

BERCY 3
10, RUE DU CENTRE
93464 NOISY-LE-GRAND CEDEX
Standard : (+33) 1 57 33 99 00

Politique de sécurité du système d'information interne de l'AIFE

Destinataires : Direction AIFE
Responsables de délégation
Tout personnel AIFE
Tout prestataire AIFE

Rédacteur : AQSSI
Vérificateur :
Approbateur : Direction

Version - Date	Emetteur	Statut/Suivi des modifications
V1.0 – 31/08/2006	Directeur AIFE	Validée
V2.0 – 19/02/2007	Directeur AIFE	Validée
V3.0 – 08/01/2008	Directeur AIFE	Validée
V4.0 – 20/11/2012	AQSSI	Validée
V4.1 – 10/07/2017	AQSSI	Validée / Mise à jour charte AIFE
V5.0 – xx/xx/2020	AQSSI	Prise en compte de la PSSIE, du RGPD, adaptations et mobilité



Objectif du document | Politique de Sécurité des systèmes d'information de l'AIFE

Mots clefs | PSSI

Résumé | Règles à appliquer en matière de sécurité des systèmes d'information au sein de l'AIFE

Sommaire

1	Objet et portée du document	4
2	Pourquoi une démarche de sécurité de l'information ?	4
3	Engagement de la direction de l'AIFE	5
4	La démarche de sécurité de l'information de l'AIFE	5
4.1	Principes de la démarche	5
4.2	Périmètre d'application	6
5	Organisation de la démarche.....	6
5.1	Implication et responsabilités individuelles.....	6
5.2	Direction de l'AIFE	6
5.3	Autorité Qualifiée en Sécurité des Systèmes d'information (AQSSI)	7
5.4	Responsable de la Sécurité des Systèmes d'Information (RSSI)	7
5.5	Référent à la protection des données personnelles	8
5.6	Equipe sécurité des systèmes d'information (SSI).....	8
5.7	Fonctions transverses	8
5.8	Maîtrise d'ouvrage déléguée	8
5.9	Maîtrise d'œuvre.....	9
5.10	Exploitants.....	9
5.11	Utilisateurs des SI de l'AIFE.....	9
6	Les règles à l'AIFE en matière de SSI	10
6.1	Principe général de la PSSI.....	10
6.2	Organisation, responsabilité et contrôle de la SSI	10
6.2.1	Organisation de la SSI	11
6.2.2	Responsabilités des autorités chargées de l'application à l'AIFE de la PSSI.....	11
6.2.3	Documentation de sécurité	11
6.3	Sécurité liée au personnel	12
6.3.1	Formation du personnel	12
6.3.2	Responsabilité et sensibilisation du personnel.....	12
6.4	Sécurité des biens physiques et matériels.....	13
6.5	Protection des données à caractère personnel	14
6.6	Sécurité physique des locaux	14
6.7	Sécurité des communications et des flux	15
6.8	Exploitation des SI	16
6.8.1	Protection des informations	16
6.8.2	Habilitations sur les systèmes d'information	17
6.8.3	Gestion des authentifiants	18
6.8.4	Traçabilité et supervision de la sécurité	19
6.8.5	Poste des exploitants.....	20
6.8.6	Maintien en conditions de sécurité et lutte contre les codes malveillants.....	21
6.8.7	Envoi en maintenance, mise au rebut, réaffectation de matériel informatique	21

6.9	Traitement des incidents de sécurité	22
6.10	Continuité d'activité	22
6.10.1	Maintien permanent de la SSI	23
6.10.2	Homologation d'un système d'information ou de ses composants.....	23

DOCUMENTS DE REFERENCE

Référence	Titre
Instruction interministérielle 1300/SGDN/PSE/PSD du 30 novembre 2011	Protection du secret de la défense nationale
Instruction interministérielle n°920/SGDN/DCSSI/DR du 12 janvier 2005	Systèmes traitant d'informations classifiées de défense de niveau Confidentiel-Défense
Recommandation n°901/DISSI/SCSSI du 2 mars 1994	Protection des systèmes d'information traitant des informations sensibles non classifiées de défense
circulaire du Premier ministre n° 5725/SG (NOR : PRMX1420095C) du 17 juillet 2014	Politique de sécurité des systèmes d'information de l'état (PSSIE)
Arrêté du 1 ^{er} août 2016	Politique générale de sécurité des systèmes d'information des ministères économiques et financiers
RGS version 2.0 du 13 juin 2014	Référentiel général de sécurité
PSSI AIFE	Politique de sécurité des systèmes d'information de l'AIFE en vigueur
RGPD, Règlement (UE) 2016/679 du 27 avril 2016	Règlement Général de la Protection des Données à caractère personnel.
Arrêté du 22 janvier 2019	Arrêté du 22 janvier 2019 portant désignation des autorités qualifiées pour la sécurité des systèmes d'information dans les services d'administration centrale, les services déconcentrés, les organismes et établissements sous tutelle du ministre de l'économie et des finances et du ministre de l'action et des comptes publics

TABLE DES ABRÉVIATIONS

Abréviation	Signification
AIFE	Agence pour l'informatique financière de l'état
AQSSI	Autorité qualifiée en sécurité des systèmes d'information
DASEC	Demande d'avis sécurité
FISEC	Fiche d'incident de sécurité
FSSI	Fonctionnaire de sécurité des systèmes d'information
MOA	Maîtrise d'ouvrage
MOE	Maîtrise d'œuvre
PSSI	Politique de sécurité des systèmes d'information
PSSIE	Politique de sécurité des systèmes d'information de l'état
RGS	Référentiel général de sécurité
RSSI	Responsable de la sécurité des systèmes d'information
RGPD	Règlement général sur la protection des données à caractère personnel
SSI	Sécurité des systèmes d'information

1 OBJET ET PORTEE DU DOCUMENT

Le présent document traite de la politique de sécurité des systèmes d'information (PSSI) de l'AIFE. Il constitue à ce titre le document fondateur de la démarche de sécurité de l'information mise en œuvre au sein de l'AIFE et couvrant l'ensemble des systèmes d'information de l'agence hors SI Chorus et SI externalisés qui font l'objet de PSSI spécifiques.

Il a pour objectif de définir et mettre en place la Politique de Sécurité des Systèmes d'Information de l'AIFE. Il expose les principes et les règles à appliquer en matière de sécurité des systèmes d'information en s'assurant que leur application soit globale, adaptée et cohérente.

Il définit le cadre dans lequel la démarche de sécurité des SI, conformément à la volonté de la direction de l'AIFE. Il transcrit ainsi le soutien fort de la direction de l'AIFE dans la mise en place et le maintien de cette démarche de sécurité de l'information.

Cette PSSI doit être diffusée à l'ensemble des personnes intervenant directement ou indirectement pour le compte de l'AIFE, qui doivent en prendre connaissance et se conformer aux règles qui leur sont applicables, en tant que point de départ de leur indispensable engagement dans cette démarche.

2 POURQUOI UNE DEMARCHE DE SECURITE DE L'INFORMATION ?

Toutes les administrations et tous les services déconcentrés de l'Etat sont tenus de mettre en œuvre l'ensemble des mesures d'organisation, techniques et relatives à l'environnement visant à assurer la protection des systèmes d'information qu'ils utilisent.

L'évolution des technologies et les comportements des utilisateurs accentuent la menace pesant sur les systèmes d'informations. Celle-ci concerne tous les critères de la Sécurité des Systèmes d'Informations (SSI) : la confidentialité, l'intégrité, la disponibilité, la traçabilité et la non répudiation. L'analyse des risques dont les résultats sont soumis à la direction permet d'identifier ce qui doit être protégé, contre qui et à quel coût.

La modernisation de l'Etat et la maîtrise des aspects budgétaires font partie des toutes premières priorités au niveau national, car ce sont des éléments indispensables au développement de l'activité économique du pays et à l'amélioration de la qualité de vie des citoyens et des entreprises (réduction de la dette, amélioration et développement des services publics,...).

Une telle modernisation et une telle maîtrise ne peuvent se réaliser qu'au travers de la mise en œuvre de systèmes d'information performants et fiables. Dans ce cadre, l'AIFE, de par ses missions en matière de conception, de développement et de mise en œuvre des systèmes fédérateurs d'information financière de l'Etat (SIFE), a un rôle fondamental à jouer.

La sécurité des informations et des systèmes qui les traitent constitue un élément clé dont l'AIFE, ses personnels, ses partenaires et ses prestataires, ont la responsabilité.

La modification non-contrôlée de telles informations, l'impossibilité de traiter ou de fournir ces informations dans les délais requis par les différentes obligations réglementaires (nationales et européennes), la divulgation de certaines de ces informations ou l'impossibilité de tracer quelles actions ont été réalisées sur quelles informations peuvent avoir des conséquences potentiellement très importantes aussi bien au niveau de l'AIFE qu'au niveau de l'Etat dans son ensemble et, par contrecoup, au niveau du pays.

Aussi, l'AIFE se doit d'assurer un niveau de sécurité adéquat aux informations et aux systèmes d'informations sous sa responsabilité.

3 ENGAGEMENT DE LA DIRECTION DE L'AIFE

Le présent document, approuvé par la direction de l'AIFE, appelé Politique de Sécurité des Systèmes Information de l'AIFE démontre l'implication forte, au plus haut niveau, de l'AIFE dans cette démarche de réduction des risques et de renforcement de la confiance vis-à-vis du système d'information financière de l'Etat.

4 LA DEMARCHE DE SECURITE DE L'INFORMATION DE L'AIFE

4.1 Principes de la démarche

Une démarche de sécurité de l'information et des systèmes d'information recouvre l'ensemble des aspects permettant de définir, atteindre et maintenir la disponibilité, l'intégrité et la confidentialité des différentes informations et des différents systèmes qui les traitent.

Ces trois éléments (disponibilité, intégrité et confidentialité) représentent les caractéristiques de sécurité de base d'une information ou d'une ressource de traitement de l'information :

- la disponibilité, caractérise l'aptitude d'une information à être accessible et utilisable par un système d'information, une entité ou un utilisateur autorisé, conformément aux exigences de délais et de performances de la, ou des, activités dans lesquelles l'information intervient ;
- l'intégrité, caractérise le fait qu'une information, et les traitements à effectuer sur cette information, ne puissent être modifiés que par une action volontaire et légitime ;
- la confidentialité, qui est la propriété pour une information de ne pas être accessible ou divulguée à des entités, personnes ou processus non autorisés ;

S'appuyant sur ces trois critères, la traçabilité caractérise la possibilité de suivre, a posteriori, les traitements appliqués à une information ou les évolutions et modifications apportées à un système d'information, afin de détecter d'éventuels incidents et les responsabilités correspondantes. Cette notion de traçabilité peut aller jusqu'à la nécessité de fournir des éléments de preuves au sens juridique du terme.

Les informations et les ressources de traitement de l'information, et donc les activités qui reposent dessus, sont exposées à des menaces de différentes natures qui peuvent être regroupées en deux grandes catégories :

- les menaces de nature humaine, qui peuvent être soit liées à des erreurs (erreur de saisie, erreur de manipulation, erreur de conception d'un système, etc.), soit liées à de la malveillance (vol /destruction / modification de données, vol /destruction de matériel, virus, etc.) ;
- les menaces liées à l'environnement (panne électrique, incendie, inondation, etc.).

Bien qu'en nombre important, ces risques ne sont pas tous de même niveau et ne représentent pas tous le même danger pour l'AIFE. Vouloir réduire à zéro tous ces risques serait extrêmement consommateur de ressources pour un résultat, in fine, impossible à atteindre.

La démarche de sécurité de l'information de l'AIFE doit donc s'inscrire dans une approche de gestion des risques permettant d'assurer à tout moment un niveau de sécurité en adéquation avec, d'une part, l'importance de chaque ressource de traitement de l'information et des données par rapport aux objectifs métiers de l'AIFE et, d'autre part, les moyens (financiers et humains) pouvant être alloués pour atteindre ce niveau.

En assurant le respect des besoins de sécurité (disponibilité / intégrité / confidentialité / traçabilité) des informations et des systèmes d'information de l'AIFE, les objectifs de cette démarche sont :

- d'assurer la continuité des activités et des services de l'AIFE vis-à-vis des utilisateurs des ministères ;
- de minimiser la possibilité qu'une menace sur la sécurité de l'information se traduise en pertes ou dommages pour l'AIFE ou les utilisateurs de ses systèmes d'information ;

- de minimiser l'étendue des pertes et dommages en cas d'incident de sécurité ;
- d'assurer une utilisation adéquate des ressources allouées à la sécurité de l'information ;
- de définir les obligations et responsabilités de chacun en matière de sécurité et de s'assurer de leur respect.

4.2 Périmètre d'application

La démarche de sécurité de l'information couvre l'ensemble des systèmes sous la responsabilité de l'AIFE tels que définis au §1, tout au long de leur cycle de vie :

- les applications métiers de l'AIFE ;
- les plateformes productives et non productives sur lesquelles reposent ou sont créées ces applications métiers ;
- les équipements et les ressources transverses utilisés en support des applications métiers de l'AIFE ;
- les équipements et les ressources transverses utilisés par l'AIFE, dans le cadre de son fonctionnement interne.

La sécurité des systèmes d'information doit être prise en compte dans toutes les phases des projets informatiques, conformément aux principes du chapitre 2.3.1 du Référentiel Général de Sécurité (RGS).

Cette démarche s'applique à tous les acteurs intervenant dans ces systèmes, qu'ils soient internes ou externes à l'AIFE.

5 ORGANISATION DE LA DEMARCHE

La démarche de sécurité de l'information s'appuie sur la mise en place d'une organisation formalisée au sein de l'AIFE, permettant d'identifier les différentes responsabilités en la matière, et sur une documentation adaptée en fonction des différents niveaux d'intervenants.

5.1 Implication et responsabilités individuelles

La réussite de la mise en œuvre de cette démarche nécessite l'implication de tous les acteurs, à tous les niveaux de l'organisation de l'AIFE et de ses partenaires et prestataires :

- tout personnel se doit de respecter les règles de sécurité qui sont applicables à son niveau et qui lui sont communiquées au travers de la documentation qui lui est fournie (charte utilisateurs, procédures opérationnelles applicables en fonction de son domaine d'activité,...). Chaque personnel doit être sensibilisé à l'importance de la sécurité de l'information et à la démarche correspondante, afin d'acquérir une culture adéquate en matière de sécurité et les réflexes correspondants, notamment en matière d'identification et de remontée d'incidents de sécurité ;
- le personnel ayant des responsabilités d'encadrement et de management doit s'assurer que les personnels et, éventuellement, les prestataires qui se trouvent sous sa responsabilité ont bien connaissance des règles de sécurité qui leur sont applicables, sont conscients de l'importance de respecter ces règles et les respectent effectivement.

5.2 Direction de l'AIFE

La direction de l'AIFE est responsable, en matière de sécurité informatique :

- De la mise en œuvre des mesures de sécurité de l'information au sein de sa direction, et des mesures de sécurité de l'information des SI dont elle assure la construction, qu'elle s'appuie sur les services d'une autre direction, ou d'un autre ministère ou qu'elle les externalise ;
- De l'arbitrage du traitement des risques majeurs ;

- De fournir les ressources nécessaires à la démarche sécurité au sein de l'AIFE ;

Les membres du comité de direction :

- Relaient la démarche sécurité auprès de leurs personnels ;
- Sont responsables de la mise en œuvre des mesures sécurité au sein de leur service.

5.3 Autorité Qualifiée pour la Sécurité des Systèmes d'information (AQSSI)

Par l'arrêté du 22 janvier 2019 portant désignation des autorités qualifiées pour la sécurité des systèmes d'information dans les services d'administration centrale, les services déconcentrés, les organismes et établissements sous tutelle du ministre de l'économie et des finances et du ministre de l'action et des comptes publics, l'AQSSI de l'AIFE est son directeur.

L'AQSSI est responsable :

- De faire appliquer la démarche de sécurité de l'information dans sa structure ;
- De s'assurer que la gestion des risques est prise en compte dans les SI ;
- De demander une évolution des PSSI de l'AIFE et du référentiel de règles dès que nécessaire ou de donner un avis en cas de consultation pour l'élaboration de nouvelles exigences ;
- De s'assurer que les contrôles internes de sécurité aptes à vérifier le niveau d'application de la PSSI-AIFE sont régulièrement effectués ;
- De l'homologation des SI ;
- De la validation ou non des dérogations à la PSSI ;
- De la validation des DASEC.

5.4 Adjoint de l'Autorité Qualifiée pour la Sécurité des Systèmes d'information (Adjoint AQSSI)

En liaison avec les services du Haut Fonctionnaire de Défense et de Sécurité des ministères financiers, l'adjoint de l'AQSSI est chargé d'assister l'AQSSI pour :

- Définir une politique de sécurité des systèmes d'information adaptée à l'AIFE ;
- S'assurer que les dispositions réglementaires et le cas échéant contractuelles sur la sécurité des systèmes d'information sont appliquées ;
- S'assurer que des contrôles internes de sécurité sont régulièrement effectués ;
- Organiser la sensibilisation et la formation du personnel aux questions de sécurité, en particulier en matière de systèmes d'information ;

S'assurer de la mise en œuvre des procédures réglementaires prescrites pour l'homologation des systèmes.

5.5 Responsable de la Sécurité des Systèmes d'Information (RSSI)

Le RSSI est responsable de :

- S'assurer de l'application, par les personnels d'exploitation et les utilisateurs, des règles de sécurité prescrites,
- Veiller au respect des exigences de sécurité contractuelles
- Veiller à la mise en œuvre des mesures de protection prescrites, établir des consignes particulières et contrôler leur application,
- Vérifier périodiquement l'installation et le bon fonctionnement des dispositifs de sécurité,
- Veiller au respect des procédures opérationnelles de sécurité propres au système d'information,

- Rendre compte de toute anomalie constatée ou de tout incident de sécurité,
- Instruire les FISEC et les DASEC,
- Rédiger les procédures de sécurité en déclinant les politiques de l'agence,
- Instruire les analyses de risques,
- Constituer les dossiers d'homologation,
- Etre membre de la cellule de crise opérationnelle.

5.6 Référent à la protection des données personnelles

La protection des données à caractère personnel s'appuie sur le référent DPD de l'AIFE qui est le représentant du délégué à la protection des données personnelles (DPD) des ministères financiers.

Le référent DPD est l'interlocuteur de la maîtrise d'ouvrage et de la maîtrise d'œuvre de l'AIFE pour la mise en œuvre du RGPD et son contrôle, pour recueillir et traiter les demandes des personnes concernées et pour la gestion des violations de données à caractère personnel traitées par l'AIFE.

Les exigences relatives à la désignation d'un délégué à la protection des données (statut, fonction, missions, qualités professionnelles) sont définies aux articles 37 à 39 du règlement européen relatif à la protection des données personnelles (RGPD). Son rôle est essentiellement d'informer, de conseiller les responsables de traitements, de contrôler le respect du RGPD, il est le point de contact de la CNIL et des « personnes concernées » par les traitements mis en œuvre, il participe au réseau des référents DPD.

5.7 Equipe sécurité des systèmes d'information (Equipe SSI)

L'équipe SSI est responsable de :

- Participer à la gestion des risques ;
- Piloter le déploiement des fonctions de sécurité ;
- D'apporter une expertise en sécurité, notamment en matière de signature, authentification, certification et outils de sécurité ;
- Instruire les FISEC et DASEC.

Elle est constituée d'agents du Département Architecture et Sécurité.

5.8 Fonctions transverses

Les fonctions transverses sont toutes les fonctions supports à l'activité :

- Gestion du budget de l'AIFE ;
- Gestion des contrats AIFE avec les tiers ;
- Gestion des RH ;
- Gestion du SI interne (bureautique, postes de travail, messagerie,...).

Dans le cadre de la démarche sécurité, les fonctions transverses de l'AIFE doivent prendre en compte les exigences de la PSSI dans leurs activités.

5.9 Maîtrise d'ouvrage déléguée

Certains départements et services de l'AIFE interviennent dans la définition des projets et dans l'expression des besoins comme Maîtrise d'Ouvrage déléguée et ils encadrent alors le mandataire dans toutes les phases de la conduite du projet. Dans le cadre de la démarche sécurité, la MOA déléguée doit veiller à :

- Prendre en compte les exigences de la PSSI dans les projets ;

- Faire réaliser une analyse de risques si possible en amont des projets ou au mieux avant la fin de la conception afin de définir des exigences de sécurité spécifiques ;
- S'assurer que les mesures de sécurité découlant de ces exigences sont pertinentes ;
- Suivre la mise en place des mesures de sécurité ;
- Actualiser l'analyse de risques.

5.10 Maîtrise d'œuvre

Les départements ou services de l'AIFE en charge de la mise en œuvre d'une solution sur la base d'un dossier établi et suivi par une maîtrise d'ouvrage sont considérés comme maîtrise d'œuvre. Dans le cas d'intervenants externes, ils agissent sous la responsabilité d'une équipe interne AIFE.

Au sein de la maîtrise d'œuvre, on distingue :

- la partie « construction », correspondant à la conception, au développement, à l'intégration et au déploiement des systèmes ;
- la partie « support », correspondant au fonctionnement permanent des applicatifs ;
- La maintenance applicative recouvre toute action de paramétrage, de requêtage ou intervention sur un élément de code d'une application métier, à des fins de maintenance corrective ou évolutive ;
- La maintenance technique recouvre toute intervention sur un composant « sur étagère » (matériel ou produit logiciel du marché) ou sur tout outil connexe à l'application, à des fins de maintenance corrective ou préventive.

Dans le cadre de la démarche sécurité, la MOE doit veiller à :

- décliner les exigences de sécurité en mesures de sécurité ;
- mettre en place les mesures de sécurité ;
- remonter à la MOA les vulnérabilités non identifiés lors de l'analyse de risques.

5.11 Exploitants

Les exploitants interviennent dans le fonctionnement au jour le jour des systèmes. On distingue les types suivants d'exploitants :

- les exploitants des infrastructures physiques au sein desquelles les systèmes sont hébergés (gestion des locaux, sécurité incendie, contrôle d'accès physique, électricité, climatisation,...) ;
- les exploitants des systèmes, en charge notamment de la gestion technique des systèmes (suivi des capacités, gestion des OS, gestion des alertes systèmes,...) ;
- les exploitants réseau, en charge de la gestion technique des différents composants réseau (routeurs, pare-feux,...).

Dans le cadre de la démarche sécurité, les exploitants doivent :

- respecter les exigences de la PSSI ;
- respecter les exigences particulières liées aux marchés afférents ;
- respecter la procédure de gestion des incidents de l'AIFE.

5.12 Utilisateurs du SI interne de l'AIFE

Les utilisateurs du SI interne de l'AIFE sont les agents de l'AIFE et tout prestataire disposant d'un accès à un des SI de l'AIFE : bureautique, messagerie, information stockée sur les serveurs de fichiers, gestion électronique de documents, etc...

6 LES REGLES A L'AIFE EN MATIERE DE SSI

Les règles applicables à l'AIFE en matière de SSI se répartissent en 7 domaines. Ces règles donnent lieu à des actions permettant leur mise en application. Dans le corps du texte, elles sont codées en fonction du domaine d'appartenance et du numéro d'apparition conformément au tableau ci-dessous :

Domaines	Codification du domaine	Codification de la première règle
Principe général pour une PSSI	GEN	GEN.CHORUS.R1
Organisation et contrôle de la sécurité des systèmes d'information	ORG	ORG.CHORUS.R1
Sécurité liée au personnel	SPE	PER.CHORUS.R1
Sécurité des biens physiques	MAT	MAT.CHORUS.R1
Sécurité liée aux Données à caractère personnel	PER	CAR.CHORUS.R1
Sécurité physique des Locaux	PHY	PHY.CHORUS.R1
Sécurité des communications et des flux	COM	COM.CHORUS.R1
Sécurité liée à l'information	SIN	SIN.CHORUS.R1
Exploitation des SI	EXP	EXP.CHORUS.R1
Sécurité des développements des SI	DEV	DEV.CHORUS.R1
Traitement des incidents de sécurité	INC	INC.CHORUS.R1
Continuité d'activité	PCA	PCA.CHORUS.R1
Maintien permanent de la SSI	MTN	MTN.CHORUS.R1

6.1 Principe général de la PSSI

La politique de sécurité des systèmes d'information détient sa légitimité de la responsabilité exercée par l'Autorité qualifiée pour la sécurité des systèmes d'information (AQSSI) en matière de SSI. Cette responsabilité s'inscrit dans l'Instruction interministérielle 1300/SGDN/PSE/PSD du 30 novembre 2011 portant sur la protection du secret de la défense nationale.

La PSSI est le document SSI de référence. Ce document est évolutif afin de préserver au mieux sa pérennité vis-à-vis de la réglementation, des techniques, des technologies en usage et de l'organisation de l'AIFE.

La PSSI de l'AIFE s'appuie sur les exigences de la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE) et sur celles définies par le ministère des finances et des comptes publics. Les exigences de ces deux PSSI doivent être respectées par l'AIFE.

GEN.AIFE.R1 La PSSI s'applique à tous les services de l'AIFE (personnels permanents ou non permanents) et, en tant que de besoins, aux organismes et aux prestataires travaillant au profit de l'AIFE.

GEN.AIFE.R3 Toute dérogation aux principes et règles de la présente PSSI est soumise à l'approbation formelle de l'AQSSI de l'AIFE. L'AQSSI peut soumettre cette dérogation à l'approbation formelle du HFDS lorsqu'il juge qu'elle déroge aux principes et règles de la PSSI des ministères financiers ou de la PSSI-Etat ou qu'elle peut porter préjudice à la sécurité collective.

6.2 Organisation, responsabilité et contrôle de la SSI

L'existence de principes et de règles applicables à l'AIFE en matière de SSI ne peut suffire à garantir la protection d'un système d'information en l'absence d'une organisation dédiée à la SSI. Pour l'application de ces règles, à tous les niveaux, les responsabilités de chacun doivent être fixées.

6.2.1 Organisation de la SSI

ORG.AIFE.R1 L'organisation de la SSI prévue par les textes doit être mise en place à l'AIFE. Elle est destinée à garantir la prise en compte et à mesurer l'efficacité de la sécurité des systèmes d'information.

L'instruction générale interministérielle n°1300/SGDN/PSE/PSD du 30 novembre 2011 définit l'organisation et les responsabilités des acteurs de la SSI.

La voie fonctionnelle SSI ministérielle est décrite dans la politique générale de sécurité des systèmes d'information pour les ministères économiques et financiers.

Pour mettre en œuvre l'ensemble des mesures destinées à assurer la protection des systèmes d'information, les acteurs de la voie fonctionnelle SSI s'appuient :

- au plan des systèmes d'informations, sur les responsables de la sécurité des systèmes d'information (RSSI) ou faisant fonction ;
- au plan local sur les administrateurs sécurité, systèmes, réseaux et les exploitants de systèmes, ces experts constituant la voie technique SSI.

ORG.AIFE.R2 L'AQSSI s'appuie sur le RSSI de l'AIFE chargé de l'assister dans la mise en œuvre, la gestion et le contrôle de la SSI.

6.2.2 Responsabilités des autorités chargées de l'application à l'AIFE de la PSSI

ORG.AIFE.R3 L'AQSSI approuve le plan d'actions SSI permettant d'atteindre les objectifs de sécurité fixés dans la Politique de Sécurité des Systèmes d'information de l'AIFE.

ORG.AIFE.R4 Le RSSI est responsable de la déclinaison des mesures de cette PSSI à l'AIFE et de planifier et rendre compte auprès de son autorité de leur mise en application.

ORG.AIFE.R5 Le RSSI coordonne les actions permettant l'intégration des clauses liées à la sécurité des systèmes d'information dans tout contrat ou convention impliquant un accès par des tiers à des informations ou à des ressources informatiques.

6.2.3 Documentation de sécurité

Le référentiel documentaire est tenu à jour par le RSSI, validé par l'AQSSI, et est tenu à disposition de tout un chacun. La documentation SSI doit couvrir l'ensemble des aspects de la SSI, organisationnels, techniques et procéduraux. Elle doit être très largement diffusée aux personnels ayant besoin d'appliquer les règles, directives et procédures d'utilisation. Notamment, tous les administrateurs systèmes et réseaux ainsi que tous les personnels intervenant dans la filière SSI doivent connaître cette documentation.

ORG.AIFE.R6 Un référentiel de la documentation est mis à disposition, par le RSSI, aux personnels devant appliquer les règles, directives et procédures de sécurité.

ORG.AIFE.R7 La documentation doit faire l'objet d'une gestion garantissant la réalisation, la duplication, l'archivage et la classification homogène des documents que ce soit pour des documents papiers ou électroniques. Tout document SSI doit faire l'objet :

- **d'un contrôle documentaire pour s'assurer que ce soit la bonne version et que le document a été validé et approuvé ;**
- **d'une mise à jour régulière, pour tenir compte de l'évolution de l'organisation, des procédures et des composants du système d'information ou de ses conditions d'exploitation ;**
- **d'une reproduction et d'une destruction garantissant la limitation stricte de ces actions aux seuls documents désignés ;**
- **d'un marquage spécifique adapté au niveau de classification et de mention de manipulation. En complément de la documentation d'exploitation, la documentation SSI propre à un système d'information lui est associée.**

6.3 Sécurité liée au personnel

Le comportement du personnel est un élément essentiel, le facteur humain est et reste le maillon faible de la SSI.

PER.AIFE.R1 Une procédure de gestion, dans les systèmes d'information, des arrivées, des mutations et des départs doit être formalisée et appliquée strictement. La procédure s'applique au personnel de l'AIFE, aux collaborateurs des organismes et des prestataires travaillant au profit de l'AIFE.

L'autorité hiérarchique est responsable de la mise en œuvre et du contrôle des règles suivantes :

PER.AIFE.R2 Le personnel appartenant ou non à l'AIFE, affecté à un emploi ou une mission permettant l'accès à des informations classifiées de défense, ou référencé au catalogue des emplois de l'AIFE doit faire l'objet d'une habilitation au classifié de défense préalable au niveau requis par le niveau de classification de ces informations ou du poste. L'autorité hiérarchique est responsable de la mise en œuvre et du contrôle de cette règle.

6.3.1 Formation du personnel

PER.AIFE.R3 Le personnel doit avoir reçu la formation SSI adaptée à l'emploi lié à son poste. Elle se traduit par l'acquisition des connaissances nécessaires de l'organisation, de la technique, de la réglementation spécifique à la SSI et au domaine d'activité concerné, pour assurer une conduite et une utilisation en accord avec les besoins de sécurité du SI.

PER.AIFE.R4 Pour les personnels non permanents, un tutorat par un personnel permanent est mis en place, afin de contrôler l'application des règles de la PSSI.

6.3.2 Responsabilité et sensibilisation du personnel

Le personnel engage sa responsabilité pénale personnelle et disciplinaire lorsqu'il accède à un système protégé et qu'il y manipule des données, des logiciels et des matériels. Il doit en être informé. Il doit en outre être sensibilisé aux risques liés à l'utilisation des nouvelles technologies de l'information et, en fonction du besoin d'en connaître, il doit être informé sur les mesures de sécurité prises pour protéger le système d'information, les données, les logiciels et les matériels auquel il accède, qu'il utilise ou qui sont mis à sa disposition.

SPE.AIFE.R5 Le personnel doit être informé des risques liés à la mise en œuvre, dans les conditions d'emploi prévues, des systèmes d'information placés sous responsabilité de l'AIFE. Le personnel concerné (agents, stagiaires, intérimaires, prestataires...) est informé de ses obligations réglementaires et de sa

responsabilité pénale personnelle et disciplinaire. Un plan de sensibilisation doit être mis en place et il est nécessaire de s'assurer que le personnel a pris connaissance de ses obligations et responsabilités.

PER.AIFE.R6 Tout intervenant tiers auquel est donné l'accès à des informations sensibles des systèmes d'information exploités pour l'AIFE doit signer un engagement de confidentialité avant d'obtenir l'accès à ces informations ou aux systèmes concernés.

Les informations couvertes par l'interdiction de divulgation de confidentialité concernent :

- **le contenu hébergé : les informations et les fonctions traitées par le système ;**
- **les informations dont la divulgation est de nature à porter atteinte à la sécurité du système (mots de passe, clés de chiffrement, documentations relative à l'architecture et la sécurité du système, etc...).**

Une procédure spécifique décrit l'organisation de la sensibilisation à la SSI au sein de l'AIFE.

6.4 Sécurité des biens physiques et matériels

MAT.AIFE.R1 Les mesures de protection des biens physiques s'adressent ;

- **aux équipements personnels de type ordinateurs portables, téléphones portables, etc... dès lors qu'ils traitent d'informations ou interfèrent avec un système d'information de l'AIFE ;**
- **aux équipements (serveurs, équipements réseaux, baies de sauvegarde, ...) localisés sur les sites hébergeant des composants des systèmes d'information de l'AIFE.**

MAT.AIFE.R2 Des contrôles périodiques assurent que les mesures de protection des biens physiques permettent de garantir en permanence la disponibilité, l'intégrité et la confidentialité des mécanismes de sécurité mis en œuvre.

MAT.AIFE.R3 Tous les biens physiques en dotation doivent faire l'objet d'une gestion permanente et effective quelle que soit leur localisation. Cette gestion inclut la gestion en configuration des équipements, de leurs programmes informatiques et de leur paramétrage.

MAT.AIFE.R4 Tous les biens physiques traitant d'informations protégées doivent faire l'objet d'un marquage correspondant au niveau des informations traitées.

MAT.AIFE.R5 Les équipements personnels communicants ou non (ordinateurs, téléphones mobiles, tablettes, supports de stockage...) ne doivent pas être connectés aux systèmes d'information placés sous la responsabilité de l'AIFE afin de ne pas interférer avec le bon fonctionnement ou de générer des vulnérabilités pour ces systèmes. Seuls les équipements fournis par l'AIFE peuvent être connectés au réseau local de l'AIFE.

MAT.AIFE.R6 Les supports (clés USB et disques amovibles) sont stockés dans des meubles fermant à clé. Il est recommandé de chiffrer les données contenues sur ces supports.

MAT.AIFE.R7 Un câble physique de sécurité doit être fourni avec chaque poste nomade. Les utilisateurs doivent être sensibilisés à son utilisation. Le PC portable doit être sécurisé avec ce câble dès lors que l'utilisateur le laisse sans surveillance dans les locaux de l'AIFE ou à l'extérieur.

MAT.AIFE.R8 Toute perte ou vol d'une ressource d'un système d'information doit être déclarée au RSSI.

MAT.AIFE.R9 Une procédure de gestion des postes et supports dans le cadre de départs de personnel ou de prestataire ou de réaffectations à de nouveaux utilisateurs ou prestataires doit être mise en place et validée par le RSSI. Elle doit définir les conditions de recours à un effacement des données.

6.5 Protection des données à caractère personnel

On entend par « donnée à caractère personnel » : toute information relative à une personne physique susceptible de l'identifier, directement ou indirectement comme par exemple : un nom, une photo, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, un matricule interne, une adresse IP, un identifiant de connexion informatique, un enregistrement vocal, etc...

CAR.AIFE.R1 Un référent RGPD doit être nommé.

CAR. AIFE.R2 Un registre des traitements des données à caractère personnel doit être tenu.

CAR. AIFE.R3 Les données à caractère personnel ne peuvent être traitées qu'en respectant strictement la finalité du traitement auxquelles elles participent.

CAR. AIFE.R4 Toute violation de données à caractère personnel doit être notifiée au référent DPD de l'AIFE, un registre doit inventorier ces violations.

CAR. AIFE.R5 Les mesures organisationnelles et techniques de protection des données à caractère personnel doivent être intégrées afin de respecter les principes de protection des données dès la conception et de protection des données par défaut.

CAR. AIFE.R6 Les mesures d'encadrement doivent être prévues pour tout transfert des données personnelles hors Union Européenne.

CAR. AIFE.R7 Une analyse d'impact doit être menée pour tous les traitements à risques élevés.

6.6 Sécurité physique des locaux

PHY.AIFE.R1 Tout équipement technique et tout local informatique hébergeant des équipements connectés aux systèmes d'information du SI de l'AIFE, doit être affecté à un responsable explicitement identifié. Tout changement d'affectation doit être suivi et acté par le responsable des locaux.

PHY. AIFE.R2 L'accès aux zones internes et restreintes (exemple : salle serveurs) doit faire l'objet d'un dispositif de contrôle d'accès physique. La délivrance des moyens d'accès physique doit respecter un processus formel d'habilitation.

PHY.AIFE.R3. En dehors des zones d'accueil du public, les visiteurs doivent être systématiquement accompagnés depuis leur entrée, pendant leur visite puis raccompagnés à la sortie par une personne de l'entité habilitée. Une traçabilité des accès des visiteurs externes aux zones internes et restreintes doit être mise en place ; ces éléments sont alors conservés un an.

Les personnes qui accèdent à ces zones doivent être identifiées nominativement (un registre des accès doit être renseigné et disponible).

PHY.AIFE.R4 Le port du badge d'identification personnelle est obligatoire pour tous les personnels de l'AIFE, les prestataires et les visiteurs.

PHY.AIFE.R5 Des mesures spécifiques de sécurité doivent être mises en œuvre pour les locaux considérés comme « zone restreinte » (exemple : salle serveurs), afin de les protéger contre les tentatives d'intrusions et de détecter les actes malveillants.

L'accès aux locaux techniques contenant des équipements d'alimentation et de distribution d'énergie, ou des équipements réseau et de téléphonie doit être physiquement protégé.

PHY.AIFE.R6 Le personnel autre que celui explicitement autorisé et habilité, appelé à intervenir dans les « zones restreintes », intervient systématiquement sous surveillance permanente d'une personne de l'entité.

PHY.AIFE.R7 L'entité doit être capable de détecter les intrusions physiques dans les « zones restreintes » et d'intervenir rapidement en dehors des périodes d'activité normales.

PHY.AIFE.R8 Le site d'hébergement doit disposer de mesures de sécurité afin de se prémunir contre les risques d'incendie, fuite d'eau, défaut de climatisation, rupture d'alimentation énergétique, rupture de lien réseau.

PHY.AIFE.R9 Les câbles électriques et de télécommunications doivent être séparés pour éviter les interférences, ils doivent également être protégés contre toute interception et dommage potentiel.

PHY.AIFE.R10 Les bureaux des agents responsables de l'exploitation du SI de l'AIFE et particulièrement ceux des équipes qui gèrent des équipements de sécurité doivent être systématiquement verrouillés en l'absence de leurs occupants.

6.7 Sécurité des communications et des flux

L'échange de données constitue l'importation ou l'exportation d'informations entre :

- des domaines ayant des politiques de sécurité différentes ;
- des réseaux de responsabilités de mise en œuvre distinctes ;
- des applicatifs distincts ;
- toute combinaison des trois items précédents.

COM.AIFE.R1 L'échange de données entre les applications de l'AIFE et des systèmes d'information extérieurs, doit être sécurisé.

Une interconnexion non maîtrisée est de nature à remettre en cause l'analyse de risque initiale, notamment le principe de cloisonnement, du besoin d'en connaître ou des données de niveaux distincts, mais aussi la disponibilité et l'intégrité des informations et des ressources.

COM.AIFE.R2 Au titre de la défense en profondeur, un zonage pour le cloisonnement réseaux par type d'utilisation doit être établi, exemple :

- une zone publique (DMZ) regroupant les machines qui hébergent des services ayant vocation à communiquer avec l'extérieur (Reverse Proxy, Serveur Web, FTP, Serveur de mail, DNS, etc.) ;
- une zone « Frontend » qui reçoit des flux provenant de la zone publique ou d'un réseau interne à l'administration

- une zone « Backend » qui reçoit des flux provenant de la zone Frontend et qui regroupe les machines n'ayant pas vocation à communiquer avec l'extérieur ;
- un réseau dédié à l'administration des machines et des équipements à partir de postes de travail situés chez l'hébergeur.

COM.AIFE.R3 Toute interconnexion d'un réseau tiers avec un réseau placé sous responsabilité de l'AIFE doit faire l'objet d'une analyse des risques résultant de cette interconnexion afin de cerner l'impact sur la sécurité des systèmes de l'AIFE et prendre les mesures de couverture si nécessaire.

COM.AIFE.R4 Seules les connexions explicitement autorisées à destination du SI de l'AIFE doivent être activées. Les demandes de raccordement doivent faire l'objet d'un visa d'un responsable désigné dans la procédure de gestion des réseaux. Pour des demandes spécifiques, une étude préalable doit être réalisée, accompagnée d'un avis technique et d'une analyse de risques. Cet ensemble (étude et avis) doit être communiqué à l'AQSSI de l'AIFE. Pour autoriser la connexion, les mesures nécessaires pour couvrir les risques identifiés devront être mises en place.

COM.AIFE.R5 Il est interdit de véhiculer des informations classifiées de défense sur le SI de l'AIFE. Le raccordement d'un réseau véhiculant des informations sensibles au réseau Internet est interdit, sauf à utiliser des dispositifs de chiffrement labellisés par l'ANSSI ou ceux ayant fait l'objet d'une procédure d'homologation.

COM.AIFE.R6 Dès lors que des informations sensibles doivent transiter sur des réseaux non sécurisés, il convient de les protéger spécifiquement (chiffrement). Le choix et le dimensionnement des algorithmes cryptographiques doivent être effectués conformément aux règles et recommandations du RGS en la matière.

COM.AIFE.R7 Tous les flux d'administration doivent être chiffrés par des procédés fiables (SSH, SSL, Ipsec, etc.), garantissant la confidentialité, l'intégrité des données et l'authentification.

COM.AIFE.R8 Des mécanismes de protection contre les attaques sur le protocole ARP doivent être implémentés. Le service global doit être protégé contre les attaques classiques sur IP et les protocoles associés.

COM.AIFE.R9 Les équipements de réseaux (comme les routeurs) doivent faire l'objet d'un durcissement spécifique comprenant notamment, outre le changement des mots de passe et certificats, la désactivation des interfaces et services inutiles, ainsi que la mise en place de mécanismes de protection du plan de contrôle.

COM.AIFE.R10 L'architecture réseau doit être décrite, formalisée à travers des schémas d'architecture et des configurations maintenus au fil des évolutions apportées au SI.

6.8 Exploitation des SI

6.8.1 Protection des informations

EXP.CHORUS.R1 Les informations, selon leur nature et leur sensibilité, doivent être protégées conformément à la présente PSSI ou, à défaut de protocole particulier, à la politique de sécurité de l'organisme émetteur.

EXP.CHORUS.R2 Les documents comportant des informations sensibles au sein de l'AIFE et ceux échangés dans les communications avec ses partenaires doivent respecter les règles édictées dans la politique de protection des documents comportant des informations sensibles (marquage, restriction de diffusion, protection, ...).

EXP.CHORUS.R3 La procédure de protection des informations sensibles et classifiées de défense s'appliquent à chaque étape de l'élaboration des informations ainsi qu'à leurs supports (depuis la création du brouillon jusqu'à son éventuelle destruction), y compris pour leur conservation et leur destruction.

EXP.CHORUS.R4 L'utilisation de données de production n'est pas autorisée sur les environnements de développement et de formation.

EXP.CHORUS.R5 Dès lors que les données de production sont hébergées sur des supports ou environnements mutualisés, des mesures spécifiques et adaptées de cloisonnement garantissant la confidentialité, doivent être mises en œuvre.

EXP.CHORUS.R6 Tout utilisateur doit verrouiller sa session avant de quitter son poste de travail.

6.8.2 Habilitations sur les systèmes d'information

La politique d'accès aux systèmes d'information de l'AIFE doit respecter le principe de tout ce qui n'est pas autorisé est interdit. Les droits d'accès d'un utilisateur doivent être fondés sur le « besoin d'en connaître » lié à sa fonction et sur le principe « du moindre privilège » nécessaire à la réalisation de l'activité quotidienne.

Une politique d'accès doit être rédigée afin de préciser les règles en matière d'attribution / suspension / suppression de droits d'un utilisateur, permettant notamment de garantir que des droits ne sont accordés et maintenus pour un utilisateur donné qu'avec l'accord formel des propriétaires des informations ou des responsables d'application concernés.

EXP.AIFE.R7 Tout utilisateur, autorisé à utiliser un système d'information de l'AIFE, doit être identifié.

EXP.AIFE.R8 En production, tout utilisateur d'un système d'information de l'AIFE doit posséder des droits d'accès correspondant à son profil utilisateur. Ces droits doivent faire l'objet d'un contrôle systématique et complet préalable à tout accès. En cas de non-conformité des actions tentées avec les droits correspondants pour cet utilisateur, le système doit soit être verrouillé, soit être limité dans certains modes.

Ces non-conformités doivent être enregistrées et déclencher une alerte afin d'analyser leur cause.

EXP.AIFE.R9 En fonction de la sensibilité du système d'information, une authentification forte peut être exigée et doit permettre d'établir de façon sûre une relation biunivoque entre la personne physique qui utilise le système et l'utilisateur identifié.

EXP.AIFE.R10 Les moyens d'authentification doivent faire l'objet d'une gestion :

- organisationnelle au niveau du service en charge du système d'information ;
- technique au niveau du système d'information.

EXP.AIFE.R11 Les droits d'accès doivent faire l'objet d'une gestion :

- organisationnelle au niveau du service en charge du système d'information ;

- technique au niveau du système d'information.

EXP.AIFE.R12 Les données d'administration et de sécurité, vitales pour le système d'information (authentification, droits d'accès, comptes administrateurs, données de filtrage des gardes de sécurité, ...) sont considérées comme des données sensibles et doivent être protégées comme telles.

EXP.AIFE.R13 Lors d'un changement de fonction, les comptes d'un utilisateur doivent être modifiés pour lui donner les droits d'accès correspondant à sa nouvelle fonction. Des droits d'accès peuvent être attribués temporairement à un utilisateur pour des besoins opérationnels. Ces droits doivent être attribués pour une période bien définie.

EXP.AIFE.R14 L'utilisation de comptes génériques est interdite en production, sauf contrainte technique incontournable nécessitant la mise en place et l'utilisation de certains comptes techniques et fonctionnels. Dans ce dernier cas, ces comptes génériques techniques et fonctionnels doivent être assignés aux seuls groupes de personnes autorisées.

La liste exhaustive de ces comptes doit être consignée dans une procédure qui définit également les modalités d'utilisation de ces comptes génériques. Les modalités d'utilisation devront garantir qu'un compte générique ne peut pas être utilisé sans que l'on puisse identifier, a posteriori, la personne ayant réalisé une action par le biais de ce compte.

EXP.AIFE.R15 Les utilisateurs des applications de l'AIFE en production n'ont pas de droits d'administration système.

EXP.AIFE.R16 En cas de départ d'un administrateur disposant de privilèges sur des composants du système d'information, les comptes individuels dont il disposait doivent être inactivés. Les éventuels mots de passe d'administration dont il avait connaissance doivent être changés (exemples : mots de passe des comptes fonctionnels, comptes génériques ou comptes de service utilisés dans le cadre des fonctions de l'administrateur).

EXP.AIFE.R17 Les exploitants et administrateurs systèmes ne doivent pas avoir accès aux données « métier » des applications en production.

EXP.AIFE.R18 L'accès aux SI de l'AIFE par les utilisateurs en nomadisme et en télétravail doit faire l'objet d'une homologation. L'homologation repose :

- sur l'analyse de la sensibilité en confidentialité et en intégrité des profils ou rôles du SI concerné,
- sur une analyse de risques présentant les mesures techniques et organisationnelles qui permettent d'atteindre un risque résiduel acceptable.

EXP.AIFE.R19 La prise de main à distance d'une ressource informatique locale ne doit être réalisée que par les personnels autorisés, chargés des SI, sur les ressources informatiques de leur périmètre, dans le respect des règles de sécurité.

6.8.3 Gestion des authentifiants

Les informations d'authentification (mots de passe d'accès aux SI, clés privées liées aux certificats électroniques, etc.) doivent être considérées comme des données sensibles. Elles doivent être stockées de façon à être accessibles uniquement par des utilisateurs autorisés.

EXP.AIFE.R20 Les mots de passe utilisés ne doivent jamais apparaître en clair dans les programmes, fichiers, scripts, traces ou fichiers journaux.

EXP.AIFE.R21 Chaque compte utilisateur doit être créé avec un mot de passe initial aléatoire unique.

EXP.AIFE.R22 Les mots de passe utilisés doivent répondre à certaines exigences pour garantir une certaine robustesse. Les règles à observer, en matière de définition de mots de passe et de durée de vie maximale, sont précisées dans une procédure. Des moyens techniques permettant d'imposer la politique de mots de passe (par exemple pour s'assurer du respect de l'éventuelle obligation relative à l'usage de caractères spéciaux) doivent être mis en place.

EXP.AIFE.R23 Des moyens techniques permettant d'imposer la politique de mots de passe (par exemple pour s'assurer du respect de l'éventuelle obligation relative à l'usage de caractères spéciaux) doivent être mis en place. A défaut, un contrôle périodique des paramètres techniques relatifs aux mots de passe doit être réalisé.

EXP.AIFE.R24 Les mot de passe et autres secrets (code pin, passphrase, ...) sont personnels et ne doivent pas être communiqués à une tierce personne. Ils engagent la responsabilité de leur détenteur. Il est interdit de conserver ses mots de passe à proximité du poste informatique où ces mots de passe sont utilisés.

EXP.AIFE.R25 L'utilisation d'un compte générique non imputable à une personne et une seule est interdite. L'utilisation de comptes génériques est seulement autorisée dans les cas suivants :

- Mise en œuvre d'une procédure d'urgence ;
- Dialogues inter systèmes / applicatifs.

EXP.AIFE.R26 Les authentifiants permettant l'administration des ressources des SI doivent être placés sous séquestre et tenus à jour, dans un coffre, une armoire fermée à clé ou un coffre-fort électronique. Tout accès d'administration à une ressource informatique doit pouvoir être tracé et permettre de remonter à la personne exerçant ce droit.

EXP.AIFE.R27 L'utilisation d'une messagerie autre que la messagerie professionnelle pour des usages professionnels est interdite.

6.8.4 Traçabilité et supervision de la sécurité

Au niveau de chaque application des SI de l'AIFE, les besoins en matière d'auditabilité doivent être identifiés d'un point de vue métier par le chef de projet. Ces besoins sont ensuite traduits en exigences de journalisation aux niveaux applicatif, système et réseau au travers d'une politique de journalisation et en prenant en compte les exigences qui suivent. Cette politique doit spécifier, à chaque niveau de composant (réseau, système, applicatif), les événements à journaliser et les données correspondantes, ainsi que les exigences en matière de conservation et de protection des journaux d'événements (disponibilité, intégrité, confidentialité). En cas de nécessité d'accès ou d'activités temporaires non-prévues (par exemple, besoin opérationnel ponctuel), la politique doit être complétée afin de s'assurer que ces besoins ponctuels ne remettent pas en cause les besoins d'auditabilité.

EXP.AIFE.R28 Le chef de projet doit recenser les obligations légales de journalisation et identifier les besoins métiers, afin de déterminer des exigences d'auditabilité.

EXP.AIFE.R29 Toutes les actions réalisées en production sur le SI doivent être journalisées. Le contenu des journaux ainsi que les événements spécifiques devant figurer dans ces journaux doivent être renseignés dans une procédure soumise à l’approbation de l’AQSSI.

EXP.AIFE.R30 Une procédure doit reprendre tout le paramétrage et les processus de sauvegarde et de purge retenus. La modification de ces journaux, par action manuelle (par opposition à une action automatisée), doit générer une alarme et consigner une alerte dans un journal dédié à la supervision.

EXP.AIFE.R31 Les connexions réseau doivent être consignées dans des journaux. Les tentatives d’accès aux réseaux des SI de l’AIFE, les interruptions et les connexions établies doivent apparaître dans ces journaux. Les alertes réseaux doivent être remontées auprès de l’administrateur ou de l’exploitant. Les modalités et la signification des codes générés doivent être précisées dans une procédure.

EXP.AIFE.R32 Les opérations d’administration (techniques et fonctionnelles) doivent être tracées à un niveau permettant de gérer l’imputabilité au niveau individuel des actions d’administration.

EXP.AIFE.R33 Les journaux doivent être conservés sur dix-huit mois glissants, hors contraintes légales et réglementaires particulières imposant des durées de conservation spécifiques.

EXP.AIFE.R34 L’analyse des journaux relatifs à l’utilisation d’un système d’information est indispensable en phase d’exploitation ou d’utilisation. Elle doit permettre de détecter, d’imputer et de réagir *a posteriori* à toute utilisation non conforme (accidentelle ou intentionnelle) de l’un quelconque des composants du système.

EXP.AIFE.R35 Un système de détection et de prévention d’intrusion doit permettre de détecter tout dysfonctionnement et toute tentative d’accès interdite ou frauduleuse d’un équipement, d’un système ou d’une application dédié aux SI de l’AIFE. Ce système doit remonter des alertes auprès des administrateurs et exploitants désignés dans une procédure. Celle-ci doit également comporter les processus à respecter pour gérer les alertes et intervenir au plus tôt sur les équipements ou systèmes défectueux. En cas de détection de tentatives d’accès interdites ou frauduleuses, la procédure doit prévoir une alerte du RSSI de l’AIFE et si nécessaire de l’AQSSI.

EXP.AIFE.R36 Les différents composants (aux niveaux réseau, système et applicatif) mettant en œuvre des fonctions de journalisation doivent être synchronisés vis-à-vis d’une source de temps commune et fiable.

6.8.5 Poste des exploitants

EXP.AIFE.R37 Le poste de travail des exploitants techniques et applicatifs doit répondre aux exigences suivantes :

- Il est dédié à l’exploitation ;
- Il n’est pas raccordé directement sur internet ;
- Il n’est jamais connecté à un réseau WIFI ;
- Son système d’exploitation et ses logiciels sont à jour des correctifs de sécurité ;
- N’y sont laissés que les logiciels et le paramétrage strictement nécessaire aux activités des exploitants ;
- Il doit être isolé physiquement et logiquement des autres postes de travail et serveurs n’ayant pas de rapport avec les activités d’exploitation ;

- Les ports USB sont désactivés ;
- Son firewall est activé et paramétré ;
- Son disque dur est chiffré ;

EXP.AIFE.R38 Les exploitants ne disposent d'aucun droit d'administration sur leurs postes.

6.8.6 Maintien en conditions de sécurité et lutte contre les codes malveillants

EXP.AIFE.R39 Le système d'information de l'AIFE doit être protégé par des anti-virus à jour (serveurs d'interconnexion, serveurs applicatifs et postes de travail).

EXP.AIFE.R40 Des moyens de vérification antivirale des medias doivent être mis à disposition des utilisateurs, afin de permettre une vérification du contenu du support avant utilisation sur un poste ou un serveur raccordé au réseau des SI de l'AIFE.

EXP.AIFE.R.41 Les logiciels de détection de codes malveillants installés sur les postes de travail et les serveurs, doivent permettre de contrôler tous les flux venant de l'extérieur, sous forme de messages électroniques, de pages web visitées ou de fichiers. Un contrôle de non contamination des serveurs Web de production doit être effectué périodiquement.

EXP.AIFE.R42 En aucun cas, un système de protection contre les codes malveillants ne devra être désactivé sans validation préalable de l'AQSSI de l'AIFE.

EXP.AIFE.R43 Les composants logiciels des SI du l'AIFE doivent être tenus à jour des correctifs de sécurité. Les actifs matériels et logiciels doivent être inventoriés afin d'effectuer le suivi des évolutions, des licences, des compatibilités.

EXP.AIFE.R44 En cas d'alerte grave (attaque virale, faille critique) annoncée notamment par le CERT-FR (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques), le correctif doit être appliqué dans un délai de 24 heures sur les infrastructures hébergeant le système de l'administration (serveurs, pare-feu, routeurs ouverts vers l'extérieur).

Lorsqu'aucun correctif n'est disponible, les recommandations de l'éditeur ou du CERT-FR dans le cadre d'un contournement provisoire doivent être suivies.

EXP.AIFE.R45 Il est obligatoire de choisir des produits et des services de sécurité ayant fait l'objet d'une labellisation par l'ANSSI quand ceux-ci sont disponibles et qu'ils répondent aux besoins opérationnels du système d'information.

EXP.AIFE.R46 La configuration de chaque composant ou chaque type de composants des applications de l'AIFE (réseau, serveurs, postes de travail) doit être formalisée et tenue à jour. Pour chaque composant, ou type de composant, des responsables de configuration (responsable, administrateur, exploitation) doivent être identifiés. Ils ont en charge la définition des configurations et la vérification de leur application. Chaque configuration peut comporter des éléments de base et des éléments supplémentaires (par exemple, outils logiciels non nécessaires sur tous les équipements mais ayant fait l'objet d'une validation et pouvant être installés en fonction du besoin).

6.8.7 Envoi en maintenance, mise au rebut, réaffectation de matériel informatique

EXP.AIFE.R47 Les supports de stockage de données (disques durs, bandes de sauvegardes, etc...) ne peuvent être réutilisés à d'autres fins que celles prévues initialement.

EXP.AIFE.R48 Les données doivent être chiffrées ou effacées de manière sécurisée avant l'envoi en maintenance externe de toute ressource informatique.

EXP.AIFE.R49 Lorsqu'une ressource informatique est amenée à quitter définitivement le service, les données présentes sur les disques durs ou la mémoire intégrée doivent être effacées de manière sécurisée avant mise au rebut.

6.9 Traitement des incidents de sécurité

Les dispositions techniques et organisationnelles doivent être prises pour cantonner au maximum les dommages résultant d'une atteinte à la SSI, que son origine soit accidentelle ou intentionnelle.

INC.AIFE.R1 La détection d'un incident de sécurité (critères de disponibilité, intégrité, confidentialité) doit être déclarée dans les plus brefs délais par toute personne le constatant à l'AQSSI de l'AIFE. De même toute suspicion de présence d'une faille informatique doit être signalée dans les mêmes conditions afin de prévenir tout incident de sécurité.

INC.AIFE.R2 Tout incident de sécurité, quel que soit son niveau de gravité, doit donner lieu à l'ouverture d'une fiche d'incident par son observateur (FISEC). Cette fiche doit ensuite être transmise par l'observateur à sa hiérarchie et à l'AQSSI de l'AIFE. Le modèle de cette fiche incident doit faire apparaître la nature, la cible, les impacts, les causes et les actions correctrices entreprises. Un statut doit être défini pour chaque incident selon son évolution dans le circuit de gestion d'un incident (analysé, qualifié, en cours de traitement, clos...).

INC.AIFE.R3 L'AQSSI informe le Fonctionnaire de Sécurité des Systèmes d'Information (FSSI) des incidents majeurs.

6.10 Continuité d'activité

PCA.AIFE.R1 Un plan de continuité d'activité et un plan de reprise d'activité doivent être établis pour tout l'AIFE afin d'en assurer, en cas de sinistre, la continuité d'activité. Ils doivent indiquer les mesures techniques, organisationnelles, procédurales assurant la continuité d'activité du système, ou en cas de sinistre la reprise d'activité conformément aux exigences.

PCA.AIFE.R2 Les plans de continuité et de reprise d'activité doivent être tenus à jour.

PCA.AIFE.R3 Pour chaque serveur et service participant aux SI de l'AIFE, une procédure de sauvegarde adaptée doit être définie. Elle doit être conforme au plan de continuité.

PCA.AIFE.R4 Les données sauvegardées doivent être conservées de manière à garantir leur disponibilité en cas de sinistre sur les locaux hébergeant les ressources sauvegardées. Ces données doivent être traitées de manière à garantir leur confidentialité.

PCA.AIFE.R5 Les sauvegardes doivent être testées régulièrement afin de garantir la capacité de restituer l'environnement complet d'un composant du système d'information.

PCA.AIFE.R6 Les sauvegardes de données ne doivent pas être soumises aux mêmes risques de sinistres que les données sauvegardées.

PCA.AIFE.R7 Les demandes de récupération de données sauvegardées doivent faire l'objet d'une procédure de contrôle stricte afin de garantir que toute demande de restauration d'une donnée est faite sous contrôle de la personne propriétaire de l'information et que cette demande est autorisée.

PCA.AIFE.R8 Les sauvegardes des certificats et des clés cryptographiques doivent être décrites dans une procédure. Les modalités de restauration doivent également être définies, indiquant les personnes autorisées à intervenir et leurs responsabilités selon la nature des clés à restaurer.

6.10.1 Maintien permanent de la SSI

MTN.AIFE.R1 Afin de s'assurer du respect de la réglementation et de la conformité des procédures et du maintien permanent de la SSI, l'AQSSI fait effectuer périodiquement des inspections, des contrôles ainsi que des audits des organisations et des systèmes. Les actions correctrices résultant de ces contrôles et audits doivent faire l'objet d'une planification par l'entité responsable et doivent être validées par l'AQSSI.

MTN.AIFE.R2 Un programme d'audit annuel doit être établi à l'année N-1 afin d'identifier et de prioriser les composants des SI qui devront être audités. Ce programme est composé par le RSSI et soumis à la validation de l'AQSSI.

6.10.2 Homologation d'un système d'information ou de ses composants

La décision d'homologation est un acte formel par lequel l'Autorité d'homologation (désignée par l'autorité qualifiée) valide la mise en exploitation du système d'information.

Une procédure définit l'organisation mise en œuvre au sein de l'AIFE et précise les principes et règles qui s'imposent pour procéder à l'homologation des systèmes d'information.

MTN.AIFE.R3 L'homologation est requise pour l'ensemble du système d'information, (avant sa mise en production) ou des composants assurant la collecte, le traitement, le stockage, la diffusion, la protection des informations classifiées de défense ou sensibles, dans les conditions d'emploi définies.

MTN.AIFE.R4 L'homologation de sécurité est subordonnée au respect des standards de sécurité ministériels en vigueur, notamment DNSSEC, entêtes http, messagerie, cloisonnement réseau, etc...

MTN.AIFE.R5 Tout système d'information assurant la collecte, le traitement, le stockage, la diffusion, la protection des informations classifiées de défense ou sensibles doit faire l'objet d'une révision de son homologation préalablement attribuée, dès lors que :

- les conditions d'emploi ont évolué ;
- le terme de l'homologation est échu ;
- des évolutions fonctionnelles ou techniques ont été apportées.

