange d'informations sensibles à partir du niveau « Diffusion Restreinte ».

Les bornes de communication DECT sont regroupées au sein de réseaux dédiés et filtrés vis-à-vis des autres réseaux. Seuls les protocoles indispensables à leur fonctionnement sont admis avec les relais de communication.

8.4 Contrôles de la conformité des postes de travail

Utiliser des outils de vérification automatique de la conformité

Il est de la responsabilité des STIC de déployer l'ensemble des postes de travail de leur périmètre en respectant les processus suivants :

- un enregistrement du poste de travail dans le service de résolution de noms DNS CEA,
- un enregistrement du poste de travail dans l'annuaire Active Directory de référence,
- l'installation de l'agent Antivirus configuré suivant la politique nationale,
- l'installation d'un agent de collecte (relevé de la configuration logicielle) alimentant les serveurs nationaux,
- la configuration de la politique de journalisation nationale,
- la mise en place de la collecte des journaux d'activité vers les collecteurs du centre de supervision,
- la mise à jour de l'inventaire.

²² qui est considéré comme un téléphone fixe (cf. § 1-Préambule), par opposition à la téléphonie mobile, mais nécessite néanmoins des mesures spécifiques.

Référence du document : RSSN-SSI-01-01	Page 55 / 62
Titre du document : PSSI CEA	Indice : 9

À partir de ses informations, l'ensemble des postes²³ fait partie d'un processus de vérification de la conformité sous la maîtrise du STIC. Ces rapports de conformité du parc sont mis à disposition des ASSI de centre et du RSSI. Les anomalies détectées font l'objet de traitement d'incident (de type « Anomalie »).

²³ y compris les postes d'administration, blanc, verts, jaunes et rouges

Référence du document : RSSN-SSI-01-01	Page 56 / 62
Titre du document : PSSI CEA	Indice : 9

9. SÉCURITÉ DU DÉVELOPPEMENT DES SYSTÈMES

9.1 Prise en compte de la sécurité dans le développement des SI

Intégrer la sécurité dans les développements locaux

Les développements applicatifs relevant des serveurs mutualisés à l'échelle du périmètre du centre ou du périmètre national sont placés sous la maîtrise d'ouvrage du STIC ou de la DSI. Lorsque ces développements relèvent de systèmes d'information soumis à homologation, leur mise en production est soumise à l'accord préalable de l'autorité d'emploi après avis de l'autorité d'homologation.

Les personnels en charge du développement doivent utiliser des environnements dédiés à cette activité sans aucun impact avec les systèmes en production.

Intégrer des clauses SSI dans les contrats de sous-traitance de développement informatique

Toutes les prestations de sous-traitance de développement informatique sont soumises à l'accord préalable de l'officier de sécurité du périmètre concerné. Ce dernier spécifie le type de marché et la mise en œuvre d'une annexe de sécurité si des informations sensibles sont détenues par le prestataire.

Les clauses SSI de l'annexe de sécurité sont spécifiées par l'ASSI de l'unité, elles définissent des mesures de protection pour le développeur conformes au niveau de sensibilité du marché.

Les postes de travail des développeurs sont soumis aux mêmes protections que les postes de travail des utilisateurs CEA lorsque la prestation est internalisée et à des protections équivalentes lorsque celle-ci est externalisée. En fonction de la nature de l'application développée, des protections supplémentaires peuvent être mises en œuvre pour s'assurer de l'intégrité du développement (communication vers internet proscrite, usage de la messagerie interdit, règles d'usage des supports amovibles, gestion des sources de référence et de confiance...).

9.2 Prise en compte de la sécurité dans le développement des logiciels

Limiter les fuites d'information

Les informations techniques fournies dans le cadre de la prestation ne peuvent dépasser le niveau de sensibilité du marché spécifié par l'officier de sécurité. Le titulaire doit disposer des mêmes protections pour le développement que les utilisateurs qui accèdent aux informations de même niveau de sensibilité.

Les échanges d'information doivent être protégés en confidentialité par des outils de chiffrement adaptés au niveau de sensibilité traité.

Réduire l'adhérence des applications à des produits ou technologies spécifiques

Il est de la responsabilité du STIC de vérifier l'adéquation des technologies utilisées avec les standards de conformité édictés par la DSI. Cette adéquation tant sur le matériel que sur les logiciels mis en œuvre doit être validée par le STIC avant la passation du marché.

Instaurer des critères de développement sécurisé

Les critères de sécurité liés aux équipements utilisés par les développeurs dépendent de la sensibilité des informations traitées mais également de la finalité du service développé (une perte d'intégrité durant la phase de développement peut avoir un impact fort sur la sécurité du système une fois en production).

Concernant la sensibilité des données traitées par le développeur.

	CD/SD	CCEA	Diffusion Restreinte	Diffusion Ordinaire
Marché	Classé ou à clause	Sensible	Sensible	Ordinaire
Développement	Sur système homologué	Sur système homologué	Dépend de la finalité du service (peut nécessiter une homologation pour le SI de développement)	

Référence du document : RSSN-SSI-01-01	Page 57 / 62
Titre du document : PSSI CEA	Indice : 9

Le développement d'un service doit être réalisé dans un environnement qui limite la capacité d'une cyber-attaque visant à implémenter du code malveillant dans un service critique

Finalité	Service Rouge	Service Jaune	Service Vert	Service local
Développement	Poste isolé internet Messagerie DR Supports fournis par le CEA	Poste isolé internet Messagerie DR Supports fournis par le CEA	Internet autorisé Messagerie autorisée	

Intégrer la sécurité dans le cycle de vie logiciel

Il est de la responsabilité du chef de projet de veiller au respect des règles de sécurité prescrites dans le cahier des charges et d'intégrer la vérification des mécanismes de sécurité dans les phases de recette. Le chef de projet est également en charge de fournir les conditions de maintenance applicative pour garantir le maintien de sécurité ainsi que les modalités d'accès aux événements de sécurité (authentification, modification des droits d'accès, violation d'usage) à la supervision.

Améliorer la prise en compte de la sécurité dans les développements Web

Les développements d'application Web font l'objet de vérification du niveau de sécurité par des outils de scans automatisés. La correction des vulnérabilités génériques découvertes sur un développement Web incombe au chef de projet. L'absence de correction est susceptible de conduire à un retard de la mise en production.

Calculer les empreintes de mots de passe de manière sécurisée

La mise en œuvre du mécanisme d'authentification propre à l'application doit être évitée au profit d'une authentification centralisée reposant notamment sur les annuaires Active Directory et sur des protocoles d'authentification robustes ou sur la détention d'un certificat de l'IGC CEA.

- Il est également recommandé de mettre en place une autorisation basée sur des groupes de sécurité d'appartenance dans les annuaires Active Directory..

Lorsque l'application nécessite un annuaire propre d'authentification ou d'autorisation, les mécanismes d'authentification ou d'autorisation doivent être validés par l'ASSI de l'unité qui s'assure de leur conformité avec la présente PSSI. Le stockage d'éléments d'authentification de l'utilisateur en clair ou par un chiffrement réversible est proscrit.

9.3 Sécurisation des applications à risques

Mettre en œuvre des fonctionnalités de filtrage applicatif pour les applications à risque

Dans le cadre de l'homologation d'application, compte tenu de l'évaluation des risques résiduels et pour améliorer la protection des données face à des attaques portant sur l'applicatif, certaines solutions tierces de filtrage applicatif doivent être mises en œuvre. L'utilisation de proxy assurant des opérations de filtrage applicatif (en particulier entre les flux d'administration et les flux d'usage) est recommandée sur les applications exposées au réseau public comme internet.

Référence du document : RSSN-SSI-01-01	Page 58 / 62
Titre du document : PSSI CEA	Indice : 9

10. TRAITEMENT DES INCIDENTS

10.1 Chaînes opérationnelles

10.1.1 Traitement des alertes de sécurité émises par l'ANSSI

Chaînes opérationnelles SSI

Les alertes émises par l'ANSSI au niveau national sont adressées :

- aux listes alertes : alerte-ssi@cea.fr
- au service S³I de DSSN : alerte-ssi-dssn@cea.fr pour les recherches de marqueurs
- au CCC – en cas de succession ou de situation Piranet.

Mobilisation en cas d'alerte

Les alertes de sécurité sont traitées conjointement par les membres des listes : alerte-ssi@cea.fr et alerte-ssi-dssn@cea.fr. Elles font l'objet d'un traitement local en se reposant sur les membres des listes d'alertes définies pour chaque établissement.

Les signalements ou directives organisationnelles sont relayés auprès des ASSI concernés.

Sur incident majeur (type CRISE), DSSN assure la coordination avec l'administration générale du CEA par le biais du Centre de Coordination de Crise.

10.1.2 Remontée des incidents de sécurité rencontrés

Qualification et traitement des incidents

Les alertes sont qualifiées suivant leur impact et leur périmètre.

On distingue les événements de type :

- Anomalie : signal faible, justifie une levée de doute auprès de l'exploitation et de l'utilisateur, niveau utilisé pour traiter les non-conformités à la PSSI,
- Incident : des événements dans les journaux indiquent une menace interceptée par les équipements de sécurité,
- Alerte : des événements dans les journaux indiquent une menace non interceptée ou partiellement par les équipements de sécurité,
- Crise : Les événements relèvent d'une cyber attaque avérée et en cours. Ces événements significatifs peuvent faire l'objet d'un signalement auprès du COSSI (CERT-FR)

Les incidents portant atteinte à la disponibilité sont pris en charge et qualifiés par l'exploitation. Les incidents portant atteinte à l'intégrité et à la confidentialité sont pris en charge et qualifiés par le RSSI.

Remontée des incidents

Les incidents de type crise font l'objet d'un signalement auprès de l'administration générale du CEA et du COSSI par le relais du RSSI.

Référence du document : RSSN-SSI-01-01	Page 59 / 62
Titre du document : PSSI CEA	Indice : 9

11. CONTINUITÉ D'ACTIVITÉ

11.1 Gestion de la continuité d'activité

11.1.1 Mise en œuvre plan local de sécurité des Systèmes d'Information (PSI)

Définition du plan local de sécurité des Systèmes d'Information (PSI)

Un PSI maintient l'activité informatique, lié à une activité métier critique, et/ou permet la remise en service dans les plus brefs délais possibles, tout en réduisant les conséquences financières.

Ce plan intervient dans le but d'atténuer l'impact des catastrophes pour sauver l'activité, mais aussi pour assurer un niveau de fiabilité auprès des partenaires et clients.

L'objectif est de pallier les menaces pesant sur l'activité du CEA en trouvant des solutions de prévention adéquates.

Un PSI se décline en :

Plan de continuité d'activité – PCA des SI

- vise à réduire au minima une interruption d'activité du système d'information et des activités en dépendant en cas de sinistre – implique une redondance de l'ensemble des équipements et infrastructure, et en terme informatique une double localisation d'exploitation (double site chaud)²⁴

Plan de reprise d'activité – PRA des SI

- vise à limiter à un délai réduit, prédéterminé, et accepté préalablement par l'autorité d'emploi, une interruption d'activité du système d'information et des activités en dépendant en cas de sinistre – implique une redondance partielle des équipements et infrastructure (site chaud et site de repli)

Plan de protection du patrimoine (protection des seules données) – PPP des SI

- vise à protéger le seul patrimoine de données des conséquences d'un sinistre, pour une reprise de l'activité ultérieure (sans obligation a priori de délai) nécessite un plan de sauvegarde des données

Il est de la responsabilité du STIC de disposer d'un inventaire exhaustif des systèmes d'information à haute valeur/risque relevant de leur périmètre. Ces applications/données sont identifiées par les unités à l'aide des études d'impact. Les applications/données relevant d'un risque de pertes inacceptables²⁵ dans la cartographie des risques de la direction générale du CEA sont déclarées auprès du RSSI.

L'ASSI de centre a un droit de regard sur l'inventaire.

En cas d'adhérence avec les infrastructures nationales (serveurs nationaux, réseau de transport CEAnet ou accès internet, messagerie), les applications nécessitant une haute disponibilité²⁶ doivent impérativement être portées à la connaissance de la DSI et du RSSI.

Sur la base du Plan de continuité d'activité du centre, le STIC décline le Plan de sécurité informatique [PSI].

Suivi de la mise en œuvre du plan de continuité d'activité local des Systèmes d'Information (PCA des SI)

L'ASSI de Centre s'assure de la bonne mise en œuvre par la chaîne informatique (DSI - USCI - STIC) du volet SI – PSI locale, et des dispositions prévues dans le « plan de continuité d'activité du centre ».

Les ASSI d'unité établissent les procédures dites de secours en cas d'indisponibilité durable du système d'information.

²⁴ s'applique aux activités nécessitant un haut besoin en terme de disponibilité

²⁵ Risques pour la population, risque pour l'image, risque pour la santé, risque pour l'activité du CEA, risque pour les engagements du CEA ... - liste non exhaustive

²⁶ Exigence de fonctionnement en mode 24/7 avec une tolérance d'interruption maximale de 4 heures par mois

Référence du document : RSSN-SSI-01-01	Page 60 / 62
Titre du document : PSSI CEA	Indice : 9

Mise en œuvre des dispositifs techniques et des procédures opérationnelles

Il est de la responsabilité du STIC d'assurer le maintien en condition opérationnelle des procédures et dispositifs techniques de secours détaillés dans le PCA du centre.

Protection de la disponibilité des sauvegardes

Les sauvegardes des données relevant du PRA du centre doivent être gérées conformément à la stratégie de sauvegarde et d'archivage spécifiée par la DSI.

Protection de la confidentialité des sauvegardes

Conformément à l'architecture de stockage et de sauvegarde, les sauvegardes de données bénéficient de la même protection que les données sauvegardées en termes de confidentialité.

11.1.2 Maintien en conditions opérationnelles du plan local de sécurité des SI (PSI)

Exercice régulier du plan local de sécurité des Systèmes d'Information (PSI)

À l'initiative de l'ASSI de centre, des exercices annuels sont mis en œuvre par le STIC pour vérifier l'intégrité des deux sites de production et du site mort de stockage en cas de sinistre. En cas d'adhérence avec les infrastructures nationales, le RSSI et la DSI doivent être informé en amont de l'opération. Les USCI doivent participer à la mise en œuvre de l'exercice, notamment au regard des impacts sur les infrastructures nationales.

Mise à jour du plan local de sécurité des Systèmes d'Information (PSI).

L'ASSI de centre assure le maintien à jour du plan local de sécurité des Systèmes d'Information (PSI) de son centre. La DSI assure le maintien à jour du plan local de continuité d'activité des systèmes d'information des infrastructures nationales.

Le RSSI valide le plan de continuité d'activité des systèmes d'information d'importance vitale dans le cadre du processus d'homologation.

Référence du document : RSSN-SSI-01-01	Page 61 / 62
Titre du document : PSSI CEA	Indice : 9

12. CONFORMITÉ, AUDIT, INSPECTION ET CONTRÔLE

12.1 Contrôles réguliers

Contrôles locaux

Le STIC contrôle la sécurité de ses serveurs, la mise en œuvre des protections de ses administrateurs, la bonne gestion des droits d'administration et la conformité de ses services avec la présente PSSI. Le STIC assure aussi le traitement des incidents de son périmètre en termes de remédiation.

Les ASSI de Direction opérationnelle sont responsables de l'application de la politique de classification de leur direction en accord avec l'officier de sécurité. Ils contrôlent également le respect de la politique de publication de leur direction conformément à la NIG sur la publication (politique qui spécifie pour la direction le mécanisme de délégation de la responsabilité éditoriale et les conditions d'obtention du « droit à publier ») dans le cadre de la mise en œuvre de sites internet de publication.

Les ASSI de centre sont responsables du contrôle de conformité de la présente PSSI dans les pratiques d'administration et les services mis en œuvre par le STIC du centre.

Les ASSI d'unité sont responsables du contrôle de conformité de la présente PSSI dans leur unité (cf. § 2.1.4).

Bilan Annuel

Le RSSI est responsable de l'élaboration du bilan annuel pour le CEA. Ce bilan annuel est validé par l'AQSSI et présenté en CSI.

Référence du document : RSSN-SSI-01-01	Page 62 / 62
Titre du document : PSSI CEA	Indice : 9

13. ANNEXES

13.1 Documents de référence

- NIG 672 & 707 : Organisation générale du CEA
- NIG 660 : Publication de travaux à caractère scientifique ou technique
- NIG 613 : Organisation de la sécurité au CEA
- NIG 608 : Charte d'utilisation des moyens informatiques et des services internet au CEA
- NIG 695 : DSSN Missions et organisation
- NIG 708 : DARCI Missions et organisation
- NIG 709 : IGN Missions et organisation
- RGPD : Politique interne : Mise en œuvre au CEA de la réglementation sur la protection des données à caractère personnel

13.2 Documents abrogés par la présente PSSI

- PGPSI : Politique Générale des Systèmes d'Information [DCS/ACI/SSI/REG/4.2/0002]
- PSR : Politique Sécurité Réseau CEA [DCS/ACI/SSI/REG/4.2/0031]
- PSSI : Plan SSI de Centre [DCS/ACI/SSI/REG/4.2/0030]
- PSSI 2017 [SPACI-SSI-REG-0324]
- Circulaire DCS n° 15
- Circulaire DCS n° 16
- Circulaire DCS n° 29