Direction du personnel,
des services et de la modernisation

Circulaire n^{o} 2005-26 du 23 mars 2005 relative à la mise en application du référentiel de sécurité des systèmes d'information (SSI)

NOR : *EQUP0510082C*

Référence : directive du Premier ministre n^{o} 5.002/SG du 18 juin 2004.
Pièces jointes : préambule du référentiel, volet organisation du référentiel, liste des règles primordiales.

Le ministre de l'équipement, des transports, de l'aménagement du territoire, du tourisme et de la mer à : - Cabinets des ministres : Monsieur le directeur de cabinet du ministre de l'équipement, des transports, de l'aménagement du territoire, du tourisme et de la mer ; Monsieur le directeur de cabinet du ministre délégué au tourisme ; Monsieur le directeur de cabinet du secrétaire d'Etat aux transports et à la mer ; Monsieur le directeur de cabinet du secrétaire d'Etat à l'aménagement du territoire. - Conseil général des Ponts et Chaussées (CGPC), inspections et assimilés : Monsieur le vice-président du conseil général des Ponts et Chaussées ; Monsieur le chef de la mission interministérielle d'inspection du logement social ; Monsieur le coordonnateur de la mission d'inspection spécialisée d'environnement ; Monsieur le chef de l'inspection du travail des transports. Administration centrale ou assimilés : Madame la directrice et Messieurs les directeurs d'administration centrale (DAEI, DAFAG, DPSM, DRAST, DGUHC, DR, DSCR, DTT, SIC, DAMGM, DTMPL, DENIM, DT) ; Monsieur le Haut fonctionnaire de défense ; Monsieur le directeur du Conseil national des transports ; Monsieur le secrétaire général du tunnel sous la Manche. - Services déconcentrés : Mesdames et Messieurs les préfets de régions ; Mesdames les directrices et Messieurs les directeurs des directions régionales de l'équipement ; Mesdames et Messieurs les préfets de départements ; Mesdames les directrices et Messieurs les directeurs des directions départementales de l'équipement ; Messieurs les directeurs des centres d'études techniques de l'équipement ; Messieurs les chefs des services de navigation du Nord-Est, du Nord - Pas-de-Calais, Rhône-Saône, de la Seine, de Strasbourg, de Toulouse ; services maritimes et de navigation de Gironde, du Languedoc-Roussillon et de Nantes ; services maritimes du Nord, de la Seine-Maritime, des ports de Boulogne-sur-Mer et de Calais, des Bouches-du-Rhône. - Ecoles et formation : Monsieur le directeur de l'école nationale des travaux publics de l'Etat ; Monsieur le directeur de l'ENTE et Messieurs les directeurs des établissements d'Aix-en-Provence et de Valenciennes de l'Ecole nationale des techniciens de l'équipement ; Monsieur le directeur du centre de formation polyvalent de Brest ; Monsieur le directeur du centre d'évaluation, de documentation et d'innovation pédagogiques ; Madame la directrice et Messieurs les directeurs des centres interrégionaux de formation professionnelle d'Aix-en-Provence, Arras, Clermont-Ferrand, Mâcon, Nancy, Nantes, Paris, Rouen, Toulouse et Tours. - Services techniques centraux et assimilés : Monsieur le directeur du centre d'études sur les réseaux, les transports, l'urbanisme et les constructions publiques ; Monsieur le directeur du service d'études et d'aménagement touristique de la montagne ; Monsieur le directeur du centre d'études des tunnels ; Monsieur le directeur du centre national des ponts de secours ; Monsieur le directeur du service d'études techniques des routes et autoroutes ; Monsieur le directeur du service technique des remontées mécaniques et des transports guidés ; Monsieur le directeur du centre d'études techniques maritimes et fluviales. - Etablissements publics : Monsieur le directeur des Voies navigables de France (VNF) ; Monsieur le directeur de l'Agence nationale pour l'amélioration de l'habitat (ANAH). - Copie : DGAC ; LCPC ; AQSSI ; Réseau informatique.

La généralisation de l'accès à l'internet, l'ouverture sur l'Europe, la mise en œuvre progressive des téléprocédures pour le bénéfice du citoyen et de l'entreprise, l'obligation de l'Etat de travailler en réseau conduisent à renforcer la vigilance du ministère en matière de sécurité des systèmes d'information (SSI).

Dans ce cadre, le plan de renforcement des SSI (PRSSI 2004-2007) impulsé par le Premier ministre exige une accentuation de l'effort consacré à cet égard.

Les systèmes d'information étant devenus indissociables de nos métiers et de fait stratégiques, il devient impératif de leur offrir un environnement protégé. Les réseaux, la messagerie, les centres serveurs, les centraux téléphoniques, les outils bureautiques, les applications, les accès physiques et logiques, l'environnement humain représentent autant d'enjeux.

A cet effet, le schéma directeur des systèmes d'information et de communication (SDSIC), prochainement publié, intégrera un volet sécurité spécifiant l'organisation et les actions à mener dans ce domaine. Il attribue les responsabilités comme suit :

- le responsable de la sous-direction DPSM/SI est responsable de la politique informatique nationale y compris la sécurité des systèmes d'information et du fonctionnement des infrastructures nationales ;
- le chef de service est responsable en outre de la mise en œuvre de la politique nationale, des systèmes d'information et infrastructures locaux ainsi que l'organisation correspondante ;
- la direction d'administration centrale est responsable des systèmes d'information métier nationaux dont elle a la charge.

Ces responsables se doivent d'initier, d'organiser et de suivre la prise en compte de la sécurité des systèmes

d'information à leur niveau. Pour cela, ils s'appuieront sur :

- l'autorité qualifiée en matière de sécurité des systèmes d'information (AQSSI) du ministère en la personne du sous-directeur des systèmes d'information de la DPSM ;
- un représentant SSI qui sera le relais de l'AQSSI dans chaque direction d'administration centrale ;
- un responsable de la sécurité des systèmes d'information (RSSI), garant de la sécurité dans chaque service.

Pour mener ces actions, les acteurs précités devront se référer aux recommandations du référentiel SSI. Il clarifie les objectifs de sécurité de manière pertinente, aide à la réalisation, puis à l'évaluation du plan local de sécurité.

Le RSSI devra conduire les phases de connaissance, d'action et d'évaluation en s'entourant d'appuis, celui du chef de service, du responsable informatique et d'autres acteurs. Il pourra utiliser les mesures d'accompagnement suivantes :

- la publication sur intranet du référentiel, de ressources documentaires, ainsi qu'un guide d'évaluation du niveau de sécurité du service ;
- une assistance pour la mise en œuvre du référentiel, par la mise à disposition des experts des Cété : conseillers en management de l'informatisation sur les aspects organisationnels et supports techniques sur la partie technique ;
- des formations proposées par les CIFP à destination des RSSI pour le volet organisationnel et des cellules informatiques pour les volets techniques.

Vous veillerez à la mise en œuvre du référentiel SSI. Ce référentiel est applicable dès à présent, mais la mise en œuvre de certaines règles peut nécessiter un certain temps. Il devra être appliqué intégralement au 1er janvier 2007 ; cependant, vous veillerez à appliquer avant le 1er juillet 2005 les règles primordiales du point de vue de la sécurité dont la liste est annexée à la présente circulaire.

Le haut fonctionnaire de défense,
G. Leblanc

Pour le ministre et par délégation :
Le directeur du personnel, des services et de la modernisation, vice-président de la Comib,
C. Parent

Direction du personnel, des services et de la modernisation

Référentiel de sécurité
des systèmes d'information pour les services
PRÉAMBULE
Janvier 2005
Version 1.0
SOMMAIRE

1. **Avant-propos**

Le présent document constitue le référentiel de sécurité des systèmes d'information du ministère. Il s'appuie sur des documents législatifs ou normatifs ainsi que sur les recommandations interministérielles, notamment de la direction centrale de la sécurité des systèmes d'information (DCSSI) et sur l'expérience et le savoir-faire du ministère.

1.1. *Concepts manipulés*

Référentiel de sécurité des systèmes d'information (SSI) :

Ensemble formalisé des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du système d'information et télécommunication du ministère.

Règles de sécurité :

Les règles de sécurité définissent les moyens et les mesures à mettre en œuvre dans le cadre de la politique de sécurité du ministère. Elles sont répertoriées par domaine à travers différents documents :

- préambule pour les règles de portées générales ;
- volet O pour les règles du domaine organisationnel ;
- volets 1 à 7 pour les règles techniques. Ces règles techniques sont explicitées dans des fiches détaillées et des procédures pour la mise en œuvre.

1.2. *Conventions d'écriture*

Dans la suite des volets du référentiel, nous utiliserons les conventions suivantes :

Numérotation des règles techniques :

La numérotation des règles commence par S, suivi du numéro du volet traité, puis du numéro de chapitre suivi d'un numéro incrémental. Exemple : S15.01 : Volet 1, chapitre 5, règle n^{o} 1.

Niveaux de recommandations :

O (obligatoire) : l'application de ces règles est obligatoire.

R (recommandé) : l'application de ces règles est fortement recommandée mais non obligatoire.

S (règle spécifique) : l'application de ces règles est obligatoire dans des cas particuliers.

2. **Qu'est ce que la sécurité des systèmes d'information (SSI) ?**

Le besoin de sécurité d'un système d'information se « mesure » généralement en termes de confidentialité (cf. note 1) , intégrité (cf. note 2) , disponibilité (cf. note 3) et, de plus en plus, en terme d'imputabilité (cf. note 4) (ou preuve). Afin d'effectuer ses « mesures », il est nécessaire de définir au préalable :

Les biens qui doivent être protégés ;

- les besoins de sécurité propres à chacun de ces biens ;
- leurs vulnérabilités ;
- les menaces découlant des vulnérabilités recensées ;
- les parades (ou contre-mesures) envisageables contrant les menaces identifiées.

2.1. *Les biens des services*

L'inventaire et la gestion des biens à sécuriser sont de la responsabilité du service. Ces biens doivent avoir suffisamment

de « valeur » ou d'importance pour justifier un certain degré de protection. Une estimation des risques acceptés par rapport à l'impact subit en cas de perte est à étudier pour chaque bien identifié.

Sont inclus en tant que biens :

- le patrimoine matériel, composé des biens matériels nécessaires au fonctionnement de ses activités et à la continuité du service public. Ce patrimoine est, dans une mesure significative, composé des matériels de télécoms et informatiques (systèmes centraux, serveurs, réseau, postes de travail, imprimantes...) ;
- le patrimoine immatériel, composé de toutes les informations concourant à l'exploitation des services qu'il offre (bases de données, documents électroniques, etc.) ;
- les informations relatives à son personnel dont l'altération ou la divulgation pourrait porter atteinte à la vie privée ;
- les informations en temps de crise ;
- le savoir-faire (productions du service telles que rapports, études, notes et données scientifiques, etc.) ;
- les locaux (au sens large du terme).

2.2. *Le besoin de sécurité des systèmes d'information*

Pour chaque bien identifié, il est nécessaire d'évaluer quel est son ou ses besoins en matière de disponibilité, intégrité, confidentialité et non-répudiation (preuve).

Exemple : les données concernant le personnel doivent avoir un niveau élevé de confidentialité et d'intégrité.

2.3. Les vulnérabilités

Ce sont les faiblesses en matière d'implantation physique, d'organisation, de personnel, de matériel ou logiciel concernant les systèmes d'information et qui peuvent être exploitées par une menace pour s'introduire dans le système et causer des dommages.

Par exemple, l'absence d'un mécanisme de contrôle d'accès à une base de données est une vulnérabilité qui peut favoriser une intrusion et causer le vol d'informations.

Une analyse des biens doit prendre en compte la vulnérabilité de chacun des biens.

2.4. *Les menaces*

Une menace engendre des attaques directes ou indirectes sur le service. À ce titre, elle peut amener à la dégradation des conditions de travail, mettre en péril le système d'information jusqu'à provoquer son indisponibilité. Elle peut être source de dégradation, destruction ou divulgation de données.

2.4.1. Typologie des menaces

Interne - utilisation des moyens autorisés à des fins non professionnelles ou personnelles ;
- usurpation de droits (passer de simple utilisateur à administrateur, etc.) ;
- accès à des ressources sensibles (mots de passe, fichiers de données, etc.) ;
- accès à des ressources interdites ;
- utilisation non conforme (déontologie, morale, législation, règles prescrites, modification non autorisée de configuration, mise en place de moyens illégaux, introduction ou utilisation de logiciels illicites (ex : copie de logiciel, utilisation sans licence d'exploitation, etc.) ;
- erreurs (saisie, manipulation, etc.) ;
- panne provoquant une indisponibilité (incident, malveillance, négligence, erreur).

Externe - intrusion ;
- usurpation d'identité ;
- pollution logicielle (virus, vers, chevaux de Troie, trappes, etc.) ;
- destruction.

2.4.2. Le risque

Il représente la potentialité qu'a une certaine menace d'exploiter les vulnérabilités. Le risque augmente suivant la valeur ou l'importance du bien (impact) et son niveau de vulnérabilité.

2.4.3. L'impact

Un événement indésirable portant atteinte aux biens peut avoir un impact plus ou moins important.

Les conséquences directes sont souvent l'indisponibilité mais peuvent aller jusqu'à la dégradation ou la perte du bien. L'incident engendre généralement un dysfonctionnement partiel voir total du service.

L'impact peut traduire la valeur qu'on attache à un bien.

2.4.4. Les contraintes

Les objectifs, stratégies et politiques doivent prendre en compte les contraintes et exigences du ministère. Ces contraintes peuvent être de niveau organisationnel, environnemental, législatif, technique, financier ou délais.

2.5. *Les parades*

Les parades sont des mesures mises en place afin de réduire les vulnérabilités du système et limiter l'impact subi lors d'un incident.

Par exemple, pour une base de données se trouvant sur un poste isolé, on peut contrôler l'accès physique au poste et avoir une copie (sauvegarde) dans un endroit sécurisé.

Mais pour des cas plus complexes où les données sont réparties dans un réseau étendu, une parade peut être une combinaison de plusieurs mesures de sécurité.

Dans ce cas, répondre à l'objectif de sécurité peut amener à définir des règles de sécurité dans différents domaines (organisation, réseaux, serveurs, ...).

Les mesures qui peuvent être mises en œuvre sont les suivantes :

- mesures dissuasives : respect des mesures qui peuvent être mis en œuvre ;
- mesures structurelles : règlements ;
- mesures préventives : sensibilisation du personnel, veille technologique, suivi technique en liaison avec le centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques (CERTA (cf. note 5)) ;
- mesures palliatives et de récupération.

2.6. *Combien coûte la non-sécurité ?*

On dit souvent que « la sécurité, ça coûte cher », mais on oublie que l'absence de sécurité coûte plus cher encore. Tout l'art de la gestion du risque est de trouver le juste compromis entre « ce que ça coûte » et « ce que l'on risque de perdre ». La SSI n'est donc pas une recherche mythique « du risque zéro », mais plutôt la recherche de l'organisation offrant la meilleure efficacité.

Le « retour sur investissement » d'une politique de prévention est d'abord financier. Il s'évalue en dommages directs évités : pertes de données, de propriétés intellectuelles, de savoir-faire, d'informations...

Ces dommages sont souvent cités car leurs coûts sont visibles ; mais il ne faut pas oublier le coût en « organisation » des malveillances informatiques qui sont souvent supportés par la collectivité tout entière. Elles s'expriment par exemple en diminution de l'efficacité, en pertes de capacité et de productivité :

- indisponibilité des machines générant des pertes de temps (une intrusion peut « coûter » une coupure des services de plusieurs heures) ;
- immobilisation des personnels pour réparer (personnels techniques) ou pour attendre le retour à une situation normale (utilisateurs).

C'est aussi une altération de l'image du ministère et, par contrecoup, de la confiance de nos partenaires.

3. **Pourquoi un référentiel ?**

3.1. *Contexte de la sécurité des systèmes d'information*

Compte tenu du niveau des risques liés à la pression continue de la menace, une défaillance de la sécurité du système d'information pourrait entraîner des conséquences irréversibles sur la réalisation des objectifs stratégiques du ministère ou vis à vis du respect de ses obligations ou engagements.

Face aux menaces qui pèsent sur les systèmes d'information, l'utilisateur (cf. note 6) exige une protection adaptée des informations et des services de traitement, d'archivage et de transport de l'information. La sécurité est donc devenue l'une des dimensions essentielles de la stratégie du ministère et elle doit être prise en compte dès la conception d'un système d'information afin d'assurer la protection des biens et des personnes et du patrimoine du ministère. Ainsi, la sécurité des systèmes d'information vise en particulier à protéger les composantes suivantes :

- le patrimoine matériel, composé des biens matériels nécessaires au fonctionnement de ses activités et dont la détérioration pourrait interrompre, diminuer ou altérer son activité ; ce patrimoine est essentiellement composé des technologies de l'information et de communication (serveurs, réseau, postes de travail, téléphonie...), mais aussi des procédures et applications logicielles traduisant les processus et les fonctions métiers du ministère ;
- le patrimoine immatériel et intellectuel, composé de toutes les informations concourant au métier de l'organisme (données scientifiques, techniques, professionnelles, administratives...) ;
- les informations relatives aux personnes (physiques et morales) avec qui le ministère est en relation, dont la destruction, l'altération, l'indisponibilité ou la divulgation pourrait entraîner des pertes ou porter atteinte à son image de marque voire entraîner des poursuites judiciaires.

Rappelons que les risques informatiques, tout comme les risques informationnels, sont des risques opérationnels pour les systèmes d'information malgré leur caractère partiellement immatériel.

3.2. *Nécessité d'un référentiel SSI*

Dans ce contexte, DPSM/SI a souhaité faire rédiger un référentiel de sécurité des systèmes d'information, afin, d'une part de spécifier les objectifs de sécurité d'un système de manière pertinente, et d'autre part d'avoir les moyens d'évaluer la

réalisation de ces objectifs de sécurité en mesures afin de garantir un certain niveau de confiance dans la sécurité du système.

Le référentiel SSI constitue un cadre de référence et de cohérence :

- pour l'intégration de la sécurité lors de la conception d'un système d'information ;
- pour l'ensemble des activités et des acteurs du ministère par rapport auxquels toute évolution du système d'information devra être justifiée ;
- pour aider les personnes chargées d'élaborer et de mettre en œuvre des mesures, des consignes et des procédures cohérentes en vue d'assurer la sécurité des systèmes d'information ;
- pour prendre en compte les référentiels de sécurité et d'exploitation (cf. note 7) réalisés lors de la mise en place du réseau interministériel Ader, ces mesures s'appliquant à tous les agents et équipements raccordée directement ou indirectement à ce réseau.

Ce référentiel SSI offre les bénéfices suivants :

- une vision stratégique de la gestion des risques globaux, dont la SSI, visant à informer les maîtrises d'ouvrage des enjeux et susciter la confiance dans le système d'information ;
- la mise en évidence des objectifs, obligations et engagements du ministère vis-à-vis de ses usagers et partenaires en fonction des lois applicables, ainsi que les principes de sécurité régissant la protection de son propre patrimoine ;
- la promotion de la coopération entre les différents services ou unités du ministère pour l'élaboration et la mise en œuvre de telles mesures, consignes et procédures ;
- l'assurance de la cohérence et de la pérennité des actions de sécurité (analyse de risques, mise en œuvre des mesures...) en indiquant les directives nécessaires, notamment pour tout choix technique mais aussi organisationnel ou contractuel, en matière de sécurité ;
- une graduation des moyens (avec une proportionnalité assurée par l'analyse des risques) par application des principes et règles de sécurité minimale à respecter pour l'ensemble des activités et des systèmes ;
- la sensibilisation aux risques menaçant les systèmes d'information et les moyens disponibles pour s'en prémunir et informer l'ensemble des acteurs sur leurs responsabilités ;
- une aide aux chefs de projet pour intégrer la sécurité au plus tôt dans les développements de nouveaux services du système d'information.

De plus, l'élaboration du référentiel SSI est l'occasion de repenser dans une démarche structurée et à finalité opérationnelle, la sécurité du système d'information en commençant par l'organisation mise en place pour répondre à ce besoin en modifiant la culture du ministère.

Il est un élément de la politique générale du ministère et à ce titre il est en accord avec le schéma directeur des systèmes d'information et communication.

3.3. *Les bases de légitimité du référentiel SSI*

Les règles contenues dans ce document puisent leur légitimité dans les lois, les réglementations, les normes et les recommandations émanant d'instances internationales, nationales ou professionnelles. Elles constituent une synthèse homogène et cohérente des règlements antérieurs.

Préservation des intérêts vitaux de l'Etat.

Les organismes gouvernementaux et ceux qui collaborent avec eux sont soumis au respect des lois nationales et aux instructions interministérielles.

Lorsqu'un ministère, y compris en dehors de sa mission propre, est amené contractuellement ou non à utiliser ou traiter des informations sensibles il doit appliquer les lois et les textes réglementaires spécifiques qui s'y rapportent.

Les deux recommandations sur la protection des éléments non classifiés de défense s'appliquant au ministère sont les suivantes :

- la recommandation REC 901 (cf. note 8) qui recommande une harmonisation entre les mesures prises au titre de la protection du secret de défense et celles concernant la protection des informations sensibles ;
- la recommandation REC 600 (cf. note 9) présente des recommandations relatives aux informations, aux systèmes ou aux applications ne relevant pas du secret de défense, mais dont la destruction, le détournement ou l'utilisation frauduleuse pourraient porter atteinte aux intérêts nationaux, au patrimoine scientifique et technique ou à la vie privée ou professionnelle des individus. Ces recommandations concernent la sécurité des postes de travail autonomes ou connectés à un réseau.

3.3.2. Préservation des intérêts particuliers du ministère

Le ministère doit protéger son métier et sa culture notamment son savoir-faire ce qui lui impose de prendre toutes les mesures nécessaires pour garantir la pérennité de son action.

3.3.3. Protection du patrimoine

Le traitement d'informations liées aux personnes physiques et le respect des règlements qui lui sont imposés dans le cadre de ses missions, oblige le ministère à protéger son patrimoine sur lequel repose sa capacité à maintenir et à développer des services efficaces et de qualité.

La protection de ce patrimoine contre toute possibilité d'altération ou de divulgation, interne ou externe, constitue un des

objectifs majeurs pour le ministère. Pour cela :

- les relations de l'organisme avec son environnement doivent être formalisées par des contrats passés avec des tiers ;
- les engagements pris envers d'autres organismes font l'objet de contrats ou de conventions où peuvent figurer en particulier des clauses spécifiques concernant la sécurité des systèmes d'information. Elles sont d'autant plus importantes que la nature des engagements concerne une composante stratégique. Un exemple est celui des contrats de sous-traitance, pour lesquels il existe souvent des clauses spécifiques relatives par exemple à la fourniture de programmes-sources et à leur usage.
- dans le cadre de coopération internationale, les engagements contractuels garantissent les parties et doivent être en accord avec la réglementation des pays concernés.

Plus généralement, dans le cadre des relations avec l'environnement, le service demandeur doit faire valoir les exigences suivantes :

- vis-à-vis des fournisseurs : le devoir de conseil, de qualité et de pérennité de la maintenance et de l'assistance ;
- vis-à-vis des prestataires de services : le devoir de conseil, l'obligation de moyens et de résultats ;
- vis-à-vis de la sous-traitance : les clauses spécifiques garantissant la non concurrence et la confidentialité ;
- vis-à-vis des autres ministères : les clauses spécifiques pour la coopération et l'interopérabilité des systèmes d'information.

3.3.4. Les ressources du ministère

Le service est une unité économique de production de biens ou de services, composée de ressources humaines, juridiques, techniques et financière. Les unités ont, assez souvent, des missions et des objectifs différents qui peuvent apparaître comme des contraintes que la sécurité doit prendre en compte. Par exemple :

- pour les ressources humaines : nécessité de la confidentialité des données ;
- pour les ressources juridiques : nécessité de la confidentialité des contrats ;
- pour le savoir-faire et les ressources techniques : nécessité de la protection des projets et des données ;
- pour les ressources financières : nécessité de la confidentialité des comptes avant leur publication.

3.3.5. Protection de l'image

Toute action conduisant à la divulgation, au vol, à la destruction ou à l'intégrité des informations ou des systèmes sous la responsabilité du ministère peut porter atteinte à l'image et, dans une certaine mesure, à la pérennité des services qu'elle offre.

L'un des objectifs de sécurité consiste ainsi à se protéger contre tout risque d'atteinte de la pérennité des services qu'il rend dans le cadre de sa mission.

3.3.6. Disponibilité des systèmes d'information

Le ministère ne peut aujourd'hui assurer sa mission qu'en s'appuyant sur un système d'information disponible et fiable. L'assurance de la disponibilité des informations, des applications, des systèmes et des réseaux constitue un des objectifs majeurs de sécurité.

3.3.7. La gestion des risques : accidents, erreurs, défaillances et malveillances

Les accidents pouvant survenir à l'intérieur du ministère ou provoqués à l'extérieur de celui-ci par ses activités peuvent entraîner des atteintes aux personnes, aux biens, à l'environnement (au patrimoine national ou privé). Aussi, est-il fait obligation légale à tous les responsables de lutter, avec les moyens appropriés, contre les accidents divers.

Si cette préoccupation est généralement prise en compte au niveau de la sécurité générale (et tout particulièrement celle qui touche aux personnels), elle est rappelée dans ce chapitre pour souligner que dans de nombreux cas les accidents de toute nature peuvent avoir pour cause des erreurs ou malveillances commises dans l'utilisation du système d'information.

La liste des altérations spécifiques à la sécurité comprend habituellement, sans y être limitée, le déni d'accès à une information ou une fonction (perte de disponibilité), le dommage provoqué à une information ou une fonction par une modification non autorisée (perte d'intégrité) ou la divulgation nuisible d'une information ou une fonction à des destinataires non autorisés (perte de confidentialité).

Indépendamment de l'obligation faite par la loi, il est un devoir prioritaire pour les responsables de renforcer les contrôles de sécurité partout où il existe un risque lié à l'utilisation du système d'information.

La sécurité a trait à la protection des biens contre les menaces, ces dernières étant classées selon leur potentiel de nuisance envers les biens à protéger. Toutes les catégories de menaces devraient être prises en compte, mais dans le domaine de la sécurité, une plus grande attention est accordée aux menaces liées à des activités malveillantes ou non [ISO 15408].

3.3.8. La lutte contre la malveillance et le cybercrime

Le ministère doit prendre les mesures qu'il juge nécessaire à la protection de son système d'information (mesures de

prévention, de détection et de réparation), afin de se protéger contre les menaces redoutées, qu'elles soient accidentelles ou intentionnelles comme, par exemple, l'interception, le détournement, l'utilisation ou la divulgation non autorisée d'éléments du système d'information.

Au niveau national, les logiciels sont considérés comme des œuvres de l'esprit protégées par le code de la propriété intellectuelle (cf. note 10) et des lois réglementent les peines associées aux infractions telles que :

- la copie ou l'utilisation illicite de logiciel ;
- la divulgation non autorisée de documents techniques ou commerciaux, même après une rupture de contrat ;
- le délit ou la tentative de délit, avec ou sans entente concertée, correspondant aux infractions comme l'accès ou le maintien frauduleux dans tout ou partie d'un système, l'entrave au fonctionnement, la modification de données ;
- l'interception de télécommunications.

Au niveau de l'union européenne la REC CRIM (cf. note 11) sur la criminalité en relation avec l'ordinateur et la D250 (cf. note 12) sur la protection juridique des programmes d'ordinateur réglementent la protection du logiciel.

3.3.9. Le respect de la déontologie

L'utilisation croissante des systèmes d'information par un large public conduit à appliquer aux métiers utilisant les technologies de l'information de grands principes d'éthique tels que la garantie des droits de l'homme, la protection et le respect de la vie privée, la garantie des libertés individuelles ou publiques. Ces principes, appliqués au domaine des systèmes d'information, sont formulés :

- au niveau international par la déclaration universelle des droits de l'homme (cf. note 13) , les principes directeurs de l'ONU (cf. note 14) et les lignes directrices de l'OCDE (cf. note 15) ;
- au niveau de l'union européenne par la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (cf. note 16) et par les directives du conseil de l'union européenne notamment la directive 2002/58/CE du Parlement européen (cf. note 17) et du Conseil du 12 juillet 2002 relative au traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ;
- au niveau national par la déclaration des droits de l'homme, la loi « Informatique et Libertés » (cf. note 18) , le rapport de la CNIL sur la cyber-surveillance sur les lieux de travail publié le 5 février 2002 (cf. note 19) ;
- au niveau du ministère par les codes d'éthique des technologies de l'information.

3.3.10. Le respect des obligations juridiques

Les lois sont universelles et « nul n'est censé ignorer la loi ». Ainsi, des obligations pèsent sur les différents éléments constitutifs du ministère.

Les services du ministère doivent respecter les directives pour toutes les informations portées à leur connaissance même s'ils n'en sont pas responsables. Il est donc indispensable que toutes les obligations civiles et pénales soient connues et comprises et que chacun soit pleinement conscient de ses obligations vis-à-vis des lois et règlements afin d'assumer ses responsabilités.

Par ailleurs, le ministère et ses différents acteurs sont liés entre eux et vis-à-vis de tiers par des relations de natures diverses. Il en découle des obligations pour les personnes physiques et morales au sein du ministère comme chez les tiers avec lesquels il est en relation.

3.3.11. Le contrôle des communications

La loi relative à la liberté de communication (cf. note 20) concerne le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications.

3.3.12. La signature électronique

Suite à la loi du n° 2000-230 du 13 mars 2000 (cf. note 21) , le code civil précise : « La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission ».

Il précise également que « l'écrit sur support électronique a la même force probante que l'écrit sur support papier ».

La loi précise que : « lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous les moyens le titre le plus vraisemblable, quel qu'en soit le support ».

La directive européenne D93 (cf. note 22) précise le cadre communautaire pour les signatures électroniques.

4. **Définition du référentiel de sécurité pour les services**

4.1. *Contenu du référentiel SSI*

Le référentiel est composé d'une part d'un volet organisationnel qui décrit les principes de la SSI et l'organisation du ministère en terme de sécurité et, d'autre part, de volets techniques qui donnent les règles à respecter pour garantir la sécurité du système d'information.

Les volets techniques sont décomposés par thème :

- réseaux - liaisons et moyens actifs ;
- autocommutateurs téléphoniques ;
- serveurs ;
- postes de travail et périphériques partagés ;
- sécurité physique, locaux et accès ;
- accès informatiques, authentification ;
- applications, messagerie.

Chaque volet est constitué de deux parties, la première donnant des objectifs de sécurité relatifs à la sécurité propre au volet et la deuxième définissant les règles de sécurité. A chaque règle est associée une fiche technique détaillée qui définit le besoin, le risque et la menace qui y sont associées. Cette fiche fait référence, si nécessaire, à une procédure de mise en œuvre.

Un guide d'évaluation sera mis à disposition de chaque service en vue d'obtenir un instantanée de l'état de sécurité (points forts - points faibles).

Une charte utilisateur s'appuyant sur les règles du référentiel sera également mise à disposition pour une adaptation locale si nécessaire.

4.2. *Evolution du référentiel SSI*

Le référentiel sera mis à jour en fonction des évolutions technologiques et du contexte du ministère. Ces mises à jours seront à la charge de chaque point d'appui national pour les domaines qui les concernent sous la responsabilité de DPSM/SI.

4.3. *Diffusion du référentiel SSI*

Une circulaire d'application demandera à chaque service de mettre en œuvre les recommandations contenues dans le référentiel SSI.

L'ensemble de ces informations sera regroupé sur un site intranet qui permettra une navigation aisée entre les règles, les fiches techniques associées et les procédures.

Des journées de formation seront organisées d'une part sur la partie organisationnelle et, d'autre part, sur les volets techniques. Elles seront destinées à la voie fonctionnelle sécurité et aux personnels techniques.

Le référentiel devra être porté à connaissance des utilisateurs par des actions de sensibilisation à la sécurité et par la rédaction d'une charte utilisateur. Ces actions sont à la charge du service.

4.4. *Moyens d'évaluation de l'application du référentiel SSI*

L'évaluation de l'application du référentiel SSI peut être réalisée à la demande du service (auto-évaluation ou audit) ou lui être imposée (DPSM/SI, service du HFD ou CGPC).

MOYENS d'évaluation	**QUI DEMANDE**	**QUI RÉALISE**	**QUI REND COMPTE à qui**
L'auto-évaluation	Le service	Le service à partir : Du guide d'évaluation avec éventuellement l'aide du support technique ; De sondage aléatoire dans les unités réalisées par le responsable SSI ou la hiérarchie ; Sur la base d'une grille avec des questions clés (check-list) lors de l'entretien annuel d'évaluation.	En fonction du constat, l'ensemble des acteurs des chaînes hiérarchique, technique et fonctionnelle est susceptible d'être destinataire pour intervention éventuelle.
L'audit	Le service	Un expert du Cété Un consultant externe	L'auditeur rend compte uniquement au service demandeur sans autre communication, le service demandeur étant le propriétaire du rapport
Le contrôle	DPSM/SI Le service du HFD Le CGPC Les autorités judiciaires	DPSM/SI Service du HFD Les inspecteurs généraux lors de leurs inspections périodiques. Tout consultant mandaté. A cet effet, les services doivent tenir à jour un dossier Sécurité comprenant le tableau de bord SSI et la liste des dérogations aux règles de sécurité.	En fonction du constat, l'ensemble des acteurs des chaînes hiérarchique, technique et fonctionnelle sont susceptibles d'être destinataires.

4.5. *Champ d'applications*

4.5.1. Domaines concernés

Le ministère gère un patrimoine dont il est garant et responsable.

Les systèmes d'information supportant ce patrimoine se trouvent répartis sur de nombreux systèmes et la diversité des acteurs sont importants. La maîtrise de leur sécurité implique donc une vision globale. Par conséquent, le référentiel SSI s'applique à la totalité du système d'information du ministère. On notera, en particulier, les points suivants :

- il s'applique à un système existant ou à développer ;
- il concerne l'ensemble des aspects du système d'information (l'organisation, l'environnement physique, le développement, l'exploitation, la maintenance,...) ;
- il concerne l'ensemble du cycle de vie du système d'information et de l'information.

4.5.2. Entités concernées

Toutes les entités organisationnelles du ministère, ainsi que les services hébergés (ex : les organisations syndicales) doivent mettre en œuvre les recommandations données dans ce référentiel notamment pour ce qui concerne les règles des volets techniques.

4.5.3. Personnels concernés

Il concerne toute personne ayant accès au système d'information du ministère qu'il soit interne ou externe à celui-ci (sous-traitant, stagiaire, prestataire tel que personnels de gardiennage, personnels de nettoyage). Par conséquent, pour être appliqué, ce document doit être connu de l'ensemble de ces personnes. Il doit donc être largement diffusé, sous une forme simplifiée et didactique, à l'ensemble du personnel. Cette diffusion sera accompagnée d'une sensibilisation du personnel, portant sur le rappel des principes, de l'organisation et des règles de sécurité les concernant. A ce titre, une charte utilisateur type est mise à disposition des services.

Le volet « Organisation » du référentiel SSI au sein du ministère présente les règles organisationnelles auxquelles sont soumises toutes les personnes internes ou externes au ministère.

Chaque volet technique est constitué de trois parties, la première donnant les objectifs de sécurité relatifs au volet, la deuxième définissant les règles de sécurité associées et la dernière rassemblant les fiches techniques détaillées de ces règles. La première partie s'adresse à l'ensemble du personnel en particulier le chapitre « les principes généraux ». Les deux autres parties sont plus orientés vers le personnel technique, excepté pour les volets « poste de travail » et « accès physique » qui ont une portée plus générale en s'adressant à l'ensemble du personnel du ministère (interne et externe). A chaque règle sont associés le ou les acteurs impactés par la mise en œuvre de la règle.

5. **Règles génériques**

Ces règles sont de portée générale et doivent être appliquées par l'ensemble du personnel du ministère.

RÈGLE	PRIORITÉ	APPLICABLE pour les acteurs	DESCRIPTIF
S01.11	O	tous	Toutes les règles présentes dans ce document prédominent sur les règles antérieures.
S01.12	O	tous	Tout ce qui n'est pas explicitement autorisé est interdit.
S01.13	O	tous	Chaque service doit se protéger conformément aux spécifications du ministère.
S01.14	O	tous	L'ensemble des règles présentes dans ce document s'applique à toutes les entités du ministère y compris les services hébergés.
S01.15	O	tous	Chaque utilisateur doit appliquer les dispositions réglementaires et mettre en application les règles qui les concernent.

Direction du personnel,
des services et de la modernisation

Référentiel de sécurité
des systèmes d'information pour les services
ORGANISATION DE LA SÉCURITÉ
Version 1
de janvier 2005

SOMMAIRE

1. **Introduction**

Ce document constitue le volet organisation du référentiel sécurité du ministère. Il traduit en termes applicables la volonté du ministère de mettre en œuvre l'organisation nécessaire pour protéger de la manière la plus efficace le patrimoine que représente le système d'information, et de préserver son fonctionnement en tant qu'outil de production. Les volets techniques complètent ce document en traduisant sous forme de règles de sécurité les exigences et les moyens permettant de sécuriser toutes les ressources constituant le système d'information (applications et infrastructures) dans toutes ses phases (élaboration, exploitation, mise au rebus). La mise en œuvre de ces règles de sécurité est décrite dans des procédures.

Le référentiel concerne tous les composants matériels et logiciels du système d'information ainsi que les bâtiments et locaux du ministère. Il s'applique à l'ensemble du personnel du ministère ainsi que, de manière contractuelle à l'ensemble des partenaires, à tous les composants matériels et logiciels du système d'information et aux bâtiments et locaux du ministère, à l'exception des services sous la responsabilité de la direction générale de l'aviation civile (DGAC).

2. **Acteurs et responsabilités**

Chaque responsable d'un élément du système d'information est responsable de sa sécurité :

- la politique informatique nationale, y compris la sécurité des systèmes d'information (SSI) et le fonctionnement des infrastructures nationales, est de la responsabilité de DPSM/SI ;
- les infrastructures locales sont de la responsabilité du chef de service ;
- les systèmes d'information métier sont de la responsabilité de la direction d'administration centrale correspondante.

2.1. *Au niveau national*

2.1.1. Le ministre

La sécurité des systèmes d'information relève de la responsabilité de chaque ministre pour le département dont il a la charge.

2.1.2. Le haut fonctionnaire de défense (HFD)

Le haut fonctionnaire de défense est le conseiller du ministre en la matière. Il vérifie et garantit l'application des dispositions relatives à la sécurité de défense, à la protection du secret et à la sécurité des systèmes d'information. Il assure la liaison avec les commissions interministérielles spécialisées. En outre, il pilote la réalisation et le suivi des exercices interministériels, il élabore le bilan annuel SSI dans le champ de compétence ministériel (services et opérateurs) et le transmet à la direction centrale de la sécurité des systèmes d'informations (DCSSI).

Il peut demander, lorsqu'il le juge nécessaire, un audit sur un élément de l'infrastructure nationale ou locale ou systèmes d'informations métiers.

Il anime le réseau des délégués ministériels de défense et celui des autorités qualifiées en matière de sécurité des systèmes d'information (AQSSI) (ministère et opérateurs).

Il se fait assister dans ces missions par un fonctionnaire de sécurité des systèmes d'information (FSSI).

2.1.3. L'autorité qualifiée en matière de sécurité des systèmes d'information (AQSSI)

Le sous-directeur des systèmes d'information de la DPSM est l'AQSSI au sens de la recommandation 901 (cf. note 23) . Il

est chargé de faire élaborer et mettre en œuvre par sa sous-direction la politique informatique du ministère. Dans ce cadre :

- il informe les directions d'administration centrale et les services de cette politique et des plans d'action associés ;
- il veille au respect de cette politique et met en place les structures et méthodes de contrôle ;
- il assure la maîtrise d'ouvrage de l'infrastructure nationale (réseau, messagerie, centres serveurs, centres d'expertise et d'assistance, équipes de maîtrise d'œuvre) et à ce titre assure la maîtrise d'ouvrage de sa sécurité ;
- il demande des enquêtes/investigations se rapportant à la SSI et peut à ce titre demander l'audit d'éléments constituant l'infrastructure nationale ;
- il coordonne et pilote le dispositif de surveillance et de gestion des incidents (notamment le bon fonctionnement de la cellule d'alerte nationale) ;
- il anime le réseau des responsables SSI régionaux.

Il se fait assister pour la définition de la politique par un chargé de mission sécurité au niveau national et au niveau régional par un représentant régional SSI qui assure le suivi de la politique nationale et l'animation auprès des services.

2.1.4. Les directeurs d'administrations centrales

Les directeurs d'administrations centrales sont responsables des systèmes d'informations métiers qu'ils produisent. Ils nomment un représentant SSI qui peut être lui-même ou une personne qu'il aura désignée. Ce représentant SSI aura pour mission de :

- être le relais de l'AQSSI au niveau de la direction d'administration centrale ;
- définir la politique de sécurité particulière des applications et systèmes d'information dont la direction a la charge et en évaluer le niveau de sécurité effectif ;
- définir le niveau de sensibilité des ressources supportant leur système d'information et de les classifier en conséquence ;
- élaborer les consignes et les directives de sécurité dans la conception et la mise en œuvre des applications et systèmes d'information ;
- conseiller et assister les maîtrises d'ouvrage de projets SI en matière de sécurité ;
- s'assurer que la sécurité est bien prise en compte à toutes les étapes des projets ;
- former et sensibiliser les maîtrises d'ouvrage et les maîtrises d'œuvre à la sécurité.

2.1.5. La cellule d'alerte du ministère

Cette cellule d'alerte nationale est le point d'entrée unique des alertes du ministère aussi bien des alertes externes, provenant notamment de l'interministériel, que des alertes internes émanant des services du ministère. Elle assure le suivi des alertes sécurité.

Elle joue le rôle d'interface entre l'instance décisionnelle (AQSSI), les points d'appui concernés par une alerte et les différents acteurs qui ont besoin d'en être informés (HFD, centres serveurs et services). Elle constitue par les actions qu'elle peut engager le bras « opérationnel » de l'AQSSI.

Elle constitue un tableau de bord des anomalies/incidents qu'elle transmet mensuellement à l'AQSSI.

2.1.6. Les centres serveurs

Ils gèrent l'exploitation des applications centralisées. A ce titre, ils doivent garantir la disponibilité, la confidentialité et l'intégrité des données qui sont stockées sur les serveurs dont ils ont la responsabilité. Ils transmettent les anomalies/incidents à la cellule d'alerte.

Dans le cas où les centres serveurs sont externalisés, les contrats doivent intégrer les obligations de sécurité que doivent respecter les exploitants.

Un responsable sécurité devra être nommé pour gérer et traiter les aspects « sécurités ».

2.1.7. Les équipes ressources

Les points d'appui ont la responsabilité de traiter la sécurité dans leur domaine respectif (veille technologique, recommandations, traitement des alertes).

Sur demande, les services peuvent également consulter les experts techniques et les conseillers en management pour assurer l'évaluation et la formation. Ces deux fonctions peuvent être externes ou internes au ministère.

2.2. *Au niveau régional*

2.2.1. Les représentants régionaux SSI

Les représentants régionaux SSI (RRSSI) sont le relais de l'AQSSI au niveau régional. Dans ce cadre, ils assure le suivi de la politique informatique nationale dans le domaine de la sécurité des systèmes d'information et, à ce titre, vérifie que les chefs de service mettent en place l'organisation nécessaire et définissent leur plan d'action. Il suit l'avancement de la mise en œuvre des règles de sécurité au niveau des services et en rend compte semestriellement au niveau de l'AQSSI ou immédiatement lorsqu'un problème grave aura été constaté. Il assure, pour le compte de l'AQSSI, l'animation auprès des services (organisation de formations et information).

Il est force de proposition pour toute évolution de la politique de sécurité.

2.2.2. Les délégués ministériels de défense

Les délégués ministériels de défense sont le relais du HFD auprès des services. Il contrôle la prise en compte et la mise en œuvre de la sécurité au sein des services. Il veillera à ce qu'un rapport d'activité annuel avec tableau de bord des actions et liste des dérogations soit réalisé et transmis au service du HFD, avec copie à l'AQSSI.

Il contrôle également la mise en œuvre des mesures SSI dans les plans de sécurité (Vigipirate et Piranet entre autre).

Il assure le relais du service du HFD lors des exercices inter-ministériels.

2.3. *Au niveau local*

La politique de sécurité des systèmes d'information du ministère doit être mise en application au niveau local et adaptée aux contraintes du service. La structure de sécurité doit être mise en place pour garantir la bonne exécution des mesures de sécurité qui s'imposent. Elle doit correspondre à la structure de responsabilité hiérarchique (fonctionnelle ou opérationnelle).

2.3.1. Le chef du service

Le chef de service est responsable de l'application des mesures nationales destinées à assurer la sécurité des systèmes d'information. Il est responsable de l'ensemble des postes de travail et de leur sécurité, de l'octroi et de la gestion des droits d'accès aux diverses ressources informatiques, de l'accès aux ressources et bâtiments.

A ce titre :

- il évalue la sécurité de son service par rapport aux exigences nationales ;
- il définit les objectifs et exigences de sécurité et veille à leur respect ;
- il élabore le plan d'action et le suivi de l'application des règles du référentiel sécurité (tableau de bord) ;
- il alloue les ressources financières et humaines cohérentes avec le maintien d'un niveau de sécurité conforme aux exigences nationales ;
- il engage la réalisation d'études concernant la sécurité du système d'information dont il a la charge ;
- il contrôle le respect des règles de sécurité au sein de son service ;
- il sensibilise et responsabilise les responsables d'unité sur leur devoir de respecter et faire respecter les lois et règlements par le personnel qu'il gère ;
- il sensibilise les utilisateurs aux risques encourus par l'usage de l'informatique et leur donne les moyens d'y faire face. A ce titre, il réalise une charte utilisateur et des actions de sensibilisation.

Il nomme un responsable SSI (RSSI) qui peut-être lui-même ou une autre personne qu'il aura désignée.

2.3.2. Le responsable SSI

Le responsable SSI est garant de la sécurité du service. A ce titre, il doit veiller à l'efficacité des mesures choisies et installées. Il s'appuie sur le secrétariat général notamment le support informatique du service pour la mise en œuvre technique des mesures de sécurité. Ses missions porteront sur :

- la définition du plan d'action ;
- l'évaluation de la sécurité dans le service ;
- le suivi de la mise en œuvre des mesures de sécurité ;
- la réalisation de contrôles.

2.3.3. Les responsables d'unité

Les responsables d'unité sont responsables de l'application de la politique de sécurité des systèmes d'information au sein de leur unité. A ce titre, ils contrôlent le respect des lois et règlements par le personnel qu'ils gèrent. Tout en adoptant un comportement ayant valeur d'exemple, les responsables d'unité :

- accordent les droits d'accès en rapport avec les besoins de l'utilisateur ;
- vérifient régulièrement l'application des règles de sécurité et le respect des directives (messagerie, charte utilisateur), ainsi que l'utilisation stricte des droits accordés ;
- s'assurent de la sensibilisation effective des utilisateurs ;
- rendent compte par la voie hiérarchique au RSSI, notamment lorsqu'ils constatent le non-respect des lois et règlements par le personnel qu'il gère.

2.3.4. Le point d'alerte local

Le chef de service met en place l'organisation nécessaire pour mettre en œuvre localement un point d'alerte accessible selon les besoins du service par ses agents. Il joue le rôle d'interface entre l'instance décisionnelle (RSSI), la cellule informatique et les différents acteurs qui ont besoin d'en être informés (agents, responsables d'unité, exploitants). Il analyse et qualifie les informations et les transmet à la cellule alerte nationale si nécessaire. Il réalise un suivi des anomalies/incidents qu'il transmet régulièrement au responsable SSI du service.

2.3.5. Les agents

Chaque agent est responsable vis-à-vis de sa hiérarchie des moyens informatiques du service et notamment du poste de travail qui lui est affecté :

- il s'engage à respecter les obligations légales et réglementaires qui lui sont notifiées par l'intermédiaire d'une charte utilisateur et avoir un comportement conforme aux principes et règles énoncés au sein du code de déontologie ;
- il doit participer à toute action de sensibilisation à laquelle il est convié par sa hiérarchie ;
- il doit informer le point alerte local de tout problème rencontré sur son poste ainsi que son responsable hiérarchique lors de toute infraction à la politique de sécurité qu'il aurait commise, volontairement ou non.

2.3.6. Organisme et personnels hébergés

Les conditions d'utilisation des systèmes d'information du ministère par les organismes et personnels hébergés doivent être formalisées par une convention signée par ceux-ci. Ils sont, en outre, soumis aux même obligations que les agents du ministère.

Schéma d'organisation

3. **Mise en œuvre de la SSI**

Ce chapitre décrit les actions à engager par les différents acteurs identifiés au chapitre précédent pour mettre en œuvre la sécurité des systèmes d'information.

Dans le cadre du contrôle, deux acteurs, non nommés précédemment, peuvent être impliqués :

- le Conseil général des Ponts-et-Chaussées (CGPC) qui peut faire des contrôles dans le cadre de ses inspections ;
- les autorités judiciaires dans le cadre d'enquête.

3.1. *Au niveau du HFD*

3.1.1. Diffusion des informations liées aux plans de sécurité

Le HFD s'appuie sur les directeurs d'administration centrale et sur le réseau des délégués ministériels de défense (DRE de Zone) pour notifier les instructions concernant le niveau et les actions à engager dans le cadre des plans de sécurités (Vigipirate et Piranet entre autre) vers le responsable SSI local en tenant informé l'AQSSI et les représentant régionaux SSI.

3.1.2. Suivi et contrôle

La vérification de l'application des dispositions relatives à la sécurité de défense, à la protection du secret et à la sécurité des systèmes d'information est assuré par le réseau des délégués ministériels de défense des zones de défense.

Le HFD peut demander l'audit des éléments d'infrastructures nationales ou locales ou systèmes d'informations métiers auprès d'un organisme externe ou du bureau audit de la direction centrale de la sécurité des systèmes d'information (DCSSI).

3.1.3. Formalisation du rôle des délégués ministériels de défense

Le HFD forme les délégués ministériels de défense à la sécurité et formalise leur action dans ce domaine.

3.2. *Au niveau de l'AQSSI*

3.2.1. Rédaction de documents de référence de la politique SSI

Les orientations de la sécurité sont définit dans le cadre du schéma directeur des systèmes d'informatique et de communication (SDSIC). L'AQSSI définit le plan d'actions associées.

Pour garantir la sécurité au sein du ministère, il fait rédiger :

- les directives (plans de sécurité, notes SSI) définissant la politique SSI ;
- le référentiel SSI pour définir les objectifs et les règles à mettre en œuvre. Ce document est régulièrement mis à jour pour prendre en compte les évolutions techniques et les nouvelles missions du ministère.

3.2.2. Définition des éléments sensibles

Il définit les éléments sensibles de l'infrastructure nationale et le niveau de sécurité de chacun des éléments qui la constitue.

3.2.3. Mise en place de la cellule alerte nationale

L'AQSSI met en œuvre les moyens et l'organisation nécessaire afin que la cellule alerte nationale puisse être opérationnelle aux heures ouvrables et mobilisable, si nécessaire, 24 h sur 24 h (ex : dans le cadre de crise ou de plans sécurité de type Vigipirate.) Il formalise son fonctionnement et son interaction avec les différents partenaires (points d'appui,

centres serveurs, services, HFD et lui-même).

3.2.4. Application des règles du référentiel SSI

L'AQSSI fait appliquer par les directeurs d'administrations centrales et les chefs de services les règles SSI définies dans le référentiel SSI.

3.2.5. Application des plans de sécurité

En liaison avec le service du HFD, l'AQSSI doit décliner pour l'infrastructure nationale et les services les mesures des plans de sécurité (Vigipirate et Piranet entre autres).

A chaque niveau d'alerte devra correspondre une procédure adaptée et les actions à conduire notamment auprès des opérateurs.

L'organisation à mettre en place en cas de crise doit être consignée et portée à la connaissance des acteurs mobilisables.

L'AQSSI fait appliquer par les directeurs d'administrations centrales et les chefs de services les mesures SSI correspondantes.

3.2.6. Contrôle et suivi

L'AQSSI s'appuie sur les représentants SSI régionaux pour faire le suivi de la SSI et sur DPSM/SI pour la gestion des dérogations spécifiques.

Il demande aux services une copie du rapport d'activité sur la SSI avec tableau de bord des actions et liste des dérogations transmis annuellement au HFD.

Il peut demander l'audit des éléments d'infrastructures nationales auprès d'un organisme externe ou du bureau audit de la direction centrale de la sécurité des systèmes d'information (DCSSI).

3.2.7. Formation et sensibilisation à la SSI

L'AQSSI devra organiser les actions de formation nécessaires pour que les acteurs nationaux et les représentant régionaux SSI connaissent la politique nationale, les enjeux, les menaces et les règles de sécurité définies au sein du ministère. Des formations au centre de formation de la direction centrale de la sécurité des systèmes d'information pourront être demandées auprès du HFD/FSSI.

Il veillera à ce que la sécurité soit intégrée dans les formations initiales des informaticiens.

3.3. *Au niveau des directions d'administration centrale*

3.3.1. Nomination du responsable SSI

Le directeur d'administration centrale nomme un représentant SSI qui sera le relais de l'AQSSI. Ses missions sont formalisées lors de sa nomination.

3.3.2. Déclinaison de la politique de sécurité

La politique de sécurité particulière des applications et systèmes d'information dont la direction a la charge doit préciser :

- l'organisation de la sécurité mise en œuvre au sein de la direction ;
- le niveau de sécurité nécessaire fonction de la sensibilité des données d'une application ;
- les aspects sécurité à prendre en compte dans l'ensemble du cycle de vie des projets informatiques métiers qu'elles gèrent (étude d'opportunité, étude de faisabilité, conception générale, conception détaillée... jusqu'à la mise au rebut).

Ce document sera porté à la connaissance des personnes ayant besoin d'en connaître (maîtres d'ouvrage et maîtrises d'œuvre d'application, etc).

3.3.3. Définition des applications sensibles

Le directeur d'administration centrale fait établir par ses services chargés de la maîtrise d'ouvrage d'applications la liste des applications sensibles qu'ils gèrent et les mesures de sécurité à mettre en œuvre aux différents niveaux, en particulier dans les services utilisateurs, pour garantir la confidentialité, l'intégrité et la disponibilité des données de ces applications.

3.3.4. Application des règles du référentiel SSI

Le directeur d'administration centrale fait appliquer, pour les systèmes d'informations métiers qu'il produit, les règles de sécurité définies dans le référentiel SSI.

3.3.5. Protection des informations

Le directeur d'administration centrale prend les dispositions nécessaires pour protéger les données des applications métiers contre leur divulgation et contre leur altération (ou perte totale).

3.3.6. Contrôle et suivi

Le directeur d'administration centrale doit définir l'organisation permettant de suivre les développements et les modifications de code qui doivent donner lieu avant la mise en exploitation de chaque application à l'exécution de procédures de recettes unitaires, d'intégration et de qualification (respect des procédures ACAI).

Il peut faire réaliser un audit sur le système d'information de son domaine de compétences.

3.3.7. Formation et sensibilisation

Le directeur d'administration centrale devra veiller à ce que les maîtrises d'ouvrage et d'œuvre ainsi que les équipes de développement (interne ou externe au ministère) aient les compétences nécessaires pour assurer leur mission dans le cadre de la sécurité. Des actions de sensibilisations régulières devront être organisées et des formations seront à engager si nécessaire.

3.4. *Au niveau des représentants SSI régionaux*

3.4.1. Diffusion des documents de référence de la politique SSI

Les représentants SSI régionaux diffusent, pour le compte de l'AQSSI, les directives instructions (plans de sécurité, notes SSI) définissant la politique SSI ainsi que le référentiel SSI.

3.4.2. Contrôle et suivi

Les représentant régionaux SSI réalisent le suivi et le contrôle de la mise en œuvre de la politique de sécurité nationale pour le compte de l'AQSSI. Pour cela, ils doivent disposer d'une visibilité sur l'évolution de la sécurité dans les services. Ils doivent avoir accès à toutes les productions du service (volet sécurité du service, le suivi des anomalies/incidents, le tableau de bord des actions engagées, la liste des dérogations, etc.), les actions de sensibilisations et formations engagées.

Des visites sur sites seront organisées régulièrement avec compte rendu de visite à l'AQSSI.

3.4.3. Formation et sensibilisation à la SSI

Les représentant régionaux SSI assurent, pour le compte de l'AQSSI, l'animation auprès des services (organisation de formations et information).

3.5. *Au niveau des délégués ministériels de défense*

3.5.1. Diffusion des informations liées aux plans de sécurité

Les délégués ministériels de défense notifient, pour le compte du HFD, les instructions concernant le niveau et les actions à engager dans le cadre des plans de sécurité (Vigipirate et Piranet entre autre) vers le responsable SSI local en tenant informé l'AQSSI et les représentants régionaux SSI.

3.5.2. Contrôle et suivi

Les délégués ministériels de défense vérifient l'application des dispositions relatives à la sécurité de défense, à la protection du secret et à la sécurité des systèmes d'information dans les services.

3.6. *Au niveau des chefs de service*

3.6.1. Nomination du responsable SSI

Le chef de service nomme un responsable SSI. Ses missions sont formalisées lors de sa nomination.

3.6.2. Auto-évaluation du niveau de sécurité

Chaque service devra définir par une auto-évaluation son niveau de sécurité. Il réalisera cette auto-évaluation à partir du guide d'évaluation du référentiel sécurité. Il résultera de cette évaluation la définition des objectifs à atteindre par le service et un tableau de bord des actions à conduire en interne.

Le schéma de principe est le suivant :

3.6.3. Réalisation d'un plan SSI

Ce document, qui pourra être le volet sécurité d'un plan d'informatisation, doit décliner localement la politique nationale par rapport aux contraintes et à l'infrastructure du service. Il doit définir :

- l'organisation de la sécurité mise en œuvre au sein du service ;
- les objectifs à atteindre ;
- le plan d'action des mesures à conduire.

3.6.4. Définition des éléments sensibles

Le chef de service fait définir par son responsable SSI les éléments sensibles de l'infrastructure locale et le niveau de sécurité de chacun des éléments qui la constitue.

3.6.5. Application du plan SSI

Le chef de service fait appliquer au sein de son service le plan SSI. Pour cela, ce document est porté à la connaissance des personnes ayant besoin d'en connaître (secrétariat général notamment le support informatique, agents pour la partie organisation, etc.).

3.6.6. Application des plans de sécurité

Le chef de service doit décliner pour l'infrastructure locale les mesures des plans sécurité (Vigipirate et Piranet entre autre). A chaque niveau d'alerte devront correspondre une procédure adaptée et les actions à conduire.

L'organisation à mettre en place en cas de crise doit être consignée et portée à la connaissance des acteurs mobilisables.

3.6.7. Mise en place du point d'alerte local

Le chef de service met en œuvre les moyens et l'organisation nécessaire afin que le point d'alerte locale puisse être opérationnel aux heures ouvrables et mobilisable, si nécessaire, 24 h sur 24 h (ex : dans le cadre de crise ou de Vigipirate.) Il formalise son fonctionnement et son interaction avec les différents partenaires (agents, experts locaux et cellule d'alerte nationale) en précisant en particulier le numéro de téléphone, l'adresse mail et le numéro de fax.

3.6.8. Protection des informations

Le chef de service doit prendre les dispositions nécessaire pour protéger les informations :

- contre leur divulgation, notamment les informations sensibles (données métiers, documents contractuels, données du personnel) ;
- contre leur altération (ou leur perte totale) en particulier les données administratives, comptables, métiers (en pratique, nécessité des recommandations des DAC).

3.6.9. Formation et sensibilisation

La sensibilisation vise à faire prendre conscience à chaque agent qu'il détient une part importante de responsabilité dans la lutte contre la malveillance. Aussi, chaque service doit mener régulièrement des programmes de sensibilisation. Ils devront porter sur :

- les enjeux de la sécurité ;
- les principales menaces ;
- les lois, règlements, chartes (utilisateurs, messagerie) ;
- l'organisation de la sécurité au niveau local ;
- les comportements à adopter notamment face à un incident ;
- les règles spécifiques (sur les accès physiques, les nomades, le mot de passe, la protection juridique des informations,...).

Ces actions devront, dans la mesure du possible, être adaptées aux différents niveaux de responsabilité détenus et aux spécificités des postes de travail.

Une charte utilisateur de l'usage de l'informatique doit être diffusée à l'ensemble du personnel.

Le chef de service devra veiller à ce que son personnel technique est les compétences nécessaires pour assurer leur mission dans le cadre de la sécurité et à ce titre les amener à se former.

3.6.10. Applications de maîtrise d'ouvrage locale

Le chef de service fait établir par ses maîtrises d'ouvrages locale la liste des applications sensibles qu'ils gèrent et les mesures de sécurité à mettre en œuvre aux différents niveaux, en particulier au niveau des utilisateurs, pour garantir la confidentialité, l'intégrité et la disponibilité des données de ces applications.

Il prend les dispositions nécessaires pour protéger les données des applications de maîtrise d'ouvrage locale contre leur divulgation et contre leur altération (ou perte totale).

3.6.11. Contrôle et suivi

Chaque chef de service doit s'assurer que le tableau de bord des actions à réaliser est réactualisé régulièrement en fonction de la mise en œuvre des mesures de sécurité. Concernant les contrôles, il devra s'assurer :

- du respect des règles de sécurité au sein de son service et par les tiers (externalisation de service, infogérance) ;
- de la présence de clauses contractuelles de sécurité dans l'ensemble des contrats de fournisseurs, dans le cadre d'une sous-traitance ;

- de l'existence d'une autorisation explicite du ministère et d'une convention pour le raccordement d'un partenaire local au réseau de son service ;
- du contrôle de l'exploitation régulière des traces ;
- de la gestion des dérogations ;
- du bon fonctionnement du point d'alerte.

3.7. *Au niveau des responsables d'unité*

Ils doivent, lors des contrôles hiérarchiques, aborder l'aspect sécurité, entre autres s'assurer :
- de la bonne application des règles de gestion des accès et des habilitations ;
- du bon respect des lois, règlements et de la charte utilisateur.

4. **Gestion des incidents**

4.1. *Définition*

Un incident de sécurité est un accident, une panne ou un non-respect (intentionnel ou non) d'une procédure de sécurité. La gestion des incidents de sécurité conditionne la capacité à réagir efficacement à tout événement de nature catastrophique ou récurrente.

La finalité d'un réseau d'alerte est de provoquer une intervention aussi rapide que possible, dès qu'un incident ou une faille de sécurité est détecté, limitant ainsi les conséquences d'une dégradation ou d'un arrêt du système d'information.

4.2. *La cellule d'alerte nationale*

4.2.1. Rôles

Toutes les alertes (incident ou faille de sécurité) convergent vers la cellule d'alerte nationale. Cette structure reçoit :
- les alertes externes au ministère en provenance de l'interministériel, en particulier du Certa (cf. note 24) , ou des éditeurs de logiciel ;
- les alertes en provenance des services.

Cette cellule assure le suivi de toutes les alertes sécurité. Elle joue le rôle d'interface avec les points d'appuis concernés par une alerte et les différents acteurs qui ont besoin d'en être informés (HFD, AQSSI, centres serveurs, services).

Elle constitue, par les actions qu'elle peut engager, le bras « opérationnel » de l'AQSSI du ministère.

4.2.2. Fonctionnement

Elle demande l'évaluation de l'alerte par les points d'appui pour avis et proposition d'actions. Elle sollicite l'AQSSI pour validation des propositions d'actions ou met en œuvre les propositions dans le cas de délégation. Elle informe les acteurs (centres serveurs, opérateur et éventuellement les cellules d'alertes locales) pour traitement des actions à mettre en œuvre.

Elle publie les informations et fournit un suivi des incidents et alertes qu'elle transmet à l'AQSSI.

4.3. *Le point d'alerte local*

4.3.1. Rôle

Au niveau du service, toutes les alertes (incident ou faille de sécurité) convergent vers le point d'alerte local. Cette structure reçoit :
- les alertes externes au service en provenance de la cellule d'alerte nationale ;
- les alertes en provenance des agents.

Cette structure assure le suivi de toutes les alertes de sécurité locale. Elle résoud les problèmes qu'elle peut à son niveau. Elle transmet, si nécessaire, à la cellule alerte nationale les alertes préalablement analyser et qualifier.

Elle réalise un suivi des anomalies/incidents qu'elle transmet régulièrement au responsable SSI du service. Elle constitue par les actions qu'elle peut engager le bras « opérationnel » du responsable SSI.

4.3.2. Fonctionnement

Pour les alertes externes, ce point d'alerte aura en charge la rediffusion des alertes émanant de la cellule nationale vers les intéressés locaux (cellules informatiques, agents, hiérarchie).

Concernant les alertes internes au service, la cellule d'alerte local est directement contacté par l'agent qui constate un problème ou une anomalie sur son poste de travail. Les experts locaux jugent de la gravité de l'incident et le qualifie. Le suivi des alertes est fournit régulièrement au responsable SSI.

Dans le cas où l'incident peut avoir des répercutions sur le bon fonctionnement du système d'information national (par exemple alertes de sécurité de type virus ou coupure du réseau), il transmet l'information à la cellule d'alerte nationale après validation du représentant SSI. Il la tient informée jusqu'à la reprise normale de l'activité.

4.4. *Traitement d'un incident*

4.4.1. Schéma d'organisation

4.4.2. Pour le niveau national

Dès qu'une alerte, externe ou interne au ministère, peut avoir des répercussions sur le ministère, la cellule d'alerte nationale fait intervenir le ou les points d'appui correspondants pour expertises. Suivant les conclusions, et après avis de l'AQSSI, elle diffuse une information aux personnes ayant besoin d'en connaître et prend les décisions correctives qui s'imposent (elle peut notamment décider de couper des liaisons réseau pour isoler un service d'une invasion virale).

Lorsque la cellule d'alerte nationale reçoit un message d'incident du point d'alerte local, elle en informe si nécessaire l'AQSSI. Si l'incident est grave, elle en informera le HFD qui demandera éventuellement l'intervention du Certa (cf. note 25) .

4.4.3. Pour le niveau local

Dans le cas où un incident local peut avoir des répercussions sur le bon fonctionnement du système d'information national (par exemple, alertes de sécurité de type virus ou coupure du réseau), le point d'alerte local transmet l'information à la cellule d'alerte nationale. Il la tient informée jusqu'à la reprise normale de l'activité.

5. **Gestion des dérogations**

5.1. *Définition d'une dérogation*

Le référentiel est un ensemble de règles généralement applicables à tous les services. Dans certains cas particuliers, certaines ne sont pas adaptées et des dérogations peuvent être accordées.

L'ensemble des règles non conformes au référentiel SSI seront regroupées sous le terme générique de « dérogations ». On distingue deux types de dérogations :

- les dérogations génériques qui sont accordées pour tous les services dont la décision d'application est sous la responsabilité du RSSI local ;
- les dérogations spécifiques qui font l'objet d'une demande d'autorisation auprès de l'AQSSI du ministère.

L'AQSSI définit les règles de niveau local et celles qui doivent faire l'objet d'une dérogation spécifique.

5.2. *Les dérogations génériques*

Ces dérogations doivent être proposées par la cellule informatique au responsable SSI du service pour validation en précisant le cadre d'application. Dès acceptation par celui-ci, elles seront enregistrées localement dans un registre spécifique.

Chaque année, la cellule informatique devra analyser avec son responsable SSI l'opportunité de maintenir ces dérogations.

Cette liste de dérogations pourra être fournie sur demande à la structure de contrôle qui en ferait la demande.

5.3. *Les dérogations spécifiques*

Sont considérées comme dérogations spécifiques les dérogations ne répondant pas à la notion de dérogations génériques.

Pour obtenir cette dérogation, le service doit transmettre au DPSM/SI2 un dossier technique comprenant les informations suivantes :

- le contexte ;
- la justification de la demande en mentionnant le besoin ;
- les éléments techniques (avec schéma détaillé du réseau si nécessaire) ;
- les mesures de sécurité mises en œuvre ;
- toutes les informations qu'il jugera nécessaires.

Le bureau DPSM/SI2 donne son accord si la demande est justifiée. Cet accord sera donné pour une durée déterminée permettant au service de se mettre à niveau. La dérogation pourra être renouvelée pour une durée déterminée.

Des mesures de sécurité spécifiques pourront être demandées au service sollicitant la demande. Elles seront déclarées annuellement au FSSI dans le cadre du rapport annuel sur la sécurité des systèmes d'information.

Le DPSM/SI2 pourra, le cas échéant, réévaluer la demande de dérogation lorsque la technologie offre de nouvelles solutions.

6. **Les règles**

Ce chapitre récapitule les points les plus importants du document qui peuvent servir de tableau de bord de la SSI sur le volet organisationnel.

6.1. *Acteurs et responsabilités*

RÈGLE	PRIORITÉ	APPLICABLE pour	DESCRIPTIF

		les acteurs	
S01.01	I	HFD, AQSSI, DAC, chef de service	Définir et mettre en place l'organisation gérant la sécurité des SI.

6.2. *Mise en place de la SSI*

RÈGLE	PRIORITÉ	APPLICABLE pour les acteurs	DESCRIPTIF
S02.01	I	DAC, maîtrise d'ouvrage locale	Décliner la politique nationale pour les applications et les systèmes d'information métier dont vous êtes responsables
S02.02	I	Chef de service	Mettre en application au niveau local la politique SSI du ministère et l'adapter aux contraintes du service
S02.03	I	AQSSI, DAC, chef de service	Classer et protéger les éléments des systèmes d'information en fonction de leur sensibilité
S02.04	I	AQSSI, DAC, chef de service	Mettre en place l'organisation nécessaire pour gérer les anomalies, les incidents et les alertes
S02.05	I	HFD, AQSSI, DAC, chef de service, chef d'unité	Sensibiliser, former et informer le personnel à la sécurité des SI
S02.06	I	DAC, chef de service	Prendre les dispositions nécessaires pour protéger les informations/données
S02.07	I	AQSSI, DAC, chef de service	Décliner suivant l'infrastructure les plans de sécurité (Vipirate et Piranet en autre)

6.3. *Suivi et contrôle de la SSI*

RÈGLE	PRIORITÉ	APPLICABLE pour les acteurs	DESCRIPTIF
S03.01	I	Chef de service	L'évaluation de la sécurité de ses systèmes d'information et le suivi de la mise en œuvre des actions de sécurité correspondantes doivent être réalisés régulièrement (tableau de bord)
S03.02		HDF, DAC, chef de service, chef d'unité	Contrôler l'application des dispositifs relatifs à la sécurité

6.4. *Gestion des incidents*

RÈGLE	PRIORITÉ	APPLICABLE pour les acteurs	DESCRIPTIF
S04.01	I	Chef de service	Une procédure d'alerte en cas d'incident doit être mise en place et portée à connaissance du personnel. En cas d'incident, l'utilisateur doit savoir que faire et le faire savoir
S04.02	I	AQSSI, DAC, chef de service	Un plan de secours doit être défini et activé si nécessaire (définition, mise en œuvre, validation, contrôle)

6.5. *Gestion des dérogations*

RÈGLE	PRIORITÉ	APPLICABLE pour les acteurs	DESCRIPTIF
S05.01	I	DAC, chef de service	Tout non-respect d'une règle du référentiel sécurité doit faire l'objet d'une dérogation
S05.02	I	Chef de service	Les dérogations n'impactant que le service doivent être gérées localement (dérogation générique)
		DAC, chef de service,	Les dérogations touchant aux infrastructures nationales doivent faire l'objet

S05.03	I	responsable SSI	d'une demande de dérogation nationale

Liste des règles primordiales

Le référentiel est applicable dès à présent. Dans certains cas, sa mise en œuvre peut nécessiter un certain temps. Il devra être appliquer intégralement au 1er janvier 2007 ; exceptée pour les règles primordiales qui doivent être appliquées avant le 1er juillet 2005.

La liste de ces règles est donnée ci-dessous. Elles sont regroupées par domaine.

Organisation

LIBELLÉ DE LA RÈGLE	NUMÉRO règle
Toutes les règles présentes dans le référentiel prédominent sur les règles antérieures	S00.01
Tout ce qui n'est pas explicitement autorisé est interdit	S00.02
L'ensemble des règles présentes dans le référentiel s'applique à toutes les entités du ministère y compris les services hébergés	S00.04
Chaque service doit se protéger conformément aux spécifications du ministère	S00.03
Tout non-respect d'une règle du référentiel de sécurité doit faire l'objet d'une dérogation	S05.01
Les dérogations touchant aux infrastructures nationales doivent faire l'objet d'une demande de dérogation nationale	S05.03
Chaque utilisateur doit appliquer les dispositions réglementaires et mettre en application les règles qui le concernent	S00.05
Chaque acteur de la sécurité, doit définir et mettre en place l'organisation gérant la sécurité des systèmes d'information	S01.01
Chaque direction d'administration centrale et maîtrise d'ouvrage locale doivent décliner la politique nationale pour les applications et systèmes d'information dont ils sont responsables	S02.01
Chaque service doit mettre en application au niveau local la politique SSI du ministère et l'adapter aux contraintes du service	S02.02
Chaque acteur de la sécurité doit classer et protéger les éléments des systèmes d'information en fonction de leur sensibilité	S02.03
Chaque acteur de la sécurité doit mettre en place l'organisation nécessaire pour gérer les anomalies, les incidents et les alertes	S02.04
Chaque acteur de la sécurité doit définir et mettre en œuvre une procédure d'alerte en cas d'incident qui sera portée à la connaissance du personnel	S04.01
Chaque acteur de la sécurité doit sensibiliser, informer et former le personnel à la sécurité des systèmes d'information	S02.05
Les DAC et chef de service doivent prendre les dispositions nécessaires pour protéger les informations/données	S02.06
Chaque acteur de la sécurité doit décliner suivant l'infrastructure les plans de sécurité (Vigipirate et Piranet en autre)	S02.07
Chaque service doit évaluer son niveau de sécurité et faire le suivi de la mise en œuvre des actions correspondantes	S03.01
Chaque acteur de la sécurité doit contrôler l'application des dispositifs relatifs à la sécurité	S03.02
(1) Les acteurs de la sécurité sont : les chefs de services, les DAC, l'AQSSI.	

Réseau

LIBELLÉ DE LA RÈGLE	NUMÉRO
Le service doit désigner un responsable I-carré	S11.11
Le service doit désigner un responsable du réseau du service et des sites distants	S11.21
Seul le réseau d'interconnexion IP est autorisé pour véhiculer les données entre les services du ministère	S12.1
Le service est tenu de respecter le plan d'adressage qui lui est alloué	S13.11
Tout flux entre deux services du ministère ne doit pas être translaté	S13.14
L'utilisation du réseau du service est obligatoire (aucun réseau privé n'est autorisé)	S13.15

Les adresses IP faisant partie du plan d'adressage du ministère ne doivent pas être attribuées à un partenaire	S13.17
La liaison avec les sites distants doit être sécurisée	S14.21
Les connexions externes sont soumises à une déclaration et doivent être centralisées au siège	S14.22
S'il existe un réseau externe au sein du site distant, un poste ne peut être connecté physiquement qu'à un seul réseau, soit au réseau externe, soit au réseau du service	S14.23
Les protocoles de routage dynamique (RIP ou autres) sont absolument interdits	S14.24
Aucune connexion directe entre un service du ministère et un partenaire national ou une autre administration n'est autorisée	S14.41
Le service doit s'assurer que le partenaire local au ministère n'ait pas la possibilité d'atteindre directement ou indirectement le réseau I-carré	S14.52
Tout accès direct ou indirect, au réseau Internet est interdit, en dehors de celui offert par I-carré	S14.61
Toute autre interconnexion de réseau non prévue dans le référentiel est interdite	S14.71
Les modifications de configuration doivent être tracées	S17.23

Autocom

LIBELLÉ DE LA RÈGLE	NUMÉRO
L'administration distante doit être limitée tant que possible. Si cela est nécessaire, imposer des conditions drastiques de sécurité aux prestataires	S21.41
La fonction DISA permettant d'accéder aux services d'administration du PABX depuis l'extérieur doit être désactivée	S22.23

Serveurs

LIBELLÉ DE LA RÈGLE	NUMÉRO
Le service doit identifier et nommer les administrateurs du serveur et les opérateurs délégués - limiter le nombre d'administrateurs	S31.10
Un compte administrateur n'est utilisé que pour l'administration du serveur	S31.12
Les comptes administrateur doivent être sécurisés	S31.13
Les conditions générales d'administration de chaque serveur (administration locale, administration nationale) doivent être précisés	S31.14
Les conditions particulières d'administration à distance de chaque serveur en interne doivent être précisés	S31.15
Les conditions particulières d'administration à distance de chaque serveur par un tiers extérieur doivent être précisés. La maintenance ou la prise de contrôle à distance d'un serveur par un tiers extérieur au ministère doit être déclarée	S31.16
Chaque compte utilisateur doit être identifié et la pertinence du compte doit être vérifiée régulièrement	S31.32
L'authentifiant (identifiant et mot de passe) de l'utilisateur doit être strictement personnel et le mot de passe ne doit pas être communiqué, y compris à un administrateur, un utilisateur ne doit pas utiliser l'authentification d'un autre utilisateur	S31.33
Le serveur ne doit pas être utilisé comme poste de travail	S32.11
Les partitions sécurisées (NTFS et non FAT) doivent être utiliser	S32.31
Un seul système doit être installé sur le serveur (pas de multiboot)	S32.40
La configuration des serveurs à administration nationale ne doit pas être modifiée	S32.42
Le serveur doit être protégé contre les virus	S32.43
Les services réseau inutilisés sur les serveurs doivent être désactivés	S33.12
Les protocoles de communication inutilisés sur les serveurs doivent être désactivés	S33.21
La session en fin d'administration doit être fermée	S34.12
Une politique de sauvegarde doit être définie	S35.10
Une politique de droit d'accès des utilisateurs doit être défini	S36.13
Une politique de surveillance des serveurs SOMA doit être définie	S36.14
Les droits d'accès des personnes qui consultent les sites (internautes) doivent être définis	S36.33

Postes de travail

LIBELLÉ DE LA RÈGLE	NUMÉRO
L'utilisateur est responsable de son poste de travail	S41.12
L'utilisateur est responsable de l'application des règles de sécurité de son poste	S41.13
L'utilisateur est responsable de la sécurité des données qu'il copie ou diffuse hors de son poste (disquette, sauvegarde, poste nomade, sortie papier, courriel, etc.)	S41.14
L'utilisateur doit connaître les règlements intérieurs et extérieurs et les appliquer	S41.15
L'utilisateur doit faire remonter les incidents constatés	S41.16
Les fichiers nominatifs doivent être déclarer à la CNIL (Commission nationale informatique et libertés)	S41.17
La politique de mot de passe doit être appliquée	S41.18
Tout poste de travail doit être protégé contre les virus, notamment les nomades lorsqu'ils sont hors réseau du service	S42.22
Les accès à des réseaux externes doivent passer par le réseau local du service (pas de modem)	S42.31
Le poste nomade doit être scanné par un antivirus à jour avant l'ouverture de session sur le réseau	S42.33
Tout matériel n'appartenant pas au service et se connectant à un poste ou réseau du service doit faire l'objet d'une autorisation préalable du RSSI et de l'administrateur (ex : portable, assistant personnel, matériel utilisé par un partenaire extérieur)	S42.35
Le partage de ressource est interdit sur le poste de travail	S43.02
Les données doivent être sauvegarder régulièrement en respectant la politique de sécurité définie par le service	S43.03
La télémaintenance de postes de travail par un tiers extérieur doit être limitée et sécurisée	S43.08
Une politique de sauvegarde doit être définit et appliquée	S43.10
Le navigateur doit utiliser un serveur mandataire pour les accès vers Internet	S44.10

Accès physique

LIBELLÉ DE LA RÈGLE	NUMÉRO
La localisation du matériel doit être adaptée à leur degré de sensibilité	S51.11
La fourniture et la qualité des énergies requises doivent être assurées	S51.23
La continuité de l'alimentation électrique pour les matériels le nécessitant doit être assurée	S51.24
Les bureaux sensibles doivent être soumis à un contrôle d'accès	S51.27
Les mesures contre le vol des postes doivent être définies et appliquées	S53.12

Messagerie

LIBELLÉ DE LA RÈGLE	NUMÉRO
L'architecture nationale de la messagerie définit l'ensemble des serveurs à installer. L'installation de serveur indépendant est interdit	S711.13
La configuration du serveur hébergeant la messagerie doit être relevée	S712.10
Aucune modification du paramétrage ou adjonction de logiciels sur le serveur de messagerie ne doit être faite	S712.25
Un plan de secours (boîte aux lettres de secours) doit être défini	S712.31
La directive nationale de l'utilisation de la messagerie dans le ministère doit être respectée	S713.02
Le client de messagerie doit être configuré pour éviter toute action automatique de lecture ou ouverture de messages et fichiers attachés	S713.03
L'envoi de messages à plus de 300 destinataires extérieurs au service est interdit	S713.11
La boîte aux lettres d'unité doit permettre la continuité de service, elle doit être relevée au moins une fois par jour	S713.15
Les pourriels (spams) ne doivent pas être rediffusés	S713.17

NOTE (S) :

(1) Confidentialité : cela consiste à tenir secrètes des informations avec accès aux seules personnes autorisées.

(2) Intégrité : garantie que l'information ne peut être modifiée que par les personnes ayant droit et de façon volontaire.

(3) Disponibilité : garantie que les données sont accessibles par ceux qui en ont besoin à chaque fois que nécessaire.

(4) Non répudiation (preuve) : permet de relier chaque action sur le système d'information à un utilisateur ou à un composant du système d'information.

(5) http ://www.certa.ssi.gouv.fr/

(6) Nous distinguons en fait plusieurs types et niveaux d'utilisateurs : le maître d'ouvrage décide, définit les exigences, paye et prend la responsabilité des opérations ; le gestionnaire ou exploitant a la responsabilité des affaires courantes du système d'information au jour le jour, il est responsable des opérations et du rapport des résultats, il ne peut travailler que si le propriétaire lui précise des objectifs et s'il fournit des moyens, il n'est pas toujours l'administrateur, qui peut dépendre de lui pour des sous-objectifs précis et spécifiques, mais se trouve à ce niveau ; l'utilisateur qui emploie le système d'information en suivant des règles et des procédures définies par le ministère ou le propriétaire ; l'opérateur est un utilisateur spécifique dont la compétence permet une utilisation « professionnelle » d'un outil.

(7) La mise en place du réseau interministériel Ader a conduit à la rédaction de référentiels de sécurité et d'exploitation applicables à tous les agents et équipements raccordés directement ou indirectement à ce réseau. A ce jour, les référentiels suivants ont été rédigés et sont en cours de validation : le référentiel de nommage pour les adresses internet utilisées au sein de l'administration française (noms de domaine, adresses de messagerie, serveurs d'application) ; le référentiel technique de l'annuaire inter-administrations définissant les informations enregistrées dans cet annuaire et les modalités de son alimentation ; le profil de messagerie inter-administrations définissant les conditions des échanges entre les ministères et les fonctions à assurer par leurs serveurs de messagerie ; le référentiel de qualité de service visant à garantir la qualité de bout en bout des échanges interministériels ; le référentiel sécurité IP précisant les règles de sécurité à respecter par les entités raccordées directement ou indirectement au réseau Ader.

(8) http ://www.ssi.gouv.fr/fr/reglementation/901/index.html.

(9) http ://www.ssi.gouv.fr/fr/reglementation/600/index.html.

(10) Code de la propriété intellectuelle, article L. 621 relatif au secret de fabrique.

(11) Recommandation du Conseil de l'Europe du 19 septembre 1989 adoptée par le conseil des ministres, relative à la criminalité en relation avec l'ordinateur.

(12) Directive n° 91/250/CEE du Conseil des communautés européenne du 14 mai 1991 concernant la protection des programmes d'ordinateur.

(13) http ://www.un.org/french/aboutun/dudh.htm.

(14) http ://www.unhchr.ch/french/html/menu3/b/71_fr.htm.

(15) http ://www1.oecd.org/publications/e-book/9302012E.PDF.

(16) http ://www1.oecd.org/publications/e-book/9302012E.PDF.

(17) http ://www1.oecd.org/publications/e-book/9302012E.PDF.

(18) http ://www.legifrance.gouv.fr/texteconsolide/PPEAU.htm.

(19) http ://www.cnil.fr/thematic/docs/entrep/cybersurveillance2.pdf.

(20) http ://europa.eu.int/ISPO/legal/fr/dataprot/directiv/direct.html.

(21) http ://europa.eu.int/ISPO/legal/fr/dataprot/directiv/direct.html.

(22) Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, relative au cadre communautaire pour les signatures électroniques.

(23) http ://www.ssi.gouv.fr/fr/reglementation/901/index.html.

(24) Certa : Centre d’expertise gouvernemental de réponse et de traitement des attaques informatiques.

(25) Certa : Centre d’expertise gouvernemental de réponse et de traitement des attaques informatiques.