Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'AGRICULTURE
DE L'AGROALIMENTAIRE
ET DE LA FORÊT

Cabinet **Mission défense** **78, rue de Varenne 75349 PARIS 07 SP** **0149554955** **Secrétariat général** **Service de la modernisation** **Sous-direction des systèmes d'information**	**Instruction technique** **CAB/MD/2015-586** **09/07/2015**

Date de mise en application : Immédiate
Diffusion : Tout public

Cette instruction n'abroge aucune instruction.
Cette instruction ne modifie aucune instruction.
Nombre d'annexes : 2

Objet : politique de sécurité des systèmes d'information de l'Agriculture (PSSI/A) approuvée par la Secrétaire Générale (SG) et par le Haut Fonctionnaire de Défense et de Sécurité (HFDS).

Destinataires d'exécution
DRAAF DAAF SECRETAIRE GENERALE DIRECTEURS GENERAUX ET DIRECTEURS D'ADMINISTRATION CENTRALE

Résumé : La politique de sécurité des systèmes d'information de l'Agriculture (PSSI/A) jointe est approuvée par la Secrétaire Générale (SG) et par le Haut Fonctionnaire de Défense et de Sécurité (HFDS). Sa mise en œuvre est confiée aux services du SG, en lien avec ceux du HFDS. Cette seconde version de la PSSI/A met à jour la formalisation, la stratégie, l'organisation et les exigences de sécurité appliquées dans l'ensemble des services du ministère pour protéger son patrimoine informationnel et son système d'information. À l'instar de la première version, cette politique continue de s'appliquer dans les établissements publics de l'enseignement agricole. Les établissements publics sous tutelle gérant les aides communautaires et les organismes payeurs doivent toutefois avoir mis en place et gérer leur propre politique de sécurité des systèmes d'information, compatibles avec la présente politique. Cette mise à jour vise la prise en compte les

nouveaux usages et cadres normatifs et cherche à améliorer la lisibilité de l'ensemble. Elle est complétée par une Charte informatique délimitant les droits et devoirs des utilisateurs du système d’information.

1. Contexte

La sécurité des systèmes d'information est une préoccupation ancienne pour l'ensemble du ministère, devenue prioritaire du fait de l'ouverture des systèmes aux usagers, au travers des téléservices obligeant ainsi à garantir un certain degré de confiance, ainsi que des cadres réglementaires européens et nationaux.

Les risques informatiques, les enjeux de la protection du patrimoine informationnel ainsi que les plans de prévention et de lutte contre le terrorisme, exigent de conserver la « posture permanente de sécurité », à laquelle la politique de sécurité des systèmes d'information/Agriculture (PSSI/A) contribue.

La PSSI/A publiée en 2007 (voir SG/SM/SDSI/MSSI/C2007-1402) faisait de la sécurité des systèmes d'information une préoccupation partagée par tous : maîtres d'ouvrage des systèmes d'information, maîtres d'œuvre internes et externes, responsables hiérarchiques et utilisateurs. La présente mise à jour de la PSSI/A pérennise cette dynamique collective tout en relevant le défi de la sécurité de l'information.

2. Démarche

La sous-direction des systèmes d'information (SDSI), en lien avec les services du haut-fonctionnaire de défense et de sécurité (HFDS) et les différentes directions du ministère, a effectué une mise à jour globale de la PSSI/A en tenant compte des modifications de structures en son sein et des réorganisations au niveau de l'État (création des directions départementales interministérielles (DDI) et de la direction interministérielle des systèmes d'information et de communication (DISIC), affirmation du rôle de l'agence nationale de la sécurité des systèmes d'information (ANSSI) relevant du secrétariat général pour la défense et la sécurité nationales (SGDSN), etc.).

Prenant en compte les observations émises au sujet de la première version du document, la PSSI/A a subi des corrections importantes et a bénéficié d'un effort de simplification. Le document s'adresse à tous les agents du ministère ainsi qu'à certains prestataires et usagers : il a donc été aussi question de rendre plus lisible les droits et obligations s'appliquant à chacun en adaptant la terminologie utilisée.

La mise à jour de la PSSI/A s'insère également dans un corpus documentaire toujours plus dense. Elle a notamment été alignée sur la récente PSSI de l'État (PSSI/E) ainsi qu'à la PSSI DDI/Préfectures (applicable sur le périmètre départemental, sous l'égide des services du Premier ministre). De même, elle suit les bonnes pratiques édictées par l'ANSSI dans son guide d'hygiène informatique et a intégré les règles du règlement général de sécurité (RGS) et donc de l'homologation de sécurité.

3. Présentation de la mise à jour de la politique de sécurité

Dans un but de clarté, la PSSI/A est désormais précédée par un guide de sept pages, reprenant les principales dispositions qui fondent ainsi un socle de bonnes pratiques que tout agent se doit de respecter. Cette amélioration de la lisibilité a été renforcée par sur la forme afin de rendre le document final autoporteur.

La PSSI/A formalise l'organisation de sécurité du ministère et les exigences qui vont être appliquées à l'ensemble des agents de celui-ci mais aussi des établissements publics d'enseignement agricole. Cette mise à jour va plus loin que l'essentielle sécurité des systèmes d'information, puisqu'elle vise à installer une véritable culture de sécurité de l'information au sein du ministère.

La PSSI/A est complétée par une Charte informatique, qui délimite de manière synthétique les droits et devoirs des utilisateurs du système d'information du ministère.

4. Modalités d'application

La PSSI/A est approuvée par le secrétariat général, lequel est également chargé de la coordination de sa mise en œuvre en lien avec le service du haut fonctionnaire de sécurité et de défense.

Son application au sein des services du ministère est immédiate. La secrétaire générale, les directeurs généraux d'administration centrale et les directeurs des services déconcentrés sont chargés de son application.

Son application aux établissements publics de l'enseignement agricole sera détaillée par une note de service conjointe de la direction générale de l'enseignement et de la recherche et du secrétariat général.

Les établissements publics sous tutelle qui gèrent les aides communautaires, organismes payeurs, doivent mettre en place et gérer leur propre politique de sécurité des systèmes d'information en

cohérence avec la PSSI/A sous le contrôle du secrétariat général et du service du Haut fonctionnaire de sécurité et de défense.

L'Adjoint au haut fonctionnaire de défense et de sécurité,

Thierry Coton

La secrétaire générale,

Valérie METRICH-HECQUET

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'AGRICULTURE
DE L'AGROALIMENTAIRE
ET DE LA FORÊT

POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

Document public – Confidentialité C0

définie et approuvée le 06 Juillet 2015 par le

Service du Haut-Fonctionnaire de Défense et de Sécurité

et le

Secrétariat Général

Guide des principales bonnes pratiques issues de la PSSI-Agriculture

Dans le respect de la politique de sécurité des systèmes d'information de l'État (PSSIE) dont elle constitue une déclinaison ministérielle, la PSSI-Agriculture met en place des règles de base permettant à chacun d'adopter un comportement minimal et obligatoire en matière de sécurité des systèmes d'information au sein du ministère chargé de l'agriculture. Afin de permettre une meilleure sensibilisation et transmission de ces bonnes pratiques, le Guide des bonnes pratiques ci-après reprend les dispositions les plus importantes de la PSSI-Agriculture. Il conviendra de noter que ce Guide n'est pas exhaustif et, qu'en dernier lieu, c'est la PSSI-Agriculture qui prime sur ses dispositions.

Lignes directrices de la PSSI-Agriculture

- Mettre en place une approche conforme à l'état de l'art, précise, systématique mais néanmoins pragmatique
- Accompagner les évolutions du SI et des organisations du ministère
- Mettre en place une organisation de sécurité transversale et homogène en s'appuyant sur un réseau de correspondants de proximité
- Ne pas délaisser les problématiques de sécurité physique
- Rendre homogène le niveau de sécurité entre l'administration centrale, les services déconcentrés et les établissements publics d'enseignement
- Accompagner le schéma directeur des SI en renforçant la fiabilité et la cohérence du SI
- Promouvoir une culture de la sécurité grâce à des bonnes pratiques accessibles par tous
- Accompagner le renforcement du niveau de protection des contractants, délégataires, vacataires et autres partenaires
- Généraliser les bonnes pratiques et promouvoir l'état de l'art en matière de sécurité
- S'appuyer sur une démarche en amont d'analyse de risques et en aval de maintien en conditions de sécurité adaptés aux besoins de sécurité des SI en termes de D, I, C, P.

Organisation de la sécurité de l'information

Le **Haut Fonctionnaire de Défense et de Sécurité** (HFDS) est responsable de l'application des dispositions relatives à la sécurité de la défense nationale. Il est notamment responsable de la cohérence globale de la PSSIA ainsi que de sa conformité avec la PSSIE.

Le HFDS est assisté par un **Fonctionnaire Sécurité des Systèmes d'Information** (FSSI).

Le **Sous-Directeur des Systèmes d'Information** (SDSI) est garant de la cohérence technique des dispositifs de protection pour l'ensemble des applications ainsi que de la cohérence des politiques de sécurité techniques des applications.

La **Mission Sécurité des Systèmes d'Information** (MSSI) assure la cohérence du niveau de protection sur l'ensemble du SI et représente le SDSI dans les instances où elle intervient.

Les **Autorités Qualifiées de Sécurité des Systèmes d'Information** (AQSSI) doivent veiller à la bonne application de la PSSI-Agriculture dans la structure (direction, service, établissement) à laquelle ils sont rattachés et, en tant que de besoin, définir des consignes et directives internes propres à leur structure, en cohérence avec la présente politique.

L'AQSSI pourra s'appuyer sur les **Agents chargés de la Sécurité des Systèmes d'Information** (ASSI, note de référence n° 375/HFDS/ED du 02/10/2009).

Le directeur ou chef de service en administration centrale, service déconcentré rattaché au ministère (DRAAF et DAAF), établissement public d'enseignement agricole est AQSSI pour sa direction, son service, son établissement.

Le service en charge de la sécurité opérationnelle, **(ancien DIP, pour Département de l'ingénierie de production)** doit respecter les besoins de sécurité formulés par les conclusions des études ISP et les prendre en compte dans ses procédures d'exploitation. Il est notamment en charge des modalités techniques d'application de la PSSI-Agriculture aux domaines transverses et est responsable de la configuration des équipements informatiques de sécurité du centre de production du ministère.

Les **Équipes de maîtrise d'œuvre**, internes ou externes au ministère, doivent appliquer les mesures de sécurité lors du développement des applications du ministère.

Le **Bureau du Pilotage des Systèmes d'Information** (BPSI) doit veiller à intégrer les aspects sécurité dans le schéma directeur des systèmes d'information et à leur prise en compte au plan organisationnel et au plan technique.

Le **Bureau des Méthodes, du Support et de la Qualité** (BMSQ) s'assure de la bonne mise en œuvre de la démarche qualité dans les projets.

Le **Conseil des Systèmes d'Information** (CSI) est saisi pour avis sur la mise en

œuvre des SI du ministère.

Les **Responsables informatiques de proximité** sont les relais directs ou indirects entre les utilisateurs et la SDSI sur les questions de sécurité des systèmes d'information. Au sein de l'administration centrale, ce relais est assuré par le **Bureau d'Informatique de Proximité** (BIP), qui intervient auprès des agents dans le cadre de l'assistance et du support informatique de proximité.

Tout **agent** du MAAF ainsi que tout utilisateur temporaire doit respecter les règles et principes de la présente PSSI-Agriculture.

Tout **utilisateur temporaire**, qu'il soit agent de la fonction publique, vacataire ou prestataire externe, doit respecter les exigences de la présente PSSI-Agriculture.

Recommandations plus spécifiquement destinées aux utilisateurs

Classification des informations

Toute information, qu'elle soit électronique ou non, doit disposer d'un responsable explicitement identifié, connu et appartenant à l'organisation du ministère.

Toute information ou document produit ou traité au sein du ministère doit faire apparaître de manière claire son niveau de confidentialité.

Pour les documents non classifiés de défense, l'échelle applicable est la suivante :

- C0 – Public : Informations réputées publiques, notamment celles publiées en ligne (que ce soit en intranet ou sur internet)
- C1 – Limitée : Informations non sensibles à diffusion interne et vers les usagers/partenaires concernés
- C2 – Personnel : Document contenant des informations nominatives couvertes par les dispositions *ad hoc* de la loi « Informatique et libertés » de 1978
- C3 – Confidentiel : Document comportant des informations sensibles mais non classifiées, à diffusion limitée à une liste fermée de destinataires ayant droit d'en connaître
- C4 – Stratégique : Document comportant des informations très sensibles mais non classifiées de défense, à diffusion strictement limitée à une liste fermée et contrôlée de destinataire ayant droit d'en connaître.

Un niveau de protection adapté doit être mis en œuvre en cohérence avec le niveau de confidentialité afférent à chaque information. Typiquement, les documents de niveau C4 doivent ainsi être chiffrés (stockage et communication).

Ressources humaines

Chaque agent prendra connaissance des exigences de sécurité le concernant à sa prise de fonction et veillera à les respecter.

Virus et codes malveillants

Les serveurs de fichiers et les postes de travail doivent être équipés d'un antivirus mis à jour régulièrement.

Un contrôle antivirus doit systématiquement être effectué sur les médias (CD-ROM, support USB, fichier téléchargé, etc.).

Usages déportés et consumérisation

Le recours à des équipements (tablette, téléphone personnel, …), logiciels (suite bureautique tierce, …) ou services externalisés (par exemple, de stockage et partage d'informations dans le nuage informatique) personnels est interdit, sauf dérogation explicite et documentée, accordée après avis conforme de l'équipe informatique de proximité compétente et transmise au RSSI ou à l'ASSI. La dérogation emporte exclusion de responsabilité de la part du ministère (y compris en cas d'intervention technique assurée par un agent de l'équipe informatique de proximité), mais souligne par contre la responsabilité de l'utilisateur en cas de problème avéré de sécurité. Dans cette situation, les règles de la PSSI-Agriculture continuent à s'appliquer (par exemple, l'obligation du traitement anti-viral ou du chiffrement des documents sensibles).

Sauvegardes

Chaque agent est responsable de la sécurité des documents qu'il est amené à gérer. Si les équipes techniques mettent à disposition des moyens destinés aux sauvegardes, il est de la responsabilité de chacun de veiller à l'utilisation effective de ceux-ci.

Échanges d'information

Les supports amovibles ou mobiles (supports USB, CD, DVD, disquettes, téléphones, tablettes, etc.) pourront servir de média d'échange sous conditions qu'ils respectent les mesures de protection adaptées au niveau de classification correspondant.

Il est interdit de laisser des informations sur des appareils d'impression (photocopieurs, imprimantes, télécopieurs, etc.) ; il faut les retirer dès que possible, au mieux à la fin de l'impression.

Identification et contrôle d'accès logique

Tout utilisateur des systèmes d'information du ministère doit disposer d'un identifiant unique.

Un mot de passe est considéré comme robuste dès lors qu'il remplit les conditions suivantes :

- Le mot de passe est composé de huit caractères choisis parmi au moins trois des quatre types de caractères (lettres majuscules, lettres minuscules, chiffres, caractères spéciaux).
- Le mot de passe est unique. Si un agent dispose de plusieurs comptes, un mot de passe différent doit être utilisé pour chacun d'eux.
- Le mot de passe est difficile à deviner et facile à retenir. Ainsi, il faut impérativement éviter la répétition de termes ou de caractères, les mots communs (par exemple du dictionnaire), les prénoms et noms de personnes (l'utilisateur, ses relations ou des personnalités connues) et les

informations personnelles (dates, numéros de carte bancaire, informations sensibles).

De nombreuses méthodes mnémotechniques existent pour parvenir sans peine à un tel résultat.

Sauf dérogation accordée par l'équipe informatique de proximité après avis conforme du RSSI ou de l'ASSI, l'utilisateur ne doit pas être administrateur de son poste de travail. Dans le cas exceptionnel où, pour des raisons techniques, ces privilèges s'avéreraient indispensables à l'exécution des missions d'un agent, ceux-ci doivent alors, dans toute la mesure du possible, être associés à un compte local au poste de travail habituel de l'utilisateur concerné, qui doit s'astreindre à utiliser son compte nominal (non privilégié) tant que le recours aux privilèges élevées n'est pas strictement indispensable.

L'utilisation des certificats, fortement encouragée, est à préférer à celle du couple « utilisateur/mot de passe ».

Tout accès aux informations de niveau C2 ou plus, qu'elles soient sur un support physique ou informatique, doit être protégé.

Les droits d'accès d'un utilisateur sont fondés sur le « besoin d'en connaître » lié à sa fonction.

Tout appareil mobile (téléphone, tablette, etc.) doit être sécurisé, lorsque c'est possible, par un verrouillage système (mot de passe ou schéma de déverrouillage) ainsi que par un code PIN. Les agents seront sensibilisés à l'importance de ce verrouillage.

Gestion des incidents

La survenance d'un événement anormal affectant l'un des composants du SI doit être déclarée par tout agent le constatant auprès de son responsable informatique de proximité ou le cas échéant (pour les incidents de sécurité) de l'AQSSI dont il dépend puis le remonter à la chaîne SSI via la MSSI ou le FSSI.

Chacun doit avoir en tête que signaler un incident constitue une obligation professionnelle et le meilleur moyen de faire en sorte qu'il soit relevé : les incidents dont les équipes techniques n'ont pas connaissance ne se relèvent pas tout seuls.

Recommandations plus spécifiquement destinées aux responsables de service

Ressources humaines

Chaque agent du service est sensibilisé à la cyberdéfense, aux consignes de sécurité propres au poste occupé, au nécessaire respect de la PSSIA, à l'obligation d'alerte en cas de risque, et aux règles de confidentialité et de sécurité relatives aux informations et aux documents gérés.

Tout agent doit se montrer vigilant face aux tentatives d'attaque par ingénierie sociale (manœuvres visant l'obtention déloyale d'informations, biens ou services sensibles en exploitant la confiance ou la crédulité).

Sécurité physique des locaux et des matériels

La sécurité physique des locaux doit être cohérente avec la sécurité logique du réseau.

La libre circulation des personnes externes est interdite dans les locaux du ministère et chaque bâtiment doit filtrer la circulation des visiteurs dès l'accueil de la structure. La segmentation des locaux en zones de sécurité différenciées, associée à des règles de circulation pour les personnes externes à l'administration, participe à la sécurité du système d'information.

Échanges d'information

Toute transmission d'information de niveau C3 ou plus sera chiffrée en privilégiant un produit certifié ou qualifié par l'ANSSI. Pour le niveau C4 ou plus, le chiffrement sera obligatoirement effectué avec un produit certifié ou qualifié par l'ANSSI.

Publication de l'information

La publication d'information sur l'internet ou par tout moyen de communication au public ne concerne que des informations de niveau C0. Cette obligation s'impose à tous et dans tous les cas, notamment sur les réseaux et médias sociaux.

Assurance de conformité

Tout agent, tout service, tout SI doit se conformer aux obligations légales, réglementaires et contractuelles du ministère, en sus de la présente PSSI et conformément à la réglementation en vigueur en matière de sécurité, notamment au regard du Référentiel Général de Sécurité.

Cette stricte obligation de conformité s'applique notamment pour toutes les normes relatives à la sécurité, aux données personnelles (comme la loi Informatique et libertés de 1978) ou à la propriété intellectuelle.

Les logiciels doivent impérativement n'être utilisés qu'en conformité avec leur licence. Cette exigence s'applique de manière identique, que le logiciel ait une licence propriétaire ou libre.

Recommandations plus spécifiquement destinées aux administrateurs techniques

Formation

Tout agent exploitant le SI ou assurant des missions en lien avec la SSI a la possibilité d'être formé à la SSI et à la cyberdéfense, notamment via les stages organisés par le CFSSI de l'ANSSI après avis de son supérieur hiérarchique et du FSSI.

Procédures et responsabilités opérationnelles

Les modifications apportées aux équipements et aux systèmes informatiques du ministère doivent suivre une procédure formalisée incluant des tests de non-régression, des tests de sécurité, une mise à jour des procédures de sauvegardes.

Gestion des prestataires

Tout prestataire de service informatique doit disposer d'un contrat incluant des clauses de respect des principes de protection du SI décrits dans la présente politique, notamment au regard de la confidentialité et des transmissions d'informations.

Traces

Les traces générées par les systèmes opérés doivent être paramétrées dans la perspective du juste nécessaire à la conduite d'éventuelles investigations techniques légitimes. Il faut ainsi réduire au minimum indispensable la verbosité des systèmes.

Gestions des configurations

Les postes de travail et serveurs disposeront d'un socle technique standard, comprenant notamment une version maintenue du système d'exploitation, les mises à jour de sécurité et un antivirus.

L'ordinateur portable ou tout autre appareil mobile d'un agent traitant de données sensibles de l'Administration doit faire l'objet d'un chiffrement.

Sauvegardes

Chaque serveur du système d'information du ministère doit disposer d'une procédure de sauvegarde adaptée et conforme aux besoins exprimés par les maîtrises d'ouvrages.

Gestion de la sécurité de réseau

Le réseau des administrateurs techniques des systèmes d'information doit être cloisonné vis-à-vis du réseau principal afin de protéger les postes de travail de ces administrateurs.

Les administrateurs ont deux postes de travail distincts, l'un avec accès à l'internet et un compte non privilégié, et l'autre sans accès à l'internet mais avec le compte

d'administrateur.

Dans la mesure du possible, l'usage des comptes privilégiés (notamment le compte *root* lorsqu'il existe) est proscrit, en particulier lors d'une connexion à distance.

L'habilitation des administrateurs s'effectue selon une procédure validée par l'autorité d'homologation. Le nombre de personnes habilitées pour des opérations d'administration doit être connu et validé par l'autorité d'homologation.

Gestion des supports ou documents de sécurité

La mise à jour régulière de la documentation de sécurité est réalisée à chaque évolution significative du système d'information sous la responsabilité du SDSI.

Surveillance

Chaque système du ministère devra disposer d'une journalisation active permettant de tracer les événements sur une période au minimum égale à un mois glissant.

Homologation de sécurité des systèmes

Chaque SI permettant des échanges électroniques entre deux autorités administratives ou avec les usagers de l'une d'elle devra être homologué avant sa mise en production. C'est une démarche formalisée permettant d'identifier, d'atteindre puis de maintenir un niveau de risque de sécurité acceptable pour un SI, compte tenu du besoin de sécurité préalablement exprimé.

Développement et maintenance des systèmes

Les architectures techniques des systèmes doivent être définies par les MOE et validées par les MOA et les AQSSI correspondants.

Toute modification de système en production fait l'objet d'un mode opératoire formalisé. La modification doit être testée préalablement sur un environnement de test.

Gestion de la continuité d'activité

Toute salle informatique hébergeant des applications métiers ou d'infrastructures doit disposer d'un plan de secours informatique formalisé. Chaque activité critique du ministère doit disposer d'un plan de continuité d'activité formalisé et à jour.

« L'homme et sa sécurité doivent constituer la première préoccupation de toute aventure technologique »

Albert Einstein

in* Discours aux étudiants du California Institute of Technology*, février 1931

Table des matières

1 Stratégie de sécurité

1.1 Introduction

Une politique de sécurité des systèmes d'information (PSSI) établit le référentiel des règles applicables en matière de sécurité des systèmes d'information (SSI).

La PSSI du Ministère de l'agriculture, de l'agroalimentaire et de la forêt (PSSIA) traduit ainsi la vision stratégique du ministère pour la SSI.

L'établissement d'une PSSI est nécessaire à de nombreux égards :

- Une PSSI permet la sécurisation globale des risques pesant sur le ministère alors que les systèmes d'information (SI) sont devenus indispensables au bon fonctionnement des organismes et que les menaces informatiques sont toujours plus novatrices et étendues.
- La PSSIA est en accord avec le schéma directeur du système d'information, respecte la complémentarité avec les autres PSSI (dont la PSSI-DDI/Préfectures) et s'intègre avec la PSSI-E (PSSI de l'État), dont elle constitue la déclinaison ministérielle, pour s'appliquer de manière cohérente et ainsi prévenir les risques (accidents, erreurs, défaillances et malveillances) de manière globale.
- Une PSSI protège le patrimoine immatériel (informations, données) autant que le patrimoine matériel (biens nécessaires à l'activité) du ministère. Sont également protégées les personnes physiques et morales (le ministère, ses agents, l'État et les autres entités publiques avec lesquelles le ministère est en relation).
- La PSSIA vise la sécurité des systèmes d'information et la sécurité de l'information – les deux étant perçues comme complémentaires. Elle a ainsi vocation à prendre en compte les nouveaux usages et les réalités de manière à satisfaire au mieux les objectifs de sécurité identifiés par le ministère pour ses SI.
- La PSSIA est un document général qui doit être diffusé et connu de tous les agents internes ainsi que, le cas échéant, des personnes accédant aux SI de l'organisme (sous-traitants, prestataires, stagiaires, etc.). Elle permet de sensibiliser chaque utilisateur aux enjeux de la SSI.
- La PSSIA, dans sa version remaniée, se veut plus cohérente et lisible. Pour ce faire, elle est accompagnée d'une version simplifiée (cf. le Guide des principales bonnes pratiques qui précède la présente PSSI).

1.2 Champ d'application

La PSSI définit les règles et mesures applicables pour :

- L'administration centrale du ministère ;
- Les services déconcentrés rattachés au ministère (DRAAF, DAAF) ;
- Les établissements publics d'enseignement sous tutelle du ministère en charge de l'agriculture.

Les DDI, quant à elles, doivent appliquer la PSSI-DDI/Préfectures, qui comme indiqué est articulée et cohérente avec le présent document.

1.3 Lignes directrices de la stratégie de sécurité

Les risques pesant sur les activités du ministère appellent une réponse claire au travers de lignes directrices permettant de renforcer le niveau de protection des systèmes d'information et de formaliser une politique de sécurité ad hoc.

1.3.1 Accompagner les évolutions du SI et des organisations du ministère

La politique de sécurité doit permettre de prévenir les risques sans pour autant figer le système d'information et le rendre inapte à répondre aux nouveaux modes de travail et aux changements d'organisation nécessaires.

1.3.2 Mettre en place une organisation de sécurité transversale et homogène en s'appuyant sur un réseau de correspondants de sécurité de proximité

L'organisation de sécurité doit assurer la cohérence et la mutualisation au travers d'une chaîne de responsabilité transversale. Ainsi, le Haut Fonctionnaire de Défense et de Sécurité (HFDS) détermine la stratégie ministérielle en matière de SSI, mise en œuvre sous le pilotage opérationnel du Secrétariat Général (Sous-direction des systèmes d'information – SDSI).

Cette chaîne de responsabilité passe par les responsables hiérarchiques et repose *in fine* sur les utilisateurs du système d'information et plus particulièrement sur les responsables informatiques de proximité (BIP, RMSI, RSI, RTIC, DRTIC) qui doivent assurer la diffusion de bonnes pratiques de sécurité et la remontée d'incidents détectés au plus près du « terrain ».

1.3.3 Assurer la cohérence du niveau de protection logique et physique

Une protection efficace du système d'information passe nécessairement par la protection physique de celui-ci. Tout accès non maîtrisé au SI est un risque potentiel pour les activités critiques ou pour les informations sensibles du ministère.

Considérant la nature confidentielle des informations traitées par certains services, il est nécessaire d'adopter une protection globale alliant d'une part une protection physique de l'environnement de travail et d'autre part, une protection adéquate des infrastructures système et réseau.

1.3.4 Rendre homogène le niveau de sécurité entre l'administration centrale, les services déconcentrés et les établissements publics d'enseignement

L'utilisateur de l'administration centrale ou d'un service déconcentré rattaché au ministère (DRAAF et DAAF) doit être considéré de la même manière au regard des procédures d'accès et d'habilitation vis-à-vis du système d'information.

La fiabilité des données gérées au niveau central est directement liée à la fiabilité des données gérées au niveau local dans les services déconcentrés et les établissements publics d'enseignement.

Il est donc indispensable de promouvoir une pratique commune et équivalente en tout point en matière de « comportement » sécurité pour tous les utilisateurs et administrateurs, qu'ils soient en administration centrale ou en services déconcentrés.

Les établissements d'enseignement sont par définition amenés à être ouverts au public, mais parce qu'ils gèrent des données identifiées comme sensibles pour le ministère, ils doivent tendre vers le même niveau de sécurité que les services déconcentrés.

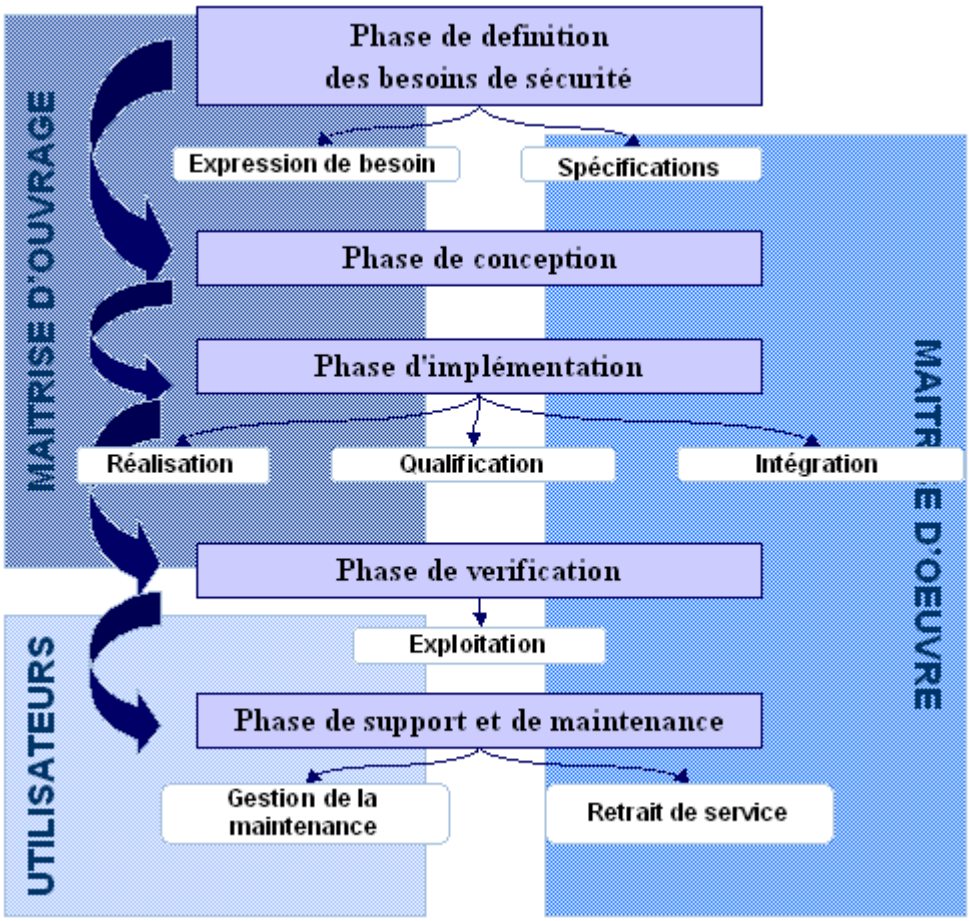
1.3.5 Accompagner le schéma directeur des SI en renforçant la fiabilité et la cohérence du SI

Le schéma directeur des systèmes d'information définit les axes majeurs et stratégiques du développement des systèmes d'information. Il se doit d'intégrer la nécessaire mise en œuvre des mesures de sécurité organisationnelles et techniques aptes à réduire les risques pesant sur ces systèmes d'information.

Il est donc indispensable que l'urbanisation des systèmes d'information prenne en compte la sécurisation des référentiels et des infrastructures techniques ou fonctionnelles sur lesquelles reposent les systèmes d'information du ministère.

1.3.6 Promouvoir une culture de la sécurité au travers de codes de bonnes pratiques accessible aux utilisateurs, maîtrises d'œuvre et maîtrises d'ouvrage

Il est rappelé par le schéma suivant, le cycle de vie d'un projet informatique.



Il est important de rappeler que le rôle d'une maîtrise d'ouvrage (MOA) est de définir le besoin des utilisateurs et notamment le besoin de sécurité vis-à-vis des informations traitées.

La maîtrise d'œuvre (MOE) se doit de développer et mettre en œuvre les mesures de sécurisation permettant de répondre au besoin.

L'exploitant doit prendre en compte les besoins de sécurité définis par les MOA dans ses procédures d'exploitation.

Les utilisateurs doivent appliquer les règles de sécurité définies.

Cette approche n'est efficace que si elle reste bien comprise par les différents acteurs.

Cette démarche se doit d'intégrer de bonnes pratiques de sécurité permettant de

garantir le niveau de protection existant et/ou attendu.

Il est donc essentiel de propager une culture sécurité via une communication adaptée aux différents acteurs.

1.3.7 Accompagner le renforcement du niveau de protection des partenaires en développant des standards et la mutualisation des moyens de protection

Le ministère est, par ses missions, ouvert sur l'extérieur et s'appuie sur un tissu important de partenaires avec qui les échanges et les interconnexions sont multiples et indispensables.

Il est donc opportun de veiller et de garantir un niveau de protection cohérent tout particulièrement quand le système d'information s'étend à des locaux hors contrôle direct du ministère, ou bien lorsqu'il est accessible par des utilisateurs qui ne font pas partie directement du ministère. La PSSIA vise à la construction d'une vision commune et partagée du niveau minimal indispensable de protection du SI.

2 Règles et exigences de sécurité

2.1 Politique de sécurité

EXG_PDS_01 La présente politique, dite PSSI-Agriculture ou PSSIA, s'applique aux entités suivantes :

- L'administration centrale ;
- Les services déconcentrés rattachés au ministère (DRAAF, DAAF) ;
- Les établissements publics d'enseignement sous tutelle du ministère de l'agriculture.

Elle contient des mesures et règles d'échange avec les autres organismes ; sous tutelle ou non du ministère. Elle est cohérente la PSSI DDI/Préfecture applicable notamment au sein des services déconcentrés sous compétences multi-ministérielles.

Elle peut être diffusée vers les prestataires et partenaires lorsque cette connaissance est nécessaire.

EXG_PDS_02 La **PSSI-Agriculture** est validée par le HFDS et le SG à chaque modification du document et approuvée formellement par le cabinet du Ministre

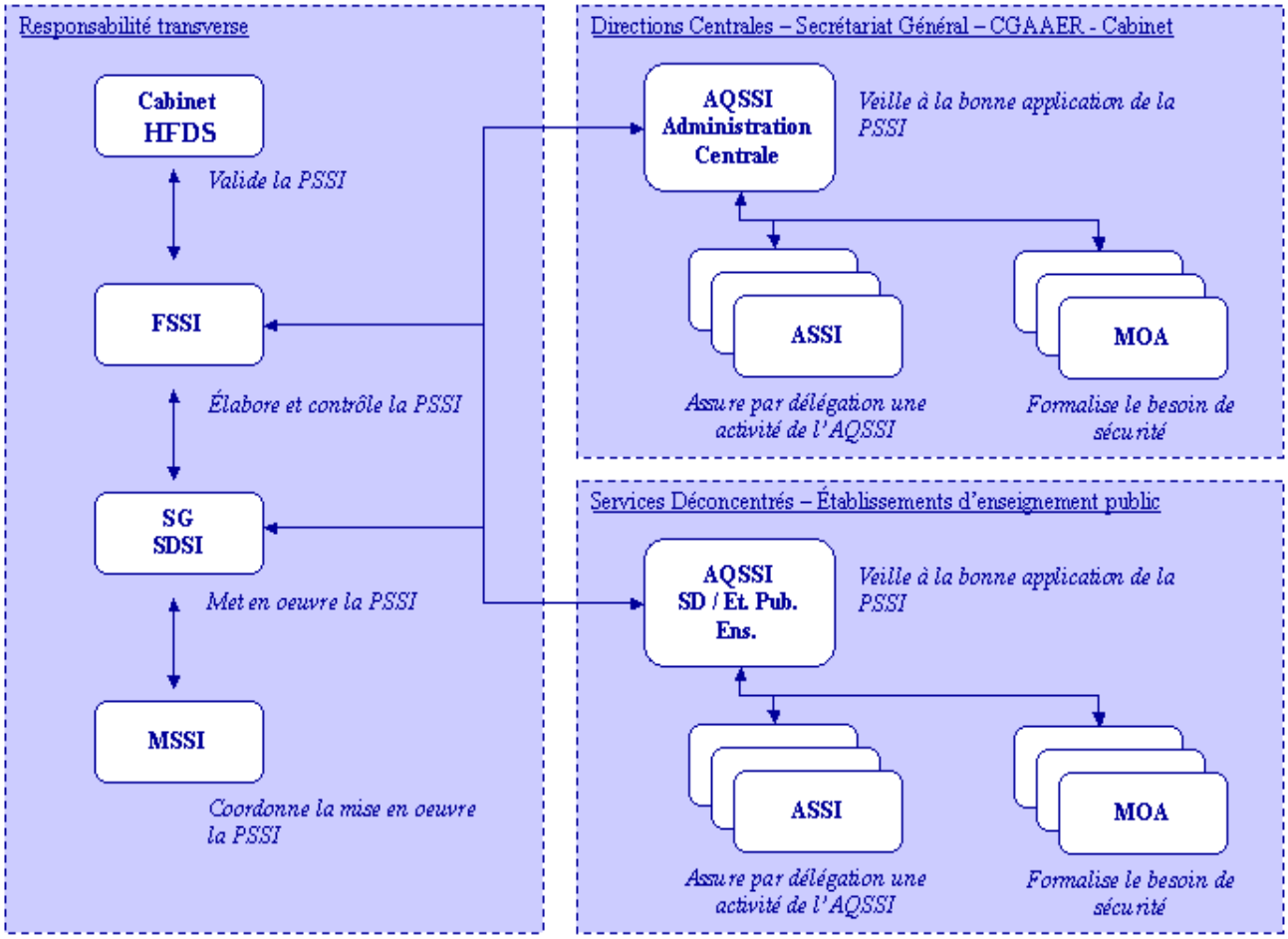
EXG_PDS_03 Une vérification de cohérence des exigences de la présente politique doit être réalisée dès qu'une évolution majeure apparaît. Cette dernière s'entend comme l'évolution majeure du contexte de l'administration, le changement technique ou organisationnel du système d'information du ministère, l'apparition d'une nouvelle menace majeure ou l'évolution des besoins de sécurité.

Cette vérification peut être aussi décidée de manière discrétionnaire, notamment à la suite d'un audit ou d'un indicent de sécurité majeur si des mesures ne sont pas identifiées dans le présent document ou sur demande d'une AQSSI, du FSSI ou du HFDS.

EXG_PDS_04 Toute modification de la PSSI-Agriculture qui aura un impact direct sur les utilisateurs entraînera nécessairement une communication.

2.2 Organisation de la sécurité de l'information

L'organisation de la sécurité des systèmes d'information est présentée au travers du schéma suivant et détaillée dans les chapitres ci-après :



2.2.1 Rôles et responsabilités des acteurs transverses

2.2.1.1 Le HFDS

EXG_ORG_01

Le HFDS est responsable de l'application des dispositions relatives à la sécurité de la défense nationale.

Conformément à l'Instruction générale interministérielle 900 et la Recommandation (ou Directive) 901, le Haut Fonctionnaire de Défense et de Sécurité est responsable de l'application des dispositions relatives à la sécurité de défense, à la protection du secret et à la sécurité des systèmes d'information.

EXG_ORG_02

Le HFDS :

- Valide la politique et ses évolutions avant approbation par le Cabinet ;
- Approuve les politiques référencées par la PSSIA (plan de continuité d'activité métiers, charte informatique, …) ;
- S'assure de la mise en œuvre des mesures nécessaires à la protection du patrimoine du ministère et des intérêts de l'État ;
- Représente le ministère dans les comités interministériels traitant de sécurité ou de sûreté de l'information ;
- Applique ou fait appliquer les plans interministériels de protection de l'information (protection de l'information classifiée de défense, plan VIGIPIRATE, …).
- Participe à la Commission d'Homologation des SI.

2.2.1.2 Le FSSI

EXG_ORG_03

Le HFDS est assisté d'un Fonctionnaire Sécurité des Systèmes d'Information.

Ses principales missions sont :

- De préciser les modalités d'application des instructions interministérielles, en particulier, il est responsable de la déclinaison des plans de protection interministériels (Piranet, sites sensibles, …) ;
- D'élaborer et de contrôler l'application des instructions particulières à son ministère ;
- D'organiser la sensibilisation des autorités ;

- D'assurer la liaison avec les commissions interministérielles et ministérielles spécialisées, en particulier, il représente le MAAF vis-à-vis de l'ANSSI ;
- Participe à la Commission d'Homologation des SI.

EXG_ORG_04 De manière permanente, le FSSI :

- Coordonne et anime les décisions prises en comité des AQSSI ; Il informe le HFDS et le Cabinet des décisions prises ;
- Est consulté pour l'organisation opérationnelle de la gestion de risque liée au système d'information ;
- Est responsable de l'analyse des risques et est responsable des préconisations pour couvrir tout risque critique pour le ministère concernant le SI ;
- Est informé des procédures de gestion et de réaction aux incidents SSI mises en place ainsi que des incidents critiques ;
- Est informé systématiquement des résultats des audits SSI menés par une MOA et ou une MOE sur une partie du SI ;
- Peut diligenter des enquêtes, suite à des incidents ou à des compromissions avérées, sur les traces des opérations réalisées sur le système d'information ;
- Assure le fonctionnement et le déploiement du réseau chiffré (ISIS) et du téléphone chiffré (Rimbaud).

EXG_ORG_05 Concernant la PSSI-Agriculture, le FSSI :

- Propose la PSSI-Agriculture au HFDS pour validation ;
- Contrôle et fait contrôler l'application de la PSSI-Agriculture ;
- Peut prendre en compte une demande d'évolution de la PSSI-Agriculture ;
- Peut déléguer partie ou totalité de la gestion de la PSSI-Agriculture ainsi que son contrôle ;
- Propose, élabore et coordonne la mise en place des PCA (Plan de Continuité d'Activités) et PRA (Plan de Reprise d'Activités).

Pour l'ensemble de ces missions, le FSSI peut demander un soutien méthodologique du SG pour réaliser les contrôles et celui d'un prestataire pour les aspects techniques. Le pilotage du prestataire peut être réalisé par la MSSI.

EXG_ORG_06 Concernant la classification de défense de l'information, le FSSI :

- Est responsable de la classification de l'information qu'il approuve et des procédures associées ;
- Valide toute déclassification d'information confidentielle.

EXG_ORG_07 Concernant la politique d'accès aux locaux hébergeant des équipements d'infrastructure, définie dans la PSSI-Agriculture, le FSSI :

- Valide la politique de contrôle des visiteurs ;
- Valide la politique de sécurité physique touchant les salles informatiques et les salles hébergeant des postes sensibles ;
- Valide la politique de sécurité physique des câblages.

2.2.1.3 Le Sous-Directeur des Systèmes d'Information

EXG_ORG_08 **Sous l'égide du secrétariat général et du service de la modernisation, le SDSI est le garant de la cohérence technique des dispositifs de protection pour l'ensemble des applications du ministère ainsi que de la cohérence des politiques de sécurité techniques des applications métiers ou transverses.**

En outre, le SDSI :

- Est force de proposition pour la mise en œuvre de la présente politique auprès des AQSSI des différentes directions de l'administration centrale ;
- Valide, d'un point de vue sécurité, les échanges d'informations avec les partenaires externes au ministère et s'assure que les contrôles de sécurité sont adaptés et opérationnels ;
- Est informé de tout incident sur le SI ;
- Est l'interlocuteur privilégié du FSSI sur les questions de sécurité ;
- Valide les politiques de sécurité des applications transverses du ministère ;
- Apporte son expertise et son conseil auprès des AQSSI de services déconcentrés.
- Est responsable de la coordination du déploiement des mesures techniques et procédures de sécurité vis-à-vis des centres de production et d'ingénierie concernant les infrastructures « support » et les applications nationales.
- Participe aux comités AQSSI ;
- Est responsable de l'inventaire des ressources du SI ;
- Valide les clauses de sécurité type qui doivent être présentes dans les contrats prestataires ;
- Valide les exigences de sécurité physique des salles informatiques ;

- Valide la politique d'identification et d'authentification des utilisateurs du SI ;
- Approuve les standards de développement des applications internes ;
- Analyse et valide le traitement des incidents critiques ;
- Valide les plans de secours et de sauvegarde ;
- Participe à la Commission d'Homologation des SI.

2.2.1.4 La Mission Sécurité des Systèmes d'Information

EXG_ORG_09

Sous l'autorité du SDSI, la MSSI a pour mission principale d'assurer la cohérence du niveau de protection sur l'ensemble du SI du ministère.

La MSSI représente la SDSI pour les questions de sécurité des SI dans toutes les instances où elle intervient.

EXG_ORG_10

Concernant la PSSI-Agriculture, la MSSI :

- Fournit les recommandations et mesures à mettre en œuvre ;
- Est responsable de la conduite des évolutions de la PSSI-Agriculture et de la communication des changements ;
- Réalise le suivi de la mise en œuvre de la PSSI-Agriculture ;
- Assure le suivi de la mise en œuvre du Plan d'actions pour l'Administration Centrale, les Services Déconcentrés, et les Établissements publics d'enseignement ;
- Supervise l'inventaire des équipements de sécurité ;
- Pilote les programmes de sensibilisation et formation à la sécurité ;
- Formalise un modèle standard de clauses de sécurité dans les contrats avec les prestataires ;
- Propose à la validation du SDSI les principes d'habilitation, la politique d'identification/authentification des utilisateurs des SI du MAAF ;
- Propose à la validation du SDSI la politique de sécurité physique des salles informatiques et des locaux techniques en ce qui concerne le contrôle d'accès ;
- Contrôle le bon respect et la bonne prise en compte des exigences sécurité par les équipes chargées de l'exploitation informatique et par les équipes chargées de l'exploitation des dispositifs de sécurité ;

- S'assure que les exigences sécurité fixées par la MOA sont cohérentes vis-à-vis de la politique de sécurité ;
- S'assure de la prise en compte des procédures de journalisation (production des traces dans des fichiers journaux) sur les composants en cours de développement et de la mise en œuvre de ces procédures sur les applications en production ;
- Contrôle ou fait contrôler la robustesse technique et organisationnelle des moyens de protection mis en place sur chaque application nationale pour répondre aux besoins de sécurité ;
- S'assure qu'un plan de sauvegarde a été spécifié par la MOA ;
- Vérifie que chaque plan de sauvegarde est régulièrement testé ;
- Assure la veille méthodologique, juridique et technologique dans le domaine de la sécurité ;
- Assure la coordination du traitement des incidents de sécurité majeurs et critiques (ouverture, qualification, traitement, clôture, lien avec les autorités externes) ;
- Définit le référentiel ISP ;
- Assure le secrétariat de la Commission d'Homologation des SI.

2.2.2 Rôles et responsabilités des Autorités Qualifiées en Sécurité des Systèmes d'Information (AQSSI)

EXG_ORG_11

Les AQSSI du ministère doivent veiller à la bonne application de la PSSI-Agriculture dans la structure (direction, service, établissement) à laquelle ils sont rattachés et, en tant que de besoin, définir des consignes et directives internes propres à leur structure, en cohérence avec la présente politique.

L'arrêté du Ministère en date 27 avril 2007 porte désignation des AQSSI. De manière générale, l'AQSSI est le directeur ou le principal responsable de la structure.

EXG_ORG_12 L'AQSSI est responsable :

- De faire appliquer la PSSI-Agriculture dans sa structure ;
- De demander une évolution de la PSSI-Agriculture dès que nécessaire ou de donner un avis en cas de consultation pour l'élaboration de nouvelles exigences ;
- De s'assurer que les contrôles internes de sécurité aptes à vérifier le niveau d'application de la PSSI-Agriculture sont régulièrement effectués ;

L'AQSSI pourra s'appuyer sur un ou plusieurs Agents chargés de la Sécurité des Systèmes d'Information (ASSI) :

- L'agent nommé doit avoir démontré une compétence suffisante pour réaliser sa mission. Le cas échéant, il devra suivre une formation préalable sans laquelle sa prise de fonction ne pourra pas être effective.
- Toute nomination doit être accompagnée d'une lettre de mission, notifiée au FSSI par l'AQSSI et d'une demande au préalable d'habilitation au secret de la défense nationale.
- La lettre de mission doit définir explicitement les rôles et responsabilités de l'agent, son périmètre d'intervention et les indicateurs de performance associés.

L'AQSSI doit, éventuellement avec l'aide du ou des ASSI qu'il aura nommés :

- Tenir à jour l'inventaire des informations sensibles détenues par sa structure ;
- Décrire le mode opératoire mis en place au sein de sa structure pour répondre aux règles et exigences de la présente politique ;
- Diffuser la PSSI-Agriculture auprès des agents de sa structure et veiller à son application ;
- Assurer la bonne définition des besoins de sécurité des projets de sa structure et de veiller à la bonne mise en œuvre par les maîtrises d'œuvres correspondantes ;
- S'assurer que les agents ont tous participé au moins à une session de sensibilisation à la sécurité ;
- S'assurer que les dispositions réglementaires et contractuelles, avec des tiers le cas échéant, relatives à la sécurité des systèmes d'information, sont formalisées et appliquées ;
- Apporter sa contribution aux plans de lutte interministériels contre le cyber-terrorisme, en prenant notamment en compte les avis ou alertes émis par le Centre d'expertise gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) et en rendant compte immédiatement aux autorités de tout incident et de tout phénomène suspect pouvant affecter la sécurité des systèmes d'information ;
- S'assurer régulièrement du bon fonctionnement du téléphone

Rimbaud et de prévenir le FSSI de toute anomalie.

EXG_ORG_13 L'AQSSI est informé :

- Des résultats des audits touchant sa structure ;
- Des modifications de la PSSI-Agriculture et les éventuels documents d'application de la politique ;
- De tout incident majeur sur le SI impactant directement les activités de sa structure ;
- Des enquêtes en cours touchant sa structure.

EXG_ORG_14 À la demande du HFDS ou du SG, les sujets de SSI peuvent être évoqués en comité des directeurs d'administration centrale (CODAC), sous la forme d'un point dédié animé par le FSSI.

À l'occasion de ce type de point, le SDSI fait état des principaux événements sécurité remontés par les AQSSI des services déconcentrés et AQSSI des établissements publics d'enseignement. La mise en condition opérationnelle des procédures de sécurité dans chaque direction et service du ministère fait également l'objet d'une revue régulière.

Le compte rendu correspondant est de confidentialité C4.

EXG_ORG_15 Le travail de l'Agent chargé de la Sécurité des Systèmes d'Information (ASSI) est encadré par la note de référence n° 375/HFDS/ED du 02/10/2009.

EXG_ORG_16 **Le directeur ou chef de service en administration centrale, service déconcentré rattaché au ministère (DRAAF et DAAF), établissement public d'enseignement agricole est AQSSI pour sa direction, son service, son établissement.**

EXG_ORG_17 Dans tous les cas, chaque directeur (AQSSI) est responsable vis-à-vis de ses services :

- D'approuver la définition du besoin de sécurité lié à ses activités, concernant les applications métiers dont il a l'usage ou la responsabilité, ainsi que de ses locaux physiques.
- De veiller à la bonne application de l'ensemble des exigences et règles qui lui sont prescrites au travers de cette présente politique.

Plus particulièrement, chaque directeur (AQSSI) :

- Est informé des enquêtes ou incidents de sécurité qui concernent ses

applications ou les personnels de sa direction ;

- Valide le Plan de Continuité d'Activité des systèmes d'information concernant sa direction et diligente des tests de fonctionnement de ce plan à une fréquence minimale d'une fois par an ;
- Identifie les membres du personnel de sa direction qui doivent pouvoir être mobilisés en cas de crise majeure ;
- Doit fournir un bilan annuel du niveau de mise en œuvre de la PSSI-Agriculture dont l'auto-diagnostic doit parvenir à la MSSI et au FSSI.

2.2.3 Rôles et responsabilités des autres acteurs

2.2.3.1 Le service en charge de la sécurité opérationnelle

EXG_ORG_18

Le service en charge de la sécurité opérationnelle (anciennement DIP, pour département de l'ingénierie de production) doit respecter les besoins de sécurité formulés par les conclusions des études visant à intégrer la sécurité dans les projets informatiques (méthode ISP) et les prendre en compte dans ses procédures d'exploitation.

Il est de plus responsable de la mise en œuvre des procédures de sécurité applicables aux services transverses apportés par la plate-forme de production (sauvegardes, sécurisation des systèmes d'exploitation, filtrage antivirus, filtrage anti-SPAM, …) qui participent à la sécurisation des applications hébergées.

Il réalise et maintient l'inventaire des ressources techniques sous sa responsabilité.

EXG_ORG_19

Toute procédure de sécurité sous responsabilité du service en charge de la sécurité opérationnelle doit être formalisée et mise à jour par ses soins.

Toute procédure de sécurité doit être validée par la MSSI.

Les procédures de sécurité du service en charge de la sécurité opérationnelle concernent au minimum pour chaque serveur hébergé :

- L'habilitation des administrateurs ;
- La protection des accès ;
- La journalisation des événements ;
- La sauvegardes des données ;
- Les mises à jour de sécurité ;
- Les audits techniques sur les équipements.

Les procédures de sécurité du Centre de production prennent en compte le plan de continuité d'activité (PCA) du MAAF en conformité avec les règles définies par la présente politique.

EXG_ORG_20

Le service en charge de la sécurité opérationnelle contribue à la détection des atteintes à la sécurité en inscrivant les incidents et anomalies dans une base *ad hoc*, il réalise la pré-qualification des incidents techniques de sécurité sur les équipements de production et assure leur traitement selon les directives établies par la MSSI.

EXG_ORG_21

Le service en charge de la sécurité opérationnelle est responsable de :

- La gestion des pare-feux (paramétrage, mise à jour, vérification de bon fonctionnement), qui filtrent les flux aux points de jonction du réseau MAAF avec les autres réseaux ;
- La gestion des équipements relais (paramétrage, mise à jour, vérification de bon fonctionnement) tels que les « proxies » et « reverse proxies » et autres « serveurs d'accès VPN », qui assurent le contrôle des flux en provenance ou à destination du réseau internet ;
- La mise en place et la gestion (définition de l'architecture, paramétrage, suivi des mises à jour, …) de la politique anti-virale des postes de travail utilisateur ;
- La mise en place et la gestion (définition de l'architecture, paramétrage, suivi des mises à jour, …) de la politique anti-virale des serveurs d'échange de courrier du ministère ;
- La gestion de la protection des serveurs de messagerie en respectant la politique de sécurité de cette infrastructure ;
- La définition du standard de sécurisation des postes de travail ;
- La gestion de l'infrastructure de gestion de certificats (IGC) en respectant les politiques de certification ;
- La veille en matière de sécurité des SI et plus particulièrement concernant le matériel qui est sous sa responsabilité ;
- La gestion des alertes de sécurité émises notamment par le CERT-FR (centre d'alerte interministériel) relatives aux différents environnements techniques utilisés dans le MAAF (postes de travail et serveurs bureautiques, équipements du Centre de production (réception des alertes, qualification des failles et alerte des responsables informatiques de proximité) ;
- Le traitement des incidents de sécurité conformément aux exigences et règles de la présente politique ;
- La validation de toute nouvelle infrastructure intégrée au Centre de Production.

2.2.3.2 Les Maîtrises d'Ouvrage

EXG_ORG_22

Toute application devant être mise en production au ministère doit disposer d'une maîtrise d'ouvrage (MOA) associée. La maîtrise d'ouvrage est

nommée par le directeur concerné qui informe le SDSI.

Toute modification de maîtrise d'ouvrage doit être validée par le directeur concerné et communiquée dans les 48 heures au SDSI.

EXG_ORG_23 Toute MOA prendra en compte les procédures de sécurité dès le démarrage du projet. En particulier, chaque MOA formalisera les besoins de sécurité identifiés pour ses projets et participe à l'élaboration des plans de continuité d'activité.

Les tâches à réaliser par la MOA sont :

- L'identification du niveau de sensibilité de chaque information gérée ;
- Une analyse de risque spécifique lié à l'application ;
- La définition du besoin de sécurité de l'application identifiant les niveaux de Disponibilité, d'Intégrité, de Confidentialité et de Preuve attendus ;
- Le besoin de ressources dédiées à la sécurité pour le déroulement du projet ;
- La définition des exigences sécurité à intégrer dans les spécifications fonctionnelles ;
- La vérification de la prise en compte effective des spécifications par des mesures de sécurité techniques robustes mises en œuvre par la maîtrise d'œuvre et l'exploitant.

2.2.3.3 Les équipes de maîtrise d'œuvre

EXG_ORG_24 **Les équipes de maîtrise d'œuvre, internes ou externes au ministère, doivent appliquer les mesures de sécurité lors du développement des applications du ministère.**

Dans ce cadre, ils doivent respecter :

- Les règles et consignes de sécurisation nécessaires :
  - À la protection des sources ;
  - Aux règles de codages ;
  - Aux règles de tests et de mise en production ;
  - À l'identification et l'authentification des utilisateurs des applications ;
  - À la protection des données traitées par les applications ;
- Les besoins de sécurité émis par les MOA ;

La maîtrise d'œuvre doit, avant la mise en production de toute application, réaliser des tests qui incluent la vérification de la mise en place du niveau de sécurité attendu par la MOA, notamment formalisé par la Politique de Sécurité de l'application.

EXG_ORG_25 Chaque maîtrise d'œuvre est nommée par le SDSI. La MSSI est informée et assiste à la réunion de lancement du projet dès lors que la maîtrise d'ouvrage a identifié l'application comme critique pour le ministère.

EXG_ORG_26 Chaque MOE définit le plan de sauvegarde opérationnel permettant de garantir que le besoin de Disponibilité et d'Intégrité des informations défini par la MOA dans sa Politique de Sécurité applicative est bien pris en compte.

Ce plan de sauvegarde opérationnel est ensuite intégré dans le plan de sauvegarde de l'exploitant (Centre de production ou exploitant externe au MAAF).

2.2.3.4 Le BPSI

EXG_ORG_27

Le Bureau du Pilotage des Systèmes d'Information (BPSI) doit veiller à intégrer les aspects sécurité au plan organisationnel et au plan technique dans le schéma directeur national des systèmes d'information.

Le BPSI, en lien avec la MSSI, veille à ce que les MOA définissent leurs besoins de sécurité en cohérence avec la politique de sécurité transversale portée par la Sous-Direction des Systèmes d'Information.

Le BPSI, en lien avec la MSSI, veille à ce que l'urbanisation des systèmes d'information prenne en compte la sécurisation des référentiels et des infrastructures techniques ou fonctionnelles sur lesquelles reposent les systèmes d'information du ministère.

Le BPSI, en lien avec la MSSI, apporte son soutien à la mise en œuvre de la PSSI-Agriculture.

2.2.3.5 Le BMSQ

EXG_ORG_28

Le Bureau des Méthodes, du Support et de la Qualité s'assure de la bonne mise en œuvre de la démarche qualité dans les projets.

En matière de sécurité, le BMSQ assure :

- Le choix et la qualité des outils du cadre de cohérence technique en liaison avec les exigences sécurité décrites dans la PSSI ;
- La sécurisation de la FORGE (outil de gestion de configurations) et tous les autres composants de l'usine logicielle préconisés par le BMSQ ;
- Le suivi des travaux de la Commission d'Architecture Applicative et Technique, qui permet de contrôler l'insertion des projets dans le cadre de cohérence technique.

2.2.3.6 Le Conseil des Systèmes d'Information

EXG_ORG_29

Le CSI est saisi pour avis du développement et de la mise en œuvre des SI du ministère.

Le CSI :

- Est informé et consulté pour les évolutions de la PSSI-Agriculture et veille avec la SDSI à l'interopérabilité de la PSSI-Agriculture avec les

partenaires du ministère ;

- Veille à ce que les organismes partenaires du ministère assurent un niveau de sécurité élevé en cohérence avec la présente politique ;
- S'assure, lors de l'examen des projets présentés en CSI :
  - De l'existence d'une expression des besoins de sécurité formalisée par la MOA ;
  - De la prise en compte de la présente politique par la MOA.

2.2.3.7 Les responsables informatiques de proximité

EXG_ORG_30

Les responsables informatiques de proximité, qu'ils soient en Administration Centrale ou en Service Déconcentré, RMSI, RSI, RTIC ou DRTIC, sont les relais directs ou indirects entre les utilisateurs et la SDSI sur les questions de sécurité des systèmes d'information.

Ils sont responsables au plan local :

- De l'application des mesures de sécurité sur les serveurs et postes de travail bureautiques, ainsi que sur les équipements réseau et de téléphonie ;
- Du cloisonnement du réseau et de sa mise en œuvre ;
- De mettre en œuvre et faire appliquer les recommandations de sécurité propres aux utilisateurs ;
- D'assurer la sensibilisation à la sécurité des systèmes d'information des utilisateurs ;
- De formaliser les procédures de sécurité de leur structure (de proximité) dans un document validé par l'AQSSI concerné ;
- De remonter et faire état de tout dysfonctionnement impactant la sécurité du SI auprès de l'AQSSI concerné et du SDSI ;
- De réaliser l'inventaire des ressources informatiques (logiciels, postes de travail, imprimantes, serveurs, équipements réseau et de téléphonie, PDA, …) ;
- De veiller au bon fonctionnement des sauvegardes locales et de leur protection ;
- De veiller à la réalisation de tests périodiques de restauration ;
- De réaliser un PCI-PCA en collaboration avec l'ASSI.

EXG_ORG_31

Au sein de l'administration centrale, le rôle de responsable informatique de proximité est assuré par le Bureau d'Informatique de Proximité (BIP), qui intervient auprès des agents dans le cadre de l'assistance et du support informatique de proximité.

Il s'assure de la conformité des postes de travail relativement à leur configuration

de sécurité, et notamment à la présente PSSI.

Ce bureau assure aussi une mission de surveillance générale de même que la réalisation d'actions, notamment en cas d'urgence, relativement aux préconisations et alertes de sécurité.

2.2.3.8 Agents

EXG_ORG_32

Tout agent habilité par son responsable hiérarchique à accéder aux locaux et ressources du réseau interne du MAAF doit respecter les règles et principes de la présente PSSI-Agriculture.

EXG_ORG_33

Tout agent doit appliquer dans les plus brefs délais les consignes de sécurité ponctuelles ou permanentes transmises par sa hiérarchie ou par l'AQSSI de son organisation.

2.2.3.9 Les utilisateurs temporaires

EXG_ORG_34

Tout utilisateur temporaire, qu'il soit agent de la fonction publique, vacataire ou prestataire externe, doit s'engager explicitement à respecter les exigences de la présente PSSI-Agriculture.

2.3 Classification des informations

EXG_CLA_01

Toute information, qu'elle soit électronique ou non, doit disposer d'un responsable explicitement identifié, connu et appartenant à l'organisation du ministère.

EXG_CLA_02

Concernant les informations non classifiées de défense, l'auteur d'une l'information ou le responsable d'une application du ministère (MOA), doit fournir une évaluation (dite DICP) du niveau de sensibilité de celle-ci en termes de :

- **Disponibilité ;**
- **Intégrité ;**
- **Confidentialité ;**
- **Preuve.**

EXG_CLA_03 Concernant les informations classifiées de défense, l'auteur et le dépositaire d'information se référera aux directives du HFDS dans le respect du cadre réglementaire pour le traitement des informations classifiées de défense (habilitation spéciale, disposition d'un coffre, séparation des réseaux).

EXG_CLA_04 La maîtrise d'ouvrage est garante des accès accordés aux informations gérées par l'application dont elle a la charge et doit examiner au minimum une fois par an les accès accordés afin d'en vérifier la cohérence et la pertinence.

EXG_CLA_05 Le réseau général du ministère ne doit traiter aucune information classifiée de défense.

EXG_CLA_06 La classification de l'information en fonction du besoin de ***Disponibilité*** est la suivante :

- **Faible (D1)** : Ce niveau traduit délai maximal d'interruption autorisée entre une semaine et un mois. Ce niveau indique que l'indisponibilité a peu de conséquences.
- **Moyen (D2)** : Ce niveau traduit un délai maximal d'interruption autorisée de 5 jours consécutifs ouvrés. Ce niveau indique que l'indisponibilité peut avoir des conséquences néfastes pour le ministère et que sa durée doit être réduite.
- **Fort (D3)** : Ce niveau traduit un délai maximal d'interruption autorisée de 2 jours consécutifs ouvrés. Ce niveau indique que l'indisponibilité a des conséquences graves pour le ministère.
- **Très Fort (D4)** : Ce niveau traduit un délai maximal d'interruption

autorisée de 8 heures consécutives ouvrées. Ce niveau indique que l'indisponibilité peut entraîner des conséquences critiques pour le ministère.

- **Vital (D5)** : Ce niveau traduit une tolérance inférieure à 4 heures. Ce niveau indique que l'indisponibilité peut avoir des conséquences très critiques pour le ministère ; ainsi, l'indisponibilité doit être réduite au minimum.

EXG_CLA_07 La classification de l'information en fonction du besoin d'***Intégrité*** est la suivante :

- **Faible (I1)** : Ce niveau traduit un besoin d'intégrité de l'information satisfait par les mesures standards mise en œuvre au ministère. Ce niveau impose que toute perte d'intégrité doit être signalée et corrigée.
- **Moyen (I2)** : Ce niveau traduit une intégrité de l'information permettant son opposabilité au niveau P2. Le risque admissible de perte ou de modification non autorisée des données est assez faible.
- **Fort (I3)** : Ce niveau traduit une intégrité de l'information permettant son opposabilité au niveau P3. Le risque admissible de perte ou de modification non autorisée des données est le plus faible possible.
- **Vital (I4)** : Ce niveau traduit une intégrité totale de l'information permettant son opposabilité au niveau P4. Le risque admissible de perte ou de modification non autorisée des données est quasi nul, que cela soit lors du stockage, du traitement ou de l'échange de ces données.

EXG_CLA_08 La classification de l'information en fonction du besoin de ***Confidentialité*** est la suivante :

- **Public (C0)** : Ce niveau concerne les informations réputées publiques, et notamment celles publiées en ligne ou via un autre moyen de diffusion au public, en particulier sur le site data.gouv.fr.
- **Interne + usager concerné (C1)** : Ce niveau traduit que la diffusion est seulement possible vers le ou les usager(s) ou le ou les agent(s) concernés par le document, à l'exclusion de toute autre personnes à l'extérieur du ministère. Le document est en revanche accessible aux agents concernés du ministère
- **Interne (C2)** : Ce niveau restreint la diffusion d'information aux seuls agents du ministère ou d'une autre administration concernée dans le respect de la loi 78-17 du 6 janvier 1978.
- **Confidentiel (C3)** : Ce niveau restreint la diffusion d'informations aux seuls agents ayant le droit d'en connaître.
- **Stratégique (C4)** : Ce niveau concerne uniquement les informations de caractère stratégique pour le ministère et faisant l'objet d'une protection ad hoc.

EXG_CLA_9 Un référentiel de mesures techniques minimales associées à chaque niveau de DICP est disponible. Il liste les éléments techniques à mettre en œuvre pour

chaque niveau (par exemple chiffrement des flux au niveau C2 et supérieurs).

EXG_CLA_10 La classification de l'information en fonction du besoin de ***Preuve*** est la suivante :

- **Faible (P1)** : Ce niveau traduit un besoin très faible et pouvant être satisfait par l'usage des procédés standards de journalisation mis en œuvre au ministère.
- **Moyen (P2) :** Ce niveau garantit un niveau de preuve uniquement opposable au sein du ministère ou de l'État. Il doit être exclu pour tout système en direction des usagers.
- **Important (P3) :** Ce niveau garantit un niveau de preuve opposable conforme aux principes de la preuve visés par les articles 1316-1 et suivants du Code civil, mais ne garantit pas l'équivalence avec un écrit. Il garantit une opposabilité de la preuve devant toutes les juridictions ne faisant pas appel à la preuve par écrit et notamment le Tribunal administratif ainsi que l'ensemble des juridictions pénales.
- **Équivalent Écrit (P4) :** Ce niveau garantit un niveau de preuve opposable conforme aux principes de la prédominance de la preuve par écrit notamment visé par l'article 1341 du Code civil. Il garantit une opposabilité de la preuve devant l'ensemble des juridictions françaises, européennes ou internationales.

2.4 Ressources humaines

EXG_SRH_01 **Chaque agent prendra connaissance des exigences de sécurité le concernant à sa prise de fonction et veillera à les respecter.**

Elles peuvent être directement intégrées à la fiche de poste mais seront plus souvent documentées au travers du livret d'accueil.

EXG_SRH_02 L'AQSSI doit veiller à ce que tout agent prenne connaissance de la charte informatique, traduisant pour l'utilisateur les règles de la présente politique à appliquer.

EXG_SRH_03 **Tout recrutement doit faire état des consignes de sécurité propres au poste ciblé, au minimum le rappel du nécessaire respect de la PSSI, de l'obligation d'alerte en cas de risque, et enfin de confidentialité et de sécurité des informations.**

EXG_SRH_04 Toute personne amenée à manipuler des outils – logiciels, matériels – permettant d'obtenir des privilèges élevés dans l'accès aux systèmes d'information du ministère, ou disposant des codes d'accès permettant d'obtenir ces privilèges, doit faire l'objet de vérifications :

- Absence de faits notoires contraires à la déontologie liée à l'utilisation d'un système d'information (recherche d'information non autorisée, abus de droits, tentative d'intrusion dans des systèmes d'information…) ;
- Vérification de l'exhaustivité et de l'exactitude du curriculum vitae du candidat ;
- Confirmation des diplômes universitaires et qualifications professionnelles déclarés.

Les contrats avec les prestataires externes doivent, en tant que de besoin, traduire cette exigence par une clause contractuelle.

EXG_SRH_05 Tout intervenant externe au ministère auquel est donné l'accès à des informations du ministère de niveau C2 ou plus doit signer un accord de confidentialité avant d'obtenir l'accès à ces informations ou aux systèmes concernés.

EXG_SRH_06 **Tout agent doit recevoir une sensibilisation à la sécurité des systèmes d'information adaptée à sa fonction. Cette sensibilisation a lieu de manière régulière, ou, *a minima*, au moment de la prise de poste.**

EXG_SRH_07 L'ingénierie sociale est une manœuvre visant l'obtention déloyale d'informations,

biens ou services sensibles en exploitant la confiance ou la crédulité.

Tout agent doit se montrer vigilant face aux tentatives d'ingénierie sociale.

Face à l'augmentation de ces manœuvres frauduleuses utilisant les failles humaines et sociales, chaque agent doit prendre garde à ne pas divulguer, volontairement ou non, des informations stratégiques ou sensibles dans ses conversations avec des tierces personnes.

Dans le même sens, chaque agent doit, grâce à des actions adaptées, garantir l'authenticité des informations qu'il échange avec un autre agent, afin de lui enlever tout soupçon d'être la cible d'une manœuvre d'ingénierie sociale.

EXG_SRH_08 Tout administrateur de sécurité doit disposer d'une formation dédiée afin de réaliser les tâches quotidiennes de sécurisation du SI. Tout administrateur a l'obligation de prendre toutes les mesures nécessaires pour garantir l'intégrité du système d'information du ministère dans une démarche cohérente et d'en informer la MSSI et le service en charge de la sécurité opérationnelle.

EXG_SRH_09 Toute personne ayant accès aux systèmes d'information du ministère – agent ou personnel sous contrat – qui cesse son activité plus de six mois (congé longue durée, fin de contrat, disponibilité, etc.) se verra suspendre tous ses accès au maximum dans les cinq jours ouvrés suivant son départ.

Le délai de cette suspension sera limité à trois semaines au maximum, les droits d'accès seront ensuite immédiatement supprimés.

EXG_SRH_10 Tout AQSSI veillera à l'existence d'une procédure d'arrivée et de départ des personnels au sein de son service. Cette procédure inclura notamment la vérification de la restitution effective des équipements appartenant au ministère et la suppression de ses différents comptes d'utilisateurs et certificats IGC.

Il veillera à ce que la charte informatique soit incluse dans le dossier d'accueil de l'agent.

2.5 Gestion des prestataires

EXG_PRE_01

Tout prestataire de service informatique doit disposer d'un contrat incluant des clauses de respect des principes de protection du SI décrit dans la présente politique, notamment au regard de la confidentialité et des transmissions d'informations.

Les contrats de services devront indiquer une période minimale de deux ans après la fin dudit contrat pendant laquelle ces obligations de confidentialité perdurent. Les clauses types seront proposées par la SDSI. Cette période sera augmentée au niveau de confidentialité du projet.

EXG_PRE_02 Si les développements sont externalisés, le prestataire doit s'engager à respecter les mesures de protection demandées par le ministère et à laisser le ministère contrôler l'efficacité des mesures.

EXG_PRE_03 En cas d'infogérance, le prestataire doit s'engager à :

- Respecter les exigences de la présente politique le concernant et garantir un niveau de protection conforme à celle-ci ;
- Assurer la protection des accès au Système d'Information du ministère par des personnels habilités et engagés formellement à ne pas nuire d'une quelconque manière à l'activité du ministère ;
- Définir une organisation de sécurité clairement identifiée, activable par le ministère en cas d'incident majeur sur le périmètre infogéré ;
- Autoriser des audits de sécurité sur les procédures et moyens mis en place pour garantir le niveau de sécurité des informations du ministère et ce, au minimum, une fois par an.

2.6 Sécurité physique des locaux et matériels

EXG_PHY_01 **La sécurité physique des locaux doit être cohérente avec la sécurité logique du réseau.**

Tout équipement technique et tout local informatique doit disposer d'un responsable explicitement identifié, connu et appartenant à l'organisation du ministère.

EXG_PHY_02 Tous les services applicatifs internes, serveurs bureautiques ou serveurs de fichiers du ministère, éventuellement tout service d'informatique en nuage, doivent être hébergés dans des locaux adaptés et mutualisés dont l'accès est limité aux membres de la SDSI ou aux équipes informatiques de proximité.

EXG_PHY_03 Toute externalisation (ou modification d'une externalisation) de service applicatif du ministère (site web, application métier, etc.) sera validée par la SDSI, et fera l'objet d'un contrat ou d'une convention entre le ministère et l'hébergeur dont la gestion sera sous la responsabilité de la SDSI.

Le contrat intégrera impérativement des engagements de protection de l'information conformes aux besoins exprimés par les MOA et par la présente politique.

EXG_PHY_04 Les salles informatiques hébergeant les composants du système d'information, serveurs ou réseaux, leurs équipements d'alimentation et de distribution d'énergie du ministère doivent être protégées en permanence contre tout accès non autorisé et contre les agressions extérieures.

Les accès à ces salles sont limités aux seules personnes habilitées. Celles-ci doivent être identifiées nominativement et la liste doit être contrôlée, au minimum une fois par an, par l'AQSSI.

EXG_PHY_05 Les locaux hébergeant les applications ou composants critiques du SI (sans oublier les composants critiques de l'infrastructure support : réseau, messagerie, autres services support) doivent bénéficier de mesures de protection appropriées, notamment contre :

- Les incendies,
- Les intrusions,
- Les dégâts des eaux,
- Les défaillances électriques,
- Les défaillances des moyens de télécommunications,
- Les défaillances de climatisation et de conditionnement d'air.

EXG_PHY_06 Le câblage téléphonique et/ou informatique doit, dans la mesure du possible, être protégé contre tout accès malveillant pouvant conduire à des écoutes ou des dégradations.

Il est indispensable de garantir la protection des accès aux équipements de terminaison et de routage par des locaux opaques et au minimum fermés à clé.

EXG_PHY_07 Les salles informatiques hébergeant notamment les composants critiques et sensibles (serveurs, équipements de sécurité et de routage, dispositifs de stockage d'informations) doivent être équipées d'un contrôle permettant de journaliser les entrées et les sorties de chaque membre du personnel et, sous la condition de respect d'une procédure formelle, des personnes non-habilitées.

EXG_PHY_08 Un système de détection d'intrusion physique dans les salles informatiques hébergeant les composants critiques et sensibles, relié à un poste permanent de surveillance comprenant au moins deux personnes capables d'intervenir rapidement, doit être opérationnel en dehors des heures ouvrées.

EXG_PHY_09 Tous les contrats (licences logicielles, contrats de maintenance, etc.) doivent être stockés de manière sûre. Cela s'entend comme un stockage dans des armoires ignifugées et fermées à clé pour l'administration centrale.

En cas de difficulté de mise en œuvre de cette exigence, un duplicata du contrat original pourra être systématiquement stocké sur un site différent dans une armoire fermée à clé.

EXG_PHY_010 **La libre circulation des personnes externes est interdite dans les locaux du ministère et chaque bâtiment doit filtrer la circulation des visiteurs dès l'accueil de la structure, où ceux-ci seront pris en charge par un agent désigné.**

La présente PSSI s'applique aux locaux dont dispose le ministère au sein d'un bâtiment hors de son contrôle.

Cette exigence ne s'applique pas dans les établissements d'enseignement, car ceux-ci accueillent des personnes extérieures. Cette exigence ne pouvant s'appliquer pleinement, il est tout de même souhaitable de la mettre en œuvre en tant que de possible sur les parties des locaux qui hébergent le personnel administratif et des salles informatiques qui hébergent les informations sensibles et applications critiques.

EXG_PHY_011 **Chaque site du ministère doit faire état, en fonction des cas, au maximum de cinq catégories de zones de circulation définies par cette exigence. Les locaux dont dispose le ministère dans des bâtiments hors de son contrôle ainsi que les établissements publics d'enseignement doivent se conformer à cette exigence.**

Les zones sont classées suivant les catégories suivantes :

- Z0 : Zone où sont localisés les bâtiments. Il s'agit en général du site dans son ensemble ;
- Z1 : Zone d'un bâtiment permettant de recevoir du public (hall, salles de réunions, salles de formation sans matériel informatique, etc) ;
- Z2 : Zone interdite au public en grand nombre et autorisée aux membres du personnel ainsi qu'au public isolé ou en petit nombre (bureaux des membres du personnel, salles de formation, salles de réunions internes, salles informatiques hébergeant des informations non sensibles et non critiques) ;
- Z3 : Zone restreinte aux seuls membres du personnel habilités (bureaux sensibles) ;
- Z4 : Zone dédiée à la protection des infrastructures critiques du système d'information (salles informatiques).

Les zones Z0, et Z1 doivent disposer de zones tampons, clairement délimitées, permettant de maîtriser le flux de visiteurs externes.

EXG_PHY_012 Chaque responsable de site décrit dans un document *ad hoc* les différentes zones définies sur le site concerné. Le document est préalablement transmis pour validation à l'AQSSI correspondant.

EXG_PHY_013 Les bureaux et salles de réunions propres aux agents seront localisés dans la zone Z2. Ils seront fermés en l'absence de leur occupant.

EXG_PHY_014 Les bureaux des agents responsables de l'exploitation des systèmes d'information et particulièrement ceux des équipes qui gèrent des équipements de sécurité doivent être systématiquement verrouillés en l'absence de leurs occupants.

EXG_PHY_015 Les zones Z3 et Z4 doivent disposer d'armoires fortes permettant de stocker de manière sécurisée les documents ou composants de niveau C3 ou plus lorsqu'ils ne sont pas utilisés par les agents.

EXG_PHY_016 Les supports de sauvegarde dédiés aux informations critiques du ministère doivent être protégés contre les risques de destruction, de divulgation et de vol. Ainsi, ces supports doivent être stockés dans des armoires ignifugées et fermées à clef.

L'externalisation périodique, hebdomadaire ou journalière, de ces supports de sauvegarde doit être mise en œuvre pour les systèmes qui sont inscrits dans le plan de continuité d'activité.

EXG_PHY_017 Le matériel de reprise de l'activité en cas de sinistre, lorsqu'il existe, doit être

localisé à l'extérieur du site hébergeant les serveurs de production habituels.

EXG_PHY_018 Pour tout centre de production, une zone de livraison et de chargement depuis l'extérieur du bâtiment sera limitée au seul personnel identifié et autorisé.

La zone de livraison et de chargement doit être conçue de manière à ce que les fournitures puissent être déchargées sans que les livreurs aient accès à d'autres parties du bâtiment.

Dans la mesure du possible, les portes extérieures d'une zone de livraison et de chargement doivent être sécurisées lorsque les portes intérieures sont ouvertes.

2.7 Exploitation des systèmes

2.7.1 Procédures et responsabilités opérationnelles

EXG_EXP_01 Toute procédure de sécurité doit être formalisée, mise à jour et contrôlée notamment les procédures de :

- Démarrage et d'arrêt des serveurs hébergés dans les salles informatiques (déroulé des opérations, intervenants autorisés) ;
- Sauvegarde des serveurs (fréquence, test de restauration, stockage des médias de sauvegarde) ;
- Maintenance des serveurs (durée, modalité d'intervention, intervenants autorisés) ;
- Gestion de la salle informatique (localisation des équipements, contrôle des dispositifs de protection).

EXG_EXP_02 **Les modifications apportées aux équipements et aux systèmes du ministère doivent suivre une procédure formalisée incluant des tests de non-régression, des tests de sécurité, une mise à jour des procédures de sauvegardes.**

Toute modification majeure sur une application critique fera l'objet d'une sauvegarde préalable permettant le retour arrière en cas de dysfonctionnement après modification.

Lorsqu'elles sont disponibles, les solutions labellisées par l'ANSSI de produits ou services de sécurité sont recommandées.

EXG_EXP_03 Le processus de modification des systèmes est porté par plusieurs acteurs dont les rôles et responsabilités doivent s'appuyer sur le principe de séparation des fonctions. Au minimum :

- La MOA décide des modifications à apporter sur un système ;
- La MOE valide la faisabilité et la non régression technique et fonctionnelle des modifications ;
- Le SDSI valide la mise en production des applications hébergées par le centre de production du ministère ; Dans le cas de la prise en charge par des centres de production tiers, le SDSI est informé de la mise en production et valide l'interconnexion éventuelle du système avec les SI du MAAF ;
- La MOA, avec le soutien éventuel de la MSSI, valide la non-régression en termes de protection des SI en réalisant le cas échéant un audit incluant la recherche de nouvelles vulnérabilités.

EXG_EXP_04 Les équipements de développement, de test et de production doivent être physiquement distincts.

Aucune modification ne sera réalisée sur une plate-forme de production sans tests préalables.

Le développement, les tests et la gestion de la production des applications exploitées seront confiées à des équipes distinctes.

Chaque équipe est responsable de la formalisation et la mise en œuvre des mesures de sécurité implicites induites par les besoins de sécurité exprimées par les MOA.

EXG_EXP_05 Les mesures de protection appliquées aux plate-formes de développement, de test et de production doivent être homogènes, au minimum en termes de contrôle d'accès, mises à jour de sécurité appliquées et suppression des comptes par défaut.

EXG_EXP_06 Dans le cas général, aucune donnée sensible ne doit être utilisée sur une plate-forme de développement, *a fortiori* les données à caractère personnel.

Si, pour des raisons techniques ou fonctionnelles et légitimes, de telles données sont néanmoins indispensables, la MOA et la SDSI formalisent cette dérogation en précisant les règles particulières de sécurité applicables.

2.7.2 Gestion des changements

EXG_EXP_07 La procédure de validation par le service en charge de la sécurité opérationnelle d'un système doit être formalisée. Celle-ci doit intégrer au minimum :

- Les capacités réseaux nécessaires au bon fonctionnement du système ;
- Les besoins de protection du système et les mesures effectives mises en place (paramétrage, patch, cloisonnement, …).

EXG_EXP_08 **La MOA doit approuver tout changement sur une application dont elle a la charge sur dossier instruit par la MOE.**

L'approbation doit être conditionnée au minimum à l'établissement par la MOE ou le Centre de Production de :

- La mise à jour des documentations associées :
- Procédures d'exploitation ;
  - Procédures de sauvegardes et de restaurations testées,
  - Procédures d'utilisation ;
- L'application des mises à jour de sécurité ;

- L'intégration ou la mise à jour des plans de secours et de continuité ;
- La mise à jour de l'analyse de risque indiquant explicitement aucun risque majeur ou critique non couvert pour le système d'information du ministère.

2.7.3 Virus et codes malveillants

EXG_EXP_09 **Les serveurs de fichiers et les postes de travail des utilisateurs doivent être équipés d'un antivirus mis à jour régulièrement fourni par le ministère (AC, Directions, DRAAF et DAAF).**

EXG_EXP_010 **Un contrôle antivirus doit être effectué sur les médias (CD-ROM, support USB, fichier téléchargé).**

EXG_EXP_011 Tout agent doit faire attention aux contenus qu'il consulte, notamment aux regards des virus, fichiers corrompus, mouchards, *spywares*, etc. Ce contrôle de l'utilisateur doit être accru au moment de la réception de courriels non sollicités ou douteux.

Aucun agent ne doit faire suivre des alertes antivirus reçues de l'extérieur.

En cas de doute, il doit contacter son responsable informatique de proximité et le cas échéant, pour l'administration centrale ou les services déconcentrés, le service en charge de la sécurité opérationnelle.

Sous l'égide de la SDSI, seuls le service en charge de la sécurité opérationnelle et la MSSI sont compétents pour faire suivre des vulnérabilités identifiées.

EXG_EXP_012 Seuls les correctifs antivirus ou système mis à disposition par la SDSI ou le service en charge de la sécurité opérationnelle peuvent être appliqués sur les postes de travail.

La procédure de mise à jour doit être quotidienne, automatique et transparente pour l'utilisateur.

Les postes nomades pourront être configurés pour se mettre à jour directement sur les sites des éditeurs de solutions antivirales ou de suite bureautique.

EXG_EXP_013 Le service en charge de la sécurité opérationnelle doit disposer des outils et moyens nécessaires pour éradiquer les nouveaux virus.

En situation de crise opérationnelle et sur feu vert du SDSI, le service en charge de la sécurité opérationnelle doit pouvoir isoler tout ou partie du réseau du ministère.

La procédure d'éradication doit être formalisée par le service en charge de la sécurité opérationnelle et la MSSI, validée par le SDSI.

EXG_EXP_014 En aucun cas, un système de protection contre les codes malveillants ne doit être désactivé sur l'initiative seule d'un utilisateur.

L'accès au paramétrage est limité à la mise à jour manuelle de la base de signature et au déclenchement d'une analyse du poste de travail.

EXG_EXP_015 Les logiciels de détection de codes malveillants installés sur les postes de travail doivent intégrer au minimum :

- L'analyse des courriers électroniques ;
- L'analyse des téléchargements ;
- L'analyse des pages web visitées ;
- L'analyse de tout dispositif amovible connecté au poste de travail ;
- L'analyse du dépôt de fichier sur l'environnement de travail.

EXG_EXP_016 Une configuration sécurisée du navigateur formalisée est distribuée sur les postes de travail. Celle-ci inclut :

- La désactivation des contrôles « activeX » non signés ;
- L'installation le plus rapidement possible des mises à jour de sécurité critiques pour les navigateurs et machines virtuelles recommandés par les constructeurs ;
- L'installation au plus tôt des mises à jour de sécurité non-critiques et/ou globales pour les logiciels ;
- L'activation d'une mesure, tel un module complémentaire, obligeant l'utilisation par défaut de la version chiffrée d'un site internet (*https*).

EXG_EXP_017 Pour analyse anti-virale des serveurs bureautiques et de production, il est possible d'employer une technologie différente de celle des postes de travail (utilisation de logiciels d'éditeurs ou de communautés différents) avec l'accord du ministère (MSSI/FSSI).

2.7.4 Gestion des traces

EXG_EXP_018 **Une configuration permettant de minimiser les traces laissées sur l'internet à la connaissance de sites et personnes tiers, souvent commerciaux, est mise en place. Cette configuration n'empêche en revanche pas la conduite d'une investigation légitime.**

Cette configuration inclut :

- L'interdiction des témoins de traçage (*cookies*) tiers n'ayant pas de stratégie de confidentialité ;
- Lorsque le navigateur le permet, l'activation de l'option « Dire de ne pas me pister » (*Do not track*) ;
- La possibilité pour l'utilisateur d'installer des modules

complémentaires permettant :

- Le blocage des publicités, réclames, fenêtres intruses non-sollicitées et n'ayant aucun lien avec l'activité de l'agent ;
- Le blocage des méthodes traçant l'utilisateur, sans sollicitation de sa part et n'ayant aucun lien avec l'activité de l'agent ;
- Le blocage des scripts, objets flash ou autres qui ne sont pas déjà bloqués par défaut.

EXG_EXP_019 Les fichiers temporaires du poste de travail, parce qu'ils peuvent permettre la consultation de données sensibles par des personnes non-autorisées, doivent être fréquemment effacés.

Sur les supports mobiles (tablettes, téléphones, etc.), la mise en cache de documents, courriels, etc. doit être limitée dans le temps de façon à ce que ne se trouvent sur l'appareil que les informations strictement nécessaires.

2.7.5 Gestion des usages déportés (*Cloud computing*) et de la consumérisation des usages (BYOD)

EXG_EXP_020 **L'utilisation de services tiers pour déporter sur un serveur distant, externe au ministère ou à l'administration française, des données ou des ressources dans un but de stockage ou de traitement informatique est interdite.**

Cette interdiction vise à empêcher les usages de *cloud computing*, ou informatique en nuage, c'est-à-dire notamment le simple stockage de données en ligne mais aussi les services de Logiciel en tant que service (bureautique en ligne par exemple) (*SaaS*), d'Infrastructure en tant que service (*IaaS*) ou de Plate-forme en tant que service (*PaaS*).

L'un de ces usages pourra être autorisé par un accord écrit et motivé de la MSSI et à la condition que ledit usage soit nécessaire pour la réalisation d'une des missions du ministère.

Par exception, un service de stockage en ligne pourra être utilisé par un agent, si les éléments suivants sont réunis. Par stockage en ligne, on entend exclusivement les systèmes de type « disque distant » à l'exclusion de ceux proposant d'autres services tels des applications bureautiques distantes.

- **Tout fichier transféré doit être chiffré avec l'un des outils mis à disposition par le ministère ;**
- **Tout chiffrement doit être protégé par un mot de passe fort, c'est-à-dire conforme aux exigences minimales dont dispose la présente PSSI (cf. « Identification et contrôle d'accès logique ») ;**

- **L'agent doit utiliser un compte ouvert auprès du prestataire de stockage en ligne spécialement pour son activité professionnelle et ne doit pas utiliser ce même compte pour son usage personnel ;**
- **Lorsque c'est possible, l'identifiant du compte de stockage en ligne ne doit pas permettre d'identifier l'agent et son activité (par exemple par une suite aléatoire de chiffres et de lettres) ;**
- **Le mot de passe du compte de stockage en ligne doit être conforme aux exigences minimales dont dispose la présente PSSI (cf. « Identification et contrôle d'accès logique ») :**
- **Le fichier transféré ne pourra être de niveau C2 ou plus et le nom de ce fichier ne doit pas donner d'information sensible sur son contenu ;**
- **L'utilisateur privilégie les prestataires de service de stockage en ligne dont les serveurs sont situés au sein de l'Union européenne.**

EXG_EXP_021

La connexion d'un équipement personnel (ordinateur, support USB, CD-ROM, etc.) appartenant à un agent à un équipement professionnel ou au réseau du ministère est strictement interdit.

On entend par connexion au réseau toute connexion utilisant un câble réseau (filaire) ou un système sans fil de type Wi-Fi.

Cette interdiction vise à proscrire la consumérisation des usages : un agent ne peut donc connecter ses équipements personnels à ses équipements professionnels. La consumération des usages vise notamment le *BYOD* (*Bring your own device*) ou AVEC (Apportez Vos Équipements personnels de Communication).

L'usage des équipements personnels est par exception autorisé pour un usage professionnel, et ce uniquement dans le cadre de la consultation de la messagerie et des outils collaboratifs connexes si les conditions suivantes sont réunies :

- **L'équipement personnel ne se connecte pas directement ou indirectement au réseau du ministère ;**
- **De manière à assurer la sécurité des données transférées, l'équipement personnel respecte les exigences de sécurité minimale suivantes :**
  - **La connexion est authentifiée via certificat électronique,**
  - **Le système d'exploitation est à jour,**

- **Le pare-feu et l'antivirus sont à jour,**
- **L'utilisation de l'équipement personnel respecte les normes en vigueur (contrat de travail, lois, règlement intérieur, etc.),**
- **L'équipement personnel respecte les normes de sécurité minimales de cette PSSI, notamment concernant les mots de passe.**
- **Dans le cadre d'un équipement mobile (téléphone, tablette), il conviendra de se conformer aux usages mobiles de la présente PSSI.**

EXG_EXP_022 Des dérogations aux deux exigences précédentes, explicites et documentées peuvent être accordées après avis conforme de l'équipe informatique de proximité compétente et transmise au RSSI ou à l'ASSI.

La dérogation emporte exclusion de responsabilité de la part du ministère (y compris en cas d'intervention technique assurée par un agent de l'équipe informatique de proximité), mais souligne par contre la responsabilité de l'utilisateur en cas de problème avéré de sécurité. Dans cette situation, les règles de la PSSI-Agriculture continuent à s'appliquer (par exemple, l'obligation du traitement antiviral ou du chiffrement des documents sensibles)

2.7.6 Gestion des configurations

EXG_EXP_023 **Les postes de travail et serveurs disposeront d'un socle technique standard.**

Ce socle comprend les principes suivants :

- La version d'utilisation du système est maintenue par le constructeur ou un service tiers et n'est pas inférieure à deux versions majeures de la version en cours ;
- Les mises à jour sécurité sont appliquées. Une procédure automatique et transparente pour l'utilisateur doit permettre au poste de travail d'être régulièrement, au minimum une fois par mois, mis à jour ;
- Une procédure doit être formalisée et appliquée pour tout serveur en production ;
- Les services inutiles sont désactivés ou désinstallés ;
- Les comptes par défaut sont supprimés ou renommés ;
- Les exécutions automatiques à partir des interfaces de communications sont interdites ;
- Les configurations en production sont archivées et documentées.

EXG_EXP_024 Les configurations des équipements de réseau et de téléphonie en production doivent être archivées et documentées.

EXG_EXP_025 L'installation et l'utilisation de logiciels, sur le réseau du ministère, non autorisés sur un poste de travail normalisé par la SDSI, est interdite.

EXG_EXP_026 Les points d'accès à l'internet sont limités au strict nécessaire pour assurer les missions du ministère.

Aucun compte d'administration ne pourra être utilisé pour accéder à l'internet.

EXG_EXP_027 Tout poste de travail ou serveur utilisant ou stockant de l'information d'un niveau C2 ou supérieur doit disposer d'une partition chiffrée dédiée à cet effet.

EXG_EXP_028 **Tout agent utilisant ou stockant de l'information d'un niveau C3 ou supérieur peut obtenir un poste de travail sécurisé et chiffré.**

2.7.7 Sauvegardes

EXG_EXP_029 **Chaque serveur du système d'information du ministère doit disposer d'une procédure de sauvegarde adaptée et conforme aux besoins exprimés par les maîtrises d'ouvrages.**

EXG_EXP_030 Les procédures de sauvegarde doivent suivre les règles suivantes :

- Ces sauvegardes doivent être réalisées selon les règles édictées par le Plan de continuité de l'activité du Centre de Production ou celui du ministère ;
- L'exécution de la sauvegarde doit être compatible avec le niveau de disponibilité des applications définie par la MOA ;
- Un média de sauvegarde de type bande magnétique ne doit pas être réutilisé avant sept jours pleins ;
- La dotation en média d'un site doit lui permettre d'assurer au minimum deux semaines à venir de sauvegarde ;
- En cas d'échec de sauvegarde automatique sur deux jours consécutifs, une sauvegarde doit être déclenchée manuellement par le service en charge de l'exploitation des serveurs.

EXG_EXP_031 Les procédures de sauvegarde ne concernent que les serveurs de production et bureautiques du ministère, cependant des espaces de stockage réseau seront mis à disposition des agents pour qu'ils puissent procéder à des sauvegardes pour les données traitées en local sur leurs postes de travail.

Si un document ou une information ne peut être sauvegardée dans le réseau du fait de son niveau de confidentialité, elle sera sauvegardée sur le poste de travail de l'utilisateur.

Les informations de niveau C3 et supérieur seront sauvegardées chiffrées.

Chaque agent est responsable de la sécurité des documents qu'il est amené à gérer. Si les équipes techniques mettent à disposition des moyens destinées au sauvegardes, il est de la responsabilité de chacun de veiller à l'utilisation effective de ceux-ci.

EXG_EXP_032 Chaque média de sauvegarde d'un composant du système d'information doit être identifié. Il doit être étiqueté au minimum avec le nom de la machine sauvegardée et un numéro de série unique.

Chaque média de sauvegarde des applications et données correspondant aux services estimés comme D3 ou plus, ou I3 ou plus, C3 ou plus, ou P3 ou plus, doit être stocké dans une armoire ignifugée et fermée à clef.

Cette armoire ne doit pas être dans le même local que les serveurs. Il est recommandé d'étendre l'application de cette mesure aux autres composants du

système d'information.

EXG_EXP_033 Les sauvegardes doivent être testées régulièrement afin de garantir la capacité de restituer l'environnement complet d'un composant du système d'information du ministère, particulièrement les applications estimées comme critiques pour les directions.

Avant la mise en production d'un nouveau système, le plan de sauvegarde doit être testé sur le nouveau composant afin de garantir la reprise des données suite à un incident potentiel.

EXG_EXP_034 Toute procédure de sauvegarde doit être revue et le cas échéant mise à jour à chaque changement de contexte d'exploitation, à chaque création ou modification d'une fonctionnalité sur l'un des composants techniques ou applicatif du SI.

Cette mise à jour inclut les tests de restauration qui doivent permettre de valider les changements effectués dans la procédure de sauvegarde.

EXG_EXP_035 Les demandes de récupération de données sauvegardées doivent faire l'objet d'une procédure de contrôle strict afin de garantir que toute demande de restauration d'une donnée est faite sous contrôle de la personne propriétaire de l'information et que cette demande est autorisée.

EXG_EXP_036 Un service d'archivage électronique sécurisé sera mis en place au sein du ministère.

La maîtrise d'ouvrage, en collaboration avec le service des archives, doit déterminer les données pour lesquelles il existe des contraintes légales, techniques, ou opérationnelles d'archivage (format, durée de stockage, …).

L'archivage privilégie l'utilisation d'un coffre-fort électronique.

Les moyens et infrastructures nécessaires à la consultation des données doivent être disponibles.

Les contraintes légales concernant l'archivage électronique doivent être satisfaites.

2.7.8 Gestion de la sécurité de réseau

EXG_EXP_037 **Le réseau des administrateurs techniques des systèmes d'information doit être cloisonné vis-à-vis du réseau principal afin de protéger les postes de travail de ces administrateurs.**

Les administrateurs ont deux postes de travail distincts, l'un avec accès à l'internet et un compte non privilégié, et l'autre sans accès à l'internet mais avec le compte d'administrateur.

Dans la mesure du possible, l'usage de comptes disposant de privilèges étendus (notamment le compte *root*) est proscrit, notamment lors d'une connexion à distance. Si l'usage d'un tel compte est nécessaire, toutes les actions devront être tracées nominativement et le mot de passe afférent devra être scindé et détenu par *n* personnes appartenant à *n* services différents.

L'habilitation des administrateurs s'effectue selon une procédure validée par l'autorité d'homologation. Le nombre de personnes habilitées pour des opérations d'administration doit être connu et validé par l'autorité d'homologation.

EXG_EXP_038 Les flux d'administration des systèmes d'information seront chiffrés sur le réseau. Si le chiffrement est impossible, l'administration sur les équipements critiques devra se faire directement sur l'équipement.

EXG_EXP_039 Tout contrat avec un fournisseur de services de télécommunication (opérateur réseau) doit exposer comment le fournisseur répond au besoin de sécurité exprimé par la MOA responsable du contrat. Ce besoin de sécurité est exprimé suivant les critères classiques de Disponibilité, Confidentialité, Intégrité et Preuve.

L'expression du besoin sera dans tous les cas définie par la MOA responsable du contrat en cohérence avec le besoin défini par les maîtrises d'ouvrage des différents systèmes d'information qui sont supportés par ce réseau.

La capacité des liaisons principales et de secours si nécessaire, la capacité à basculer sur des lignes de secours, le délai de retour en service régulier après incident, le niveau de protection vis-à-vis de l'intrusion et de l'écoute externe seront formellement définies par contrat.

EXG_EXP_040 Tout raccordement à un réseau extérieur nécessite l'approbation du SDSI. Celui-ci doit obligatoirement utiliser les moyens d'accès mis à disposition par la SDSI ou validés formellement par le SDSI.

Tout matériel ayant un accès non autorisé à un réseau externe implique le non-raccordement de celui-ci au réseau du ministère.

2.7.9 Gestion des supports ou documents de sécurité

EXG_EXP_041 **La mise à jour régulière de la documentation de sécurité est réalisée à chaque évolution significative du système d'information.**

La reproduction et la destruction de la documentation sont effectuées sur ordre de l'AQSSI qui vérifie que l'opération porte sur la totalité des documents désignés et n'affecte qu'eux seuls.

La documentation sécurité, intégrant des informations de nature à préciser les configurations des équipements de sécurité, les stratégies d'adressage, les localisations physiques des serveurs sensibles, etc. doit être systématiquement classifiée au minimum C3.

De manière générale, les documents d'application de la documentation sécurité sont classifiés au minimum C2.

EXG_EXP_042 Tout document de sécurité ou d'application doit faire apparaître le niveau de confidentialité de son contenu conformément aux exigences de la PSSI-Agriculture.

EXG_EXP_043 La maintenance des documents de sécurité est placée sous la responsabilité du SDSI et déléguée à la MSSI.

La documentation de sécurité doit être mise à jour à chaque fois que des modifications sur le système d'information le justifient, au minimum, dès lors :

- Du changement de la stratégie sécurité ;
- De la mise en place de nouvelles fonctionnalités sur le système d'information ;
- D'un incident de sécurité révélant des failles dans la gestion de la sécurité du système d'information du ministère.

EXG_EXP_044 Le contenu d'un support de type disque dur extractible ou externe qu'un service ne souhaite pas conserver doit être rendu irrécupérable.

EXG_EXP_045 Les supports (Disques durs, CD, DVD, support USB, etc.) contenant des informations sensibles doivent être stockés et mis au rebut de manière sécurisée suivant les préconisations de l'ANSSI.

La mise au rebut doit se faire par incinération, déchiquetage ou effacement des données.

EXG_EXP_046 La liste des suppressions de support ou d'équipement doit être conservée par le service opérant la suppression à des fins d'audit par le SDSI au minimum pendant 10 ans.

EXG_EXP_047 Avant la mise en exploitation d'un système, la MOA doit, en lien avec sa MOE, définir la liste des éléments susceptibles de nécessiter une mise au rebut sécurisée.

2.7.10 Échange d'information

EXG_EXP_048 **Toute transmission d'information de niveau C3 ou plus sera chiffrée.**

Si le destinataire de cette transmission d'information de niveau C3 est une personne externe au service émetteur, elle sera soumise à l'autorisation du responsable de l'information et de l'AQSSI sous la responsabilité duquel l'information a été créée.

EXG_EXP_049 **Les supports amovibles ou mobiles (supports USB, CD, DVD, disquettes, téléphones, tablettes, etc.) pourront servir de média d'échange sous conditions qu'elles respectent les mesures de protection adaptées au niveau de classification correspondant.**

L'utilisation de supports USB, téléphones ou tablettes comme support de stockage permanent est interdit.

EXG_EXP_050 **Il est interdit de laisser des informations sur des appareils d'impression (photocopieurs, imprimantes, télécopieurs, etc.) ; il faut les retirer dès que c'est possible, au mieux à la fin de l'impression.**

Il est interdit de laisser des informations C2 ou plus visibles dans les bureaux ou locaux du ministère auxquels des personnes non autorisées peuvent accéder, notamment après les heures du travail d'un agent.

EXG_EXP_051 Pour les services utilisant des informations C3 ou plus régulièrement, un dispositif d'impression sécurisé sera mis à disposition.

2.7.11 Publication de l'information

EXG_EXP_052 **La publication d'information sur l'internet ou par tout moyen de communication au public ne concerne que des informations de niveau C0.**

Ainsi, toute information de niveau C1 ou supérieur ne doit en aucun cas être publiée. Cette mesure d'applique à tous et dans tous les cas, notamment sur les réseaux et médias sociaux.

Ces prescriptions ne s'opposent cependant pas à la communication des documents, notamment lorsque cette communication s'inscrit dans le cadre d'une demande formelle au titre, par exemple, de la loi 78-753 sur la communication des documents administratifs.

EXG_EXP_053 Toute publication d'information doit respecter les normes en vigueur. Tout agent du ministère est tenu à une obligation de loyauté envers son employeur, ce qui s'apparente à un devoir de fidélité et de discrétion.

EXG_EXP_054 Les systèmes d'information qui permettent la publication d'information sur l'internet devront bénéficier de mises à jour de sécurité régulières, au minimum une fois par mois, et de protection d'accès et de détection

d'intrusion opérationnelle.

2.7.12 Surveillance

EXG_EXP_055 **Chaque système du ministère devra disposer d'une journalisation active permettant de tracer les événements sur une période au minimum égale à un mois glissant.**

EXG_EXP_056 Le système de gestion des journaux d'événement des serveurs et applications doit permettre de les archiver sur 12 mois glissants.

Cette règle doit s'appliquer à tous les composants d'infrastructure sauf justification de l'impossibilité de faire.

Cette règle ne s'applique pas aux postes de travail des agents.

EXG_EXP_057 Toute opération de maintenance ou de télémaintenance sur un poste de travail ou sur un serveur doit donner lieu à une journalisation de tous les événements induits (nom de l'intervenant, date et heure de l'intervention, actions menées, téléchargements effectués, données accédées, …).

EXG_EXP_058 Une surveillance active des points d'accès à l'internet est obligatoire, ainsi qu'une surveillance des composants critiques ou sensibles isolés et protégés sur le réseau.

Les mécanismes de journalisation et de traçabilité doivent permettre en cas d'intrusion réussie, ou de tentative d'intrusion, de disposer :

- Des éléments de traces permettant la meilleure identification possible des causes et origines de l'intrusion (remonter vers les éléments menaçants) ;
- Des éléments de traces suffisamment fiables pour permettre à l'autorité administrative ou judiciaire compétente de les accepter en tant que preuves de l'intrusion, de la tentative d'intrusion, ou de l'utilisation frauduleuse, en cas d'enquête.

EXG_EXP_059 Chaque journal d'événements doit recenser au minimum :

- Les échecs de connexion aux systèmes et aux applications ;
- Les échecs lors d'un accès à une ressource (fichier, objet, réseau, …) ;
- Les échecs lors de l'utilisation d'un privilège ;

- Les principaux événements systèmes ;
- La modification de paramètres de sécurité, d'un système ou de privilèges ;
- Le démarrage et l'arrêt d'un système ou d'une application ;
- Connexion et déconnexion ;
- Exécution de transactions sensibles ;
- La modification des comptes utilisateurs ou des groupes ;
- Prise de main à distance.

Pour chaque accès, il est recommandé d'identifier :

- L'auteur de l'événement ;
- La date et l'heure de l'événement correspondant ;
- les types d'événements ;
- les fichiers accédés ;
- les programmes ou les utilitaires utilisés.

EXG_EXP_060 Pour chaque application, il revient à la MOA et à l'AQSSI correspondant, de définir précisément,

- Les événements qui doivent être journalisés ;
- La durée de conservation de l'historique ;
- Les règles de gestion des fichiers historique ;
- Les règles de filtrage des événements conservés.

EXG_EXP_061 Il revient à la SDSI d'assurer :

- La télé-collecte sécurisée des traces de sécurité ;
- L'archivage des traces ;
- L'effacement des fichiers des traces obsolètes (Les règles relatives à la déclaration d'obsolescence et durée d'archivage doivent être fixées) ;
- Le filtrage et analyse des traces ;
- La protection des traces contre toute altération ou accès non autorisé ;
- L'alerte en cas de détection d'événements majeurs ;
- Le contrôle de l'intégrité des mécanismes de traces ;
- La destruction des traces au-delà du délai légal.

EXG_EXP_062 Afin de permettre leur présentation éventuelle devant une juridiction compétente, le recueil des éléments de preuve doit notamment respecter :

- le principe du respect de la vie privée ;
- le principe de proportionnalité et transparence ;
- le principe de la qualité et de l'exhaustivité de la preuve.

Le recueil de ces éléments doit s'opérer dans un cadre permettant de garantir la qualité, l'intégrité et la fiabilité des données considérées.

EXG_EXP_063 Un système de supervision de l'ensemble du réseau de l'administration centrale et des services déconcentrés adapté et efficace doit permettre de constater toute activité non autorisée.

Cela nécessite notamment :

- L'enregistrement et la corrélation de journaux d'événements ;
- La remontée automatisée d'alertes ;
- La synchronisation des horloges (indispensable pour la corrélation des journaux d'événements),
- Un système dédié pour l'enregistrement des journaux d'événements (serveur de journalisation) et séparé logiquement du reste du réseau.

Cette surveillance concerne tous les équipements réseaux ainsi que les points d'accès avec les réseaux tiers.

EXG_EXP_064 Les fichiers journaux des bases de données, des applications ou des systèmes d'exploitation ne doivent être supprimés qu'après avoir été sauvegardés.

2.8 Identification et contrôle d'accès logique

EXG_CAC_01

Tout utilisateur des systèmes d'information du ministère doit disposer d'un identifiant unique.

La définition de la stratégie de création de l'identifiant propre à chaque utilisateur relève de la responsabilité du SDSI.

EXG_CAC_02 Tout accès à un service applicatif traitant du C2 ou plus doit préalablement être soumis à une identification et authentification de l'utilisateur.

EXG_CAC_03 Lorsque le moyen d'authentification de l'utilisateur est le mot de passe, le contrôle et la connaissance de ce mot de passe doit rester sous la responsabilité exclusive de l'utilisateur.

Afin de garantir la robustesse du couple identifiant/authentifiant, les utilisateurs du SI doivent établir des mots de passe robustes en ce qui concerne leur authentifiant.

Un mot de passe est considéré comme robuste dès lors qu'il remplit les conditions suivantes :

- **Le mot de passe est composé de huit caractères choisis parmi au moins trois des quatre types de caractères (lettres majuscules, lettres minuscules, chiffres, caractères spéciaux) ;**
- **Le mot de passe est unique. Si un agent dispose de plusieurs comptes, un mot de passe différent doit être utilisé pour chacun d'eux ;**
- **Le mot de passe est difficile à deviner et facile à retenir. Ainsi, il faut impérativement éviter la répétition de termes ou de caractères, les mots communs (par exemple du dictionnaire), les prénoms et noms de personnes (l'utilisateur, ses relations ou des personnalités connues) et les informations personnelles (dates, numéros de carte bancaire, informations sensibles).**

En cas de contraintes particulières de sécurité, notamment concernant les administrateurs, le mot de passe devra impérativement être composé de dix caractères choisis dans les quatre types et sera changé tous les trois mois sans que le nouveau mot de passe ne puisse reprendre des groupes de caractères de l'ancien.

Les règles de robustesse des mots de passe seront actualisées en fonction des progrès techniques.

EXG_CAC_04 De manière détaillée, il est indispensable que tous les mots de passe respectent les règles ci-dessous :

- Il est formellement interdit de divulguer des mots de passe quels que soient le système et les circonstances ;
- Un utilisateur ne doit pas utiliser le compte d'un autre utilisateur pour accéder à des informations ou des applications ;
- Les utilisateurs doivent s'engager à conserver leur mot de passe confidentiel ;
- Le système sera paramétré de sorte à obliger l'utilisateur à modifier son mot de passe à la première connexion ou à l'expiration ;
- Les mots de passe ne doivent pas être visibles à l'écran durant la saisie ;
- Sauf impossibilité avérée, les mots de passe doivent être chiffrés (la plupart du temps, le chiffrement est géré automatiquement par le système) ;
- Les mots de passe ne doivent être conservés par écrit ;
- Les utilisateurs doivent avoir la possibilité de changer eux-mêmes leur mot de passe ;
- Les mots de passe doivent être traités comme des informations confidentielles C4 ;
- Les mots de passe doivent être modifiés dès que leur confidentialité peut être compromise, notamment en cas de perte ou vol de matériel ;
- La longueur minimale d'un mot de passe est de huit caractères, hors contraintes particulières de sécurité où elle est de dix caractères.
- Les mots de passe doivent être composés d'un mélange de caractères choisis parmi au moins trois des quatre types de caractères (lettres majuscules, lettres minuscules, chiffres, caractères spéciaux), hors contraintes particulières de sécurité où il est obligatoire d'utiliser les quatre types de caractères ;
- Un ancien mot de passe ne doit pas être réutilisable ;
- Un nouveau mot de passe ne doit pas réutiliser plus de trois caractères consécutifs du mot de passe précédent ;
- Les mots de passe temporaires doivent être changés à la première connexion ;
- Les mots de passe ne doivent pas être stockés dans un quelconque programme ou script permettant l'accès automatique à un service

applicatif du ministère ;

- Après installation d'une application ou d'un système, les mots de passe par défaut doivent être immédiatement modifiés ;
- Les mots de passe ne doivent pas apparaître de manière non-chiffrée dans des programmes, fichiers, traces, fichiers journaux ;
- Les mots de passe des comptes à privilèges élevés dont la perte pourrait rendre indisponible une application critique ou une information essentielle seront mis sous scellés et stockés dans un coffre sous contrôle adapté.

EXG_CAC_05 Des comptes nominatifs et des mots de passe individuels doivent être mis en place pour assurer la traçabilité des opérations et responsabiliser les utilisateurs.

Une liste des personnes autorisées doit être tenue à jour pour chaque système et chaque application. Une revue de cette liste est menée une fois par an pour chaque système par la MOA concernée.

Le libellé d'un compte utilisateur ne doit pas donner d'informations sur son niveau de privilèges ou de droits d'accès.

En dehors des comptes fonctionnels, l'utilisation de comptes génériques doit être limitée au strict minimum et ne pourra en aucun cas permettre d'accéder à des données de niveau C3 ou plus.

EXG_CAC_06 Les autorisations d'accès sur un serveur en production nécessitant des privilèges systèmes élevés données à un utilisateur doivent être justifiées par une activité de support, de maintenance ou d'administration des systèmes. Ces droits sont validés par le ou les AQSSI correspondants.

Les règles suivantes doivent être suivies pour donner ces autorisations à un utilisateur, à un administrateur ou à un tiers prestataire de service :

- Les accès privilégiés ne doivent être donnés qu'en vertu du strict besoin de la fonction ou de la mission ;
- Les privilèges associés aux logiciels de base (par exemple système d'exploitation, SGBD…) et les catégories de personnels qui y ont accès doivent être identifiés ;
- Les comptes privilégiés ne doivent pas être utilisés lorsque d'autres solutions de moindres privilèges sont possibles ;
- Autant que possible, des processus doivent être mis en œuvre pour minimiser l'utilisation des comptes privilégiés, et des comptes moins privilégiés doivent être utilisés pour l'activité quotidienne ;
- L'utilisation de ces comptes doit être auditée périodiquement, pour s'assurer que seules les personnes dont la fonction le justifie ont des accès privilégiés.

Sauf dérogation accordée par l'équipe informatique de proximité après avis conforme du RSSI ou de l'ASSI, l'utilisateur ne doit pas être administrateur de son poste de travail. Dans le cas exceptionnel où, pour des raisons

techniques, ces privilèges s'avéreraient indispensables à l'exécution des missions d'un agent, ceux-ci doivent alors, dans toute la mesure du possible, être associés à un compte local au poste de travail habituel de l'utilisateur concerné, qui doit s'astreindre à utiliser son compte nominal (non privilégié) tant que le recours aux privilèges élevées n'est pas strictement indispensable.

EXG_CAC_07

Les autorisations d'accès sur un serveur en production nécessitant les privilèges les plus étendus et donnant toutes les permissions (*root*) données à un utilisateur doivent être justifiées par une activité de support, de maintenance ou d'administration des systèmes. Ces droits sont validés par le ou les AQSSI correspondants ainsi que par la MSSI.

Un accès avec privilège élevé ou maximal ne doit en aucun cas être utilisé par un script ou un code applicatif.

En sus des règles ci-dessus devant être suivies pour l'octroi de privilèges, les règles suivantes doivent être suivies pour donner ces autorisations à un utilisateur, à un administrateur ou à un tiers prestataire de service :

- Les accès donnant toutes les permissions ne doivent être donnés qu'en vertu du strict besoin de la mission et pour une durée strictement limitée à l'exercice de celle-ci ;
- À l'issue de cette durée, les accès donnant toutes les permissions seront automatiquement révoqués ;
- Les accès donnant toutes les permissions ainsi que les actions effectuées avec ceux-ci doivent faire l'objet d'une journalisation, laquelle donne lieu à un audit effectué chaque année par la MSSI.

EXG_CAC_08 Un inventaire exhaustif des comptes privilégiés reprend :

- Les utilisateurs disposant d'un compte administrateurs (ou de privilèges supérieurs à ceux d'un utilisateur standard) sur le système d'information ;
- Des utilisateurs disposant de privilèges assez élevés pour accéder aux répertoires de travail des dirigeants ou de l'ensemble des utilisateurs ;
- Des utilisateurs disposant d'un poste non administré par le service informatique.

Cet inventaire doit être à jour et revu une fois par an.

EXG_CAC_09 La MOA définit la politique d'habilitation relative au système dont elle a la charge. Cette politique doit définir, le cas échéant, les possibilités de délégation. Par défaut, toute délégation est interdite. La politique d'habilitation doit être validée par l'AQSSI concerné.

Lorsqu'un système permet de mettre en œuvre des procédures de délégation, des moyens sont mis en œuvre pour tracer les accès aux informations de

manière à identifier le délégant et le délégataire.

Le niveau de protection de l'information mis à disposition du délégataire doit être au moins équivalent au niveau de protection mis à disposition du délégant.

Concernant l'accès à des informations sensibles, la demande de délégation sera visée et accordée par l'AQSSI de la direction concernée sauf disposition contraire définie dans la politique d'habilitation.

Les propriétaires d'information (les délégants) restent responsables de la protection des informations accessibles par le ou les délégataires sauf disposition contraire définie dans la politique d'habilitation.

La procédure de délégation, lorsqu'elle existe doit être formalisée et doit préciser nominativement les délégataires, la durée de la délégation accordée et les actions autorisées par la délégation.

EXG_CAC_010 Les informations d'authentification doivent être stockées de façon telle qu'elles soient seulement accessibles pour consultation ou modification par des utilisateurs autorisés.

EXG_CAC_011 L'identification et l'authentification doivent être traitées à travers un chemin de confiance entre l'utilisateur et le système initialisé par l'utilisateur.

Les informations d'identification et d'authentification ne doivent pas être transmises en clair sur le réseau du ministère ni ne doivent être conservées en clair sur un poste ou un serveur

EXG_CAC_012 Des moyens techniques sont mis en place afin de faire respecter les règles relatives à l'identification et l'authentification.

Ces moyens techniques permettent au minimum de :

- Bloquer les comptes administrateurs ou privilégiés tous les six mois tant que le mot de passe n'a pas été changé ;
- Bloquer toute connexion à un poste qui permettrait de se connecter sans mot de passe ou en session « Invité » ;
- Vérifier que les mots de passe respectent la politique des mots de passe ci-avant énoncée, notamment quant à leur robustesse (à défaut un contrôle périodique des paramètres techniques relatifs aux mots de passe est effectué) ;
- Bloquer l'utilisation des équipements (routeurs, serveurs, imprimantes, etc.) qui ont des éléments d'authentification par défaut tant que le mot de passe n'a pas été changé.

EXG_CAC_013 **L'utilisation des certificats électroniques respecte les politiques de certification de l'IGC du ministère publiées sur le site**

http://igc.agriculture.gouv.fr.

L'utilisation des certificats, fortement encouragée, est à préférer à celle du couple « utilisateur/mot de passe ».

EXG_CAC_014 Les responsables d'exploitation pour les comptes systèmes, les responsables informatique de proximité pour les comptes bureautiques, les MOA pour les applications doivent suspendre tous les droits d'accès d'un utilisateur immédiatement après un changement de poste ou d'emploi ou après son départ du ministère (cf. notamment l'exigence EXG_SRH_09).

EXG_CAC_015 **Tout accès aux informations de niveau C2 ou plus, qu'elles soient sur un support physique ou informatique, doit être protégé.**

De manière détaillée, le principe du « bureau net » doit être appliqué, à savoir :

- Les informations sur papier de niveau C2 ou plus doivent être mises sous clé lorsqu'elles ne sont pas utilisées, et plus particulièrement lorsque le bureau est sans occupant ;
- Les postes informatiques et autres supports informatiques (clés USB, disques amovibles, etc.) contenant des informations de niveau C2 ou plus doivent être mis sous clé lorsque le bureau est sans occupant ;
- les sessions sur les ordinateurs et les terminaux doivent être fermées ou protégées par un dispositif de verrouillage de l'écran et du clavier contrôlé par un authentifiant, lorsque ces appareils sont laissés sans surveillance ;

L'accès aux points d'entrée et de sortie du courrier doit être restreint.

Tous les documents doivent être enlevés des imprimantes et photocopieurs immédiatement après leur impression. Les documents laissés dans les imprimantes et photocopieurs en dehors des heures de travail doivent être détruits.

EXG_CAC_016 La politique d'accès doit respecter le principe selon lequel tout ce qui n'est pas autorisé est interdit.

Les droits d'accès d'un utilisateur sont fondés sur le « besoin d'en connaître » lié à sa fonction.

Les droits d'accès d'un utilisateur doivent être fondés sur le principe « du moindre privilège » nécessaire à la réalisation de l'activité quotidienne.

Lors d'un changement de fonction, les comptes d'un utilisateur doivent être modifiés pour lui donner les droits d'accès correspondant à sa nouvelle fonction.

EXG_CAC_017 Tout accès à une information de niveau C2 depuis le réseau privé du ministère ou un réseau tiers doit au minimum reposer sur :

- L'identification par identifiant – mot de passe ;
- Le chiffrement de la session d'identification – authentification.

Tout accès à une information de niveau C3 via le réseau privé du ministère ou un réseau tiers doit au minimum reposer sur :

- L'identification par identifiant – mot de passe ;
- L'authentification du serveur ;
- Le chiffrement de l'ensemble de la session entre le poste et le réseau du ministère lorsque l'accès se fait à partir d'un réseau tiers.

Tout accès à une information de niveau C4 via le réseau privé du ministère ou un réseau tiers doit au minimum reposer sur :

- L'authentification forte de l'utilisateur via certificat électronique ;
- Le chiffrement de l'ensemble de la session entre le poste et le serveur permettant l'accès à cette information ;
- La présence d'un dispositif anti-intrusion et anti-rebond sur le poste client ;
- Un dispositif de protection virale à jour sur le poste client.

Les MOA peuvent renforcer ces dispositions dans le cadre de la politique de sécurité des applications dont elles ont la charge.

EXG_CAC_018 Tout accès distant (en particulier en mode administrateur) sur un poste utilisateur ne peut se faire sans l'accord explicite de l'utilisateur au moment de cet accès.

Tout utilisateur autorisé à accéder à distance doit s'authentifier sur le réseau en utilisant en respectant les règles d'authentification de la présente PSSI.

EXG_CAC_019 En cas de télé-assistance (ou prise de main à distance), les règles suivantes doivent être respectées :

- L'opération de télé-assistance s'effectue avec le consentement de l'utilisateur sans qu'il n'ait à communiquer son mot de passe au télé-assistant ;
- L'opération de télé-assistance s'effectue de manière visuelle par affichage partagé entre l'utilisateur et le télé-assistant ;
- L'authentification des télé-assistants doit, lorsque c'est possible, être réalisée à l'aide d'un certificat délivré par l'IGC du ministère ;
- Le télé-assistant doit être un agent dûment autorisé par le ministère pour effectuer une telle opération, l'utilisateur devant être en mesure de vérifier son identité ;
- La solution de télé-assistance doit être à jour et se présenter sous la forme d'une application démarrée par l'utilisateur plutôt que d'un service

lancé automatiquement au démarrage du poste ;

- La solution de télé-assistance doit utiliser des protocoles sécurisés permettant l'authentification mutuelle entre les postes, un échange de clés de session éphémères et une protection contre les attaques courantes en la matière ;
- L'opération de télé-assistance doit être journalisée (au minimum consignation de l'adresse IP de la source, l'identité de la source, la date et l'heure de début et de fin de la prise de la main) ;
- Il doit y avoir une déconnexion ou un verrouillage automatique de toute session créée durant la prise de main à distance quand celle-ci se termine et les utilisateurs doivent s'en assurer.

EXG_CAC_020 Tout accès distant d'exploitant tiers (prestataire) doit être dûment identifié et limité dans le temps.

Dans le cas où il n'est pas possible de limiter la connexion, tous les événements d'exploitation et de maintenance doivent être tracés dans un journal d'événements dédié, qui puisse être audité et dont l'intégrité doit être garantie.

EXG_CAC_021 Les réseaux des zones Z3 seront cloisonnés et séparés logiquement du reste du réseau. Ces réseaux disposeront d'un serveur ou relais de messagerie et d'un serveur bureautique dédiés pour les besoins du service correspondant.

EXG_CAC_022 Les sessions bureautiques inactives doivent être fermées automatiquement après dix minutes d'inactivité.

Pour les sessions applicatives inactives, les MOA se prononceront sur la durée maximale d'une session qui ne doit dépasser 4H.

EXG_CAC_023 En cas d'échec de connexion à un système ou une application, la raison de cet échec doit être tracée mais ne doit pas être affichée à l'utilisateur (par exemple, compte inexistant, mot de passe invalide, …) ; le message d'erreur peut être « Échec de la connexion », sans aucune information sur l'origine de cet échec.

Des dispositifs doivent être mis en place pour limiter le nombre de tentatives de connexion, notamment :

- Bloquer le compte utilisateur après cinq échecs de connexion ;
- Accroître le temps d'attente entre deux tentatives de connexion.

EXG_CAC_024 **Tout appareil mobile (téléphone, tablette, etc.) doit être sécurisé, lorsque c'est possible, par un verrouillage système (mot de passe ou schéma de**

déverrouillage) ainsi que par un code PIN. Les agents seront sensibilisés à ce verrouillage.

Dans la mesure du possible, ces mesures de protection doivent répondre aux mêmes conditions qu'un mot de passe robuste classique. Par exemple, le code PIN doit être différent de 1234, 0000 ou de la date de naissance de la personne utilisant l'appareil.

2.9 Homologation de sécurité des systèmes

EXG_HOM_01

Conformément au Référentiel général de sécurité (RGS), chaque SI permettant des échanges électroniques entre deux autorités administratives ou avec les usagers de l'une d'elle devra être homologué avant sa mise en production.

L'homologation de sécurité est la démarche permettant d'identifier, d'atteindre puis de maintenir un niveau de risque de sécurité acceptable pour un SI, compte tenu du besoin de sécurité de ce SI, préalablement exprimé lors d'une pré-étude de sécurité.

La note de service SG/SM/SDSI/MSSI/N2012-1403 du 28 mars 2012 précise l'organisation et la méthodologie retenue par le ministère, dont les éléments fondamentaux sont repris ci-après.

EXG_HOM_02 Au sein du ministère, les autorités administratives distinctes, au sens de la procédure d'homologation de sécurité, sont :

- L'administration centrale ;
- Chaque service déconcentré ;
- Chaque établissement public d'enseignement agricole et chaque établissement public sous tutelle.

EXG_HOM_03 Chaque autorité administrative est une autorité d'homologation.

L'autorité d'homologation est chargée de prononcer la décision d'homologation du système. au nom de l'autorité administrative, elle documente ainsi formellement l'acceptation des risques résiduels en attestant que le projet a pris en compte les contraintes opérationnelles de sécurité établies.

EXG_HOM_04 La commission d'homologation est l'entité mise en place par l'autorité d'homologation. La commission d'homologation assiste l'autorité d'homologation et prépare la décision d'homologation en se réunissant tous les trois mois.

Au sein de l'administration centrale, la commission d'homologation est notamment composée de membres de droit :

- Le Secrétaire général du ministère, président de la commission ;
- Le chef de la MSSI, qui assure le secrétariat de la commission ;
- Le HFDS ;
- Le FSSI ;
- Le Chef du service de la modernisation ;

- Le président du CSI ;
- Le SDSI ;
- La MOA du SI ;
- L'ASSI ou AQSSI.

Au sein des services déconcentrés, la commission d'homologation est notamment composée de membres de droit :

- Le directeur du service déconcentré ;
- Le responsable de la mission des systèmes d'information (RMSI) ;
- L'ASSI de la structure.

Au sein des établissements publics sous tutelle, la commission d'homologation est notamment composée de membres de droit :

- Le Secrétaire général du ministère (pour les SI utilisés par l'administration centrale ou les services déconcentrés) ;
- Un représentant de la direction compétente.

EXG_HOM_05 La commission d'homologation peut se faire assister d'une commission technique, qui lui apporte un éclairage technique.

La commission technique est composée de personnalités qualifiées nommées par l'autorité d'homologation.

EXG_HOM_06 La MOA du SI demandant l'homologation doit constituer un dossier composé de :

- La demande d'homologation, elle-même composé de :
  - La synthèse de l'équipe projet,
  - La synthèse des éventuelles études de risques, audits ou tests d'intrusion,
  - Le dossier de conformité ISP et technique ;
- Le document d'avis de la commission technique, si la commission d'homologation l'a saisie, et qui est composé de :
  - Un avis sur le dossier technique,
  - Un avis sur les éléments hors-dossier.

EXG_HOM_07 La décision d'homologation, intervenant avant la mise en production opérationnelle, peut être :

- Une décision d'homologation ferme, qui est renouvelable au bout de cinq ans ;
- Une décision d'homologation provisoire, qui est assortie de réserve et

d'une brève durée au cours de laquelle le SI doit se mettre en conformité et à l'issue de laquelle la commission d'homologation statue à nouveau ;

- Une décision de refus d'homologation, qui est motivée et fait ressortir les risques résiduels jugés inacceptables.

EXG_HOM_08 Les décisions d'homologation de sécurité sont communiquées de différentes manières :

- Le HFDS est destinataire des décisions portant sur les SI du ministère (toutes autorités d'homologation confondues) et il peut demander copie d'un dossier d'homologation ;
- L'autorité d'homologation tient un rapport de ses décisions, à destination du CSI.
- L'autorité d'homologation doit rendre accessible aux utilisateurs les décisions d'homologation. Cette publication est essentielle pour garantir la confiance des utilisateurs. Elle est particulièrement importante pour les téléservices, ouverts sur les usagers ou le grand public.

EXG_HOM_09 La commission d'homologation contrôle régulièrement que le SI fonctionne en respectant ces conditions, notamment après des opérations de maintien en condition opérationnelle.

EXG_HOM_010 **Le SI doit faire l'objet d'une nouvelle procédure d'homologation de sécurité lorsque la décision d'homologation arrive au terme de l'homologation, c'est-à-dire cinq ans après la décision ferme d'homologation. Une nouvelle décision est alors nécessaire pour permettre au SI de continuer son activité.**

EXG_HOM_011 Avant le terme de l'homologation, la commission d'homologation peut examiner le besoin de renouvellement de sa décision, notamment lorsque :

- Les conditions d'exploitation du SI ont été modifiées ;
- De nouvelles fonctionnalités ou applications ont été installées ;
- Le SI a été interconnecté à de nouveaux systèmes ;
- Des problèmes d'application des mesures de sécurité ou des conditions de maintien de l'homologation ont été révélées, par exemple lors d'un audit de sécurité ;
- Les menaces sur le SI ont évolué ;
- De nouvelles vulnérabilités ont été découvertes ;
- Le système a fait l'objet d'un incident majeur de sécurité.

2.10 Développement et maintenance des systèmes

EXG_DEV_01

Le système d'information du ministère fait l'objet d'une cartographie afin de garantir la tenue à jour d'une liste complète des équipements et de faciliter la réaction en cas d'incident.

Un bilan annuel de l'application des mesures de sécurité est réalisé par les structures et transmis au FSSI sur demande.

Cette cartographie reprend au minimum :

- La liste des ressources matérielles (notamment le modèle, l'adresse IP, l'adresse MAC) et logicielles (notamment la version utilisée des logiciels principaux déployés sur ces postes) du ministère. Les postes d'administration ne sont pas exclus de cette cartographie.
- L'architecture réseau ainsi que l'identification des points névralgiques (connexions externes, serveurs hébergeant des données ou des fonctions sensibles, etc.).
- Cet inventaire matériel, logiciel et réseau doit pouvoir être vérifié par l'AQSSI une fois par an et envoyé à la SDSI (MSSI) ou au FSSI sur demande.

Le bilan comprend au minimum :

- Un Autodiagnostic de l'application des mesures de sécurité et des exigences non couvertes
- Des indicateurs de maturité SSI synthétiques

EXG_DEV_02 Les MOE doivent apporter des garanties sur la prise en compte des besoins de sécurité exprimées par les MOA.

Les architectures techniques des systèmes doivent être définies par les MOE et validées par les AQSSI correspondants.

Toute modification de système en production fait l'objet d'un mode opératoire formalisé. La modification doit être testée préalablement sur un environnement de test.

Ce mode opératoire doit être formalisé par la MOE.

EXG_DEV_03 Chaque AQSSI concerné doit s'assurer que les mesures de sécurité mises en œuvre sur les environnements de développement et de test du système d'information du ministère ou déployé chez un de ses prestataires respectent les règles spécifiques suivantes :

- Sauf impossibilité avérée, les environnements de développement et de test doivent être séparés des environnements de production.
- L'accès aux composants applicatifs (sources, exécutables, schémas de données) doit être strictement limité et basé sur le besoin

professionnel d'accéder à ces éléments.

- Seul le gestionnaire d'une librairie ou d'une ressource partagée est habilité à la modifier.

EXG_DEV_04 L'utilisation de données réelles dans le développement doit respecter :

- Les règles de confidentialité définies par le propriétaire des données et validées par l'AQSSI sous la responsabilité duquel les données ont été créées ;
- La législation sur les informations à caractère personnel (par exemple en n'utilisant que des données anonymes).

EXG_DEV_05 Les codes sources ne doivent pas être stockés sur l'environnement de production.

EXG_DEV_06 La mise en œuvre d'une solution « temporaire » ne dispense pas de respecter les exigences de protection induit par les besoins de la MOA.

EXG_DEV_07 Un audit de sécurité doit être systématiquement réalisé sur tout nouveau système qualifié de critique au sens de cette politique.

Le rapport d'audit doit fournir les recommandations à appliquer avant la mise en production pour traiter les vulnérabilités constatées de façon à répondre au besoin de sécurité formalisé par la MOA.

Le rapport d'audit doit être transmis à l'AQSSI concerné.

Cet audit est recommandé pour tous les autres systèmes.

EXG_DEV_08 Dans les applications ou formulaires, les données saisies doivent être testées avant acceptation (type, longueur, valeurs limites, …).

Toute erreur doit faire l'objet d'un événement dans un journal d'événement afin de permettre toute investigation en cas d'incident de sécurité.

EXG_DEV_09 L'intégrité des traitements et des données stockées doit être garantie notamment par des contrôles applicatifs et par des systèmes de sauvegardes.

EXG_DEV_10 Les systèmes d'application de niveau I3 ou plus, C3 ou plus, seront durcis par scellement d'environnement système ou de base de données.

EXG_DEV_11 L'utilisation de procédés cryptographiques pour la protection d'informations dans le développement d'applications doit respecter la politique de certification du ministère et de l'ANSSI.

EXG_DEV_12 Les codes sources des applications critiques au sens de cette politique doivent être audités avant mise en production.

EXG_DEV_13 Les codes sources des applications développées par le ministère sont au minimum de niveau C2.

EXG_DEV_14 Une gestion permanente des vulnérabilités des systèmes doit être réalisée pour tous les serveurs en production.

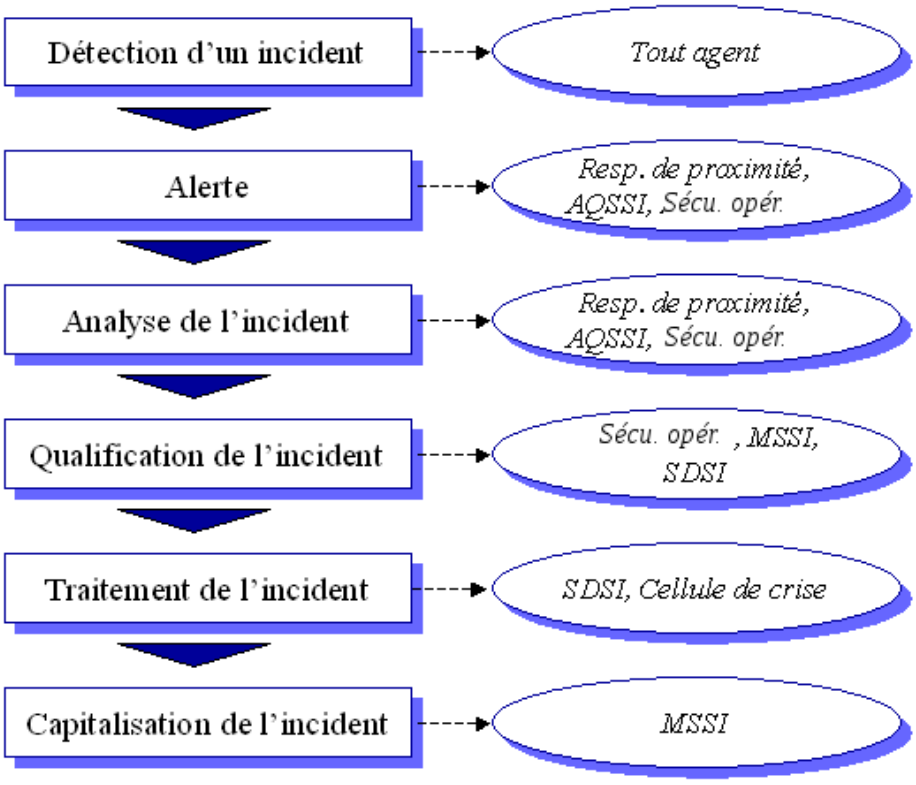
La veille, gérée par le Département de l'ingénierie de production, sera mutualisée par type de système d'exploitation.

2.11 Gestion des incidents

EXG_GDI_01

La survenue d'un événement anormal affectant l'un des composants du SI doit être déclaré par tout agent le constatant auprès son responsable informatique de proximité ou le cas échéant de l'AQSSI dont il dépend. En cas d'incident critique suspecté, le service en charge de la sécurité opérationnelle (ancien DIP et Pôle sécurité) pourra être saisi directement. La MSSI et le FSSI seront prévenus.

Le circuit de gestion d'un incident doit suivre le processus suivant :



Après sa détection l'incident est analysé par l'entité qui est alertée – responsable informatique de proximité, AQSSI – avec l'appui du service en charge de la sécurité opérationnelle. Ce dernier rend une analyse technique permettant de définir la nature de l'incident et sa portée.

En fonction d'une première estimation de sa gravité l'incident est porté immédiatement ou dès que possible à la connaissance du SDSI et de la MSSI qui sont chargés de sa qualification.

Les incidents de sécurité sont qualifiés sur trois niveaux selon qu'ils portent atteinte à la disponibilité, l'intégrité, la confidentialité et la preuve d'une application.

Un incident est :

- **mineur** s'il ne remet pas en cause la réalisation du besoin de sécurité défini par la MOA.
- **majeur** s'il remet en cause la réalisation du besoin de sécurité défini par la MOA sur une application non critique ou non sensible.
- **critique** s'il remet en cause la réalisation du besoin de sécurité défini par la MOA sur une application critique ou sensible du ministère.

Après sa qualification l'incident est traité par le SDSI.

En cas d'incident critique, le FSSI doit être alerté immédiatement pour mettre en œuvre, le cas échéant, une cellule de crise en lien avec la MSSI et le SDSI.

EXG_GDI_02 La MSSI défini et veille à la bonne application des procédures de gestion des incidents et s'assure de la formation des personnels concernés pour leur exécution.

De plus, elle définit les moyens et procédures aptes à :

- Diffuser l'alerte ;
- Collecter l'information ;
- Constituer une cellule de crise opérationnelle ;
- Décider des mesures conservatoires ;
- Élaborer un plan d'action regroupant des mesures correctives.

Les membres de la cellule de crise sont obligatoirement le SDSI, la MSSI et les services techniques, MOE et MOA concernées.

Les directeurs et le FSSI sont informés des résultats de traitement de la crise.

EXG_GDI_03 En cas d'usurpation d'un compte, l'AQSSI de la direction doit faire suspendre le compte et récupérer tous les événements concernant ce compte.

Une attention particulière doit être accordée aux comptes des agents travaillant au sein des services de zone Z3.

Les AQSSI doivent, pour ce faire, disposer des moyens permettant de détecter une éventuelle usurpation sur l'un des comptes de ces agents.

EXG_GDI_04 Tout incident de sécurité majeur ou critique doit donner lieu à l'ouverture d'une fiche incident.

Cette fiche incident doit faire apparaître la nature, la cible, les impacts et les actions correctrices entreprises.

Chaque incident a le statut suivant selon son évolution dans la chaîne de

traitement :

- Détecté ;
- Analysé ;
- Qualifié ;
- En cours de traitement ;
- Traité ;
- Capitalisé.

Chaque fiche doit être enregistrée avec un numéro d'identification unique, et être suivie et consolidée par la MSSI.

Une fois capitalisée, sa publication finale doit être validée par le SDSI et le FSSI.

EXG_GDI_05 La gestion des incidents de sécurité doit notamment considérer les événements suivants :

- Vol de matériel contenant une information de type C3 ou plus ;
- Diffusion d'informations de niveau C3 ou plus ;
- Destruction serveur ou poste de travail liée à une application critique ;
- Intrusion manifeste ou suspicion d'intrusion sur le système d'information du ministère ;
- Traitement volontaire illicite de données ;
- Compromission de fonction ;
- Usurpation de compte utilisateur ;
- Perte ou dysfonctionnements répétés des moyens de secours ;
- Perte ou dysfonctionnement répété du réseau électrique ou des dispositifs de climatisation.

EXG_GDI_06 Le système d'information doit avoir des moyens permettant de détecter efficacement les tentatives d'intrusion ou l'utilisation frauduleuse des ressources sur toute application critique ou sensible afin d'apporter une réaction efficace et appropriée.

Les moyens mis en place sont au minimum :

- Une inspection régulière des journaux d'événements de sécurité ;
- Une inspection des comptes utilisateurs autorisés ;
- Une analyse des tranches horaires d'accès ;
- L'utilisation de sondes de détection d'intrusion paramétrée et dont la base de signature est à jour.

EXG_GDI_07 La résolution d'incident récurrent doit s'appuyer sur les fiches de procédures

résultantes des incidents précédents. Ces fiches sont destinées à répondre aux incidents types.

EXG_GDI_08 La SDSI et les responsables informatiques de proximité doivent avoir le souci de déterminer le plus rapidement possible l'occurrence d'un événement constituant (ou susceptible de constituer) les prémices d'une attaque, d'un incident majeur ou à l'origine d'une malveillance.

Le Département de l'ingénierie de production doit organiser la remontée et la centralisation des détections d'incident par l'intermédiaire de processus simples d'information.

La MSSI organise la sensibilisation des utilisateurs et des exploitants au devoir de signalement de toute anomalie.

2.12 Gestion de la continuité d'activité

EXG_GCA_01

Toute salle informatique hébergeant des applications métiers ou d'infrastructures disposent d'un plan de secours informatique formalisé et à jour.

Ce plan de secours doit définir l'utilisation, au minimum, d'équipements de rechange et de sauvegardes à jour, stockés sur un site distinct et éloigné du site à protéger.

EXG_GCA_02

Chaque activité critique du ministère dispose d'un plan de continuité d'activité (PCA) formalisé et à jour.

Ce plan de continuité décrit comment, en cas de sinistre sur tout ou partie du système d'information, les différents acteurs nationaux – notamment MOA, MOE, Centre de production, SDSI – s'organisent pour gérer la crise, mettre en œuvre les procédures de secours, organiser la reprise d'activité dans les délais compatibles avec les besoins définis par la MOA.

En service déconcentré, un plan de continuité type pourra être proposé par l'AQSSI SG, validé par le FSSI et décliné localement par les AQSSI concernés.

EXG_GCA_03

Le plan de secours informatique et le plan de continuité des activités sont testés une fois par an pour les activités critiques (D3 ou plus) du ministère.

Chaque campagne de test doit faire l'objet d'un document formalisé permettant d'assurer un « retour d'expérience » et ainsi de faire évoluer ces plans pour optimiser leur fonctionnement.

EXG_GCA_04

Le plan de secours informatique concerne en premier lieu le Centre de production et l'administration centrale à Paris.

Il regroupe l'ensemble des procédures et ressources techniques prévues pour faire face à des scénarios de sinistres impactant le centre. Il doit être formalisé par la MSSI.

Le plan de secours informatique doit prévoir :·

- Un site annexe, distinct du site principal de production et apportant un niveau de protection physique homogène à celui du centre de production principal ;
- Les priorités et la progressivité du rétablissement des services (compte tenu de la criticité de chacune des applications) ;
- Les procédures de secours détaillées pour chacune des applications

identifiées D3 ou plus ;

- Les éventuelles inhibitions temporaires et acceptées de certains mécanismes de sécurité ou exigences de la présente politique ;

- Les mesures organisationnelles (gestion des membres du personnel informatique et sécurité, gestion des infrastructures, etc.) ;
- La périodicité des tests.

EXG_GCA_05 Les plans de continuité d'activité du ministère prévoient :

- Les priorités et la progressivité du rétablissement des activités métiers critiques du ministère (cabinet, HFDS, …) ;
- Les procédures dégradées éventuelles pour pallier l'arrêt du système d'information ;
- Les mesures organisationnelles ;
- Les mesures de communication ;
- La périodicité des tests.

EXG_GCA_06 Les plans de continuité d'activité du ministère doivent :

- Comprendre les risques menaçant le ministère en termes de probabilité et de conséquences à long terme, ce qui doit comprendre une identification et une classification formalisée par le FSSI par ordre de priorité des processus internes critiques après une analyse de risque établie par la MSSI ;
- Identifier tous les actifs utilisés par les processus internes critiques et particulièrement du système d'information ;
- Établir les objectifs généraux des installations de traitement informatique ;
- Garantir une vérification annuelle et mise à jour en conséquence des plans et des processus mis en place.

EXG_GCA_07 L'activation des plans de continuité d'activité est du ressort du FSSI et ce sur demande du cabinet ou tout directeur d'une des entités du ministère.

EXG_GCA_08 Les agents concernés par chaque plan seront informés par leur AQSSI respectif, sensibilisés ou, le cas échéant formés aux réactions attendues et aux procédures du plan.

2.13 Assurance de conformité

EXG_ADC_01

Tout agent, tout service, tout SI doit se conformer aux obligations légales, réglementaires et contractuelles du ministère, en sus de la présente PSSI et conformément à la réglementation en vigueur en matière de sécurité, notamment au regard du Référentiel Général de Sécurité (RGS).

Cette stricte obligation de conformité s'applique notamment pour toutes les normes relatives à la sécurité, aux données personnelles (comme la loi Informatique et libertés de 1978) ou à la propriété intellectuelle.

Toutes les obligations légales, réglementaires et contractuelles du ministère, ainsi que les mesures prises pour s'y conformer, doivent être explicitement définies, documentées et tenues à jour pour chaque système et pour l'ensemble du ministère.

La mise en conformité est assurée par chaque MOA.

EXG_ADC_02 Les droits de propriété intellectuelle de tout logiciel installé et utilisé dans le SI du ministère doivent être respectés.

Les logiciels doivent impérativement n'être utilisés qu'en conformité avec leur licence. Cette exigence s'applique de manière identique, que le logiciel ait une licence propriétaire ou libre.

L'inventaire fera état du respect de la propriété intellectuelle en mentionnant au minimum le type de licence, l'auteur ou l'éditeur du logiciel concerné et si les droits sont respectés

EXG_ADC_03 Pour toute application récupérant, utilisant ou transmettant des données personnelles, le MOA concerné doit se conformer aux obligations légales, réglementaires et contractuelles applicables, notamment à la loi 78-17 du 6 janvier 1978 (dite loi informatique et libertés).

Il doit en rendre compte au SAJ et à la MSSI.

EXG_ADC_04 Les moyens et ressources informatiques (poste de travail, accès, périphériques) mis à disposition des agents ou prestataires ne doivent pas être utilisés à des fins non autorisées.

À chaque fois que cela est possible, un message doit avertir que le système auquel accède l'utilisateur appartient au ministère et que tout accès illicite est passible de poursuites.

EXG_ADC_05 Des mécanismes de détection d'intrusion, d'inspection de contenu et de

surveillance générale sont utilisés pour prévenir et détecter les usages interdits. Ces mécanismes sont utilisés principalement aux point de jonctions entre le réseau du ministère et les réseaux tiers.

EXG_ADC_06 Les agents utilisent uniquement les dispositifs de chiffrement recommandés par la MSSI et installés par la SDSI. Ces dispositifs doivent respecter toutes les ententes, toutes les lois et toutes les réglementations en vigueur.

EXG_ADC_07 Chaque service doit mettre en place un mécanisme de contrôle interne afin de s'assurer que toutes les procédures de sécurité sont appliquées correctement, conformément aux normes, politiques de sécurité et documents d'application en vigueur.

EXG_ADC_08 Des audit de sécurité peuvent être conduits sur les points suivants :

- La politique de droit d'accès (robustesse des mots de passe, procédure de certification) ;
- L'architecture du réseau (cloisonnement des services sensibles, points d'accès aux autres réseaux contrôlés, …) ;
- Les dispositifs de sécurité (configuration des pare-feux, configuration des systèmes des applications critiques, configuration des antivirus, …) ;
- La configuration des serveurs visibles depuis l'internet ;
- La politique de sécurité du poste de travail.

La MSSI s'assure de la mise en œuvre des recommandations issues de ces audits de sécurité.

EXG_ADC_09 Des tests d'intrusion et un audit de vulnérabilité sont réalisés une fois par an sur chaque serveur critique du ministère ayant des besoins de sécurité élevés.

On entend par serveur critique tout serveur dont la pré-étude sécurité a montré des besoins de sécurité de niveau maximum sur au moins deux des quatre critères.

Les résultats d'audits doivent être communiqués au minimum au FSSI, à l'AQSSI concerné, au SDSI, à la MSSI ainsi qu'à la MOA concernée.

3 Annexe A : Glossaire et Acronymes

Glossaire général

Agent	Le terme agent est bien pris dans ce document au sens habituel, c'est-à-dire tout membre du personnel statutaire – fonctionnaire stagiaire ou fonctionnaire titulaire – et membre du personnel sous contrat – vacataire ou sous contrat à durée indéterminée. De façon plus générique, dans ce document, est assimilé à un agent tout membre du personnel dont les missions sont réalisées sous le contrôle direct de l'encadrement du ministère et qui doit donc respecter les règles de cette politique.
Personne externe	Ce terme désigne toute personne étrangère à la structure considérée, c'est à dire notamment sans lien hiérarchique avec le responsable de la structure considérée.
Membre du personnel	Le membre du personnel est une personne qui travaille pour le ministère. Ce terme est équivalent dans ce document au terme agent.

Glossaire sécurité

Actif	Tout élément ayant de la valeur pour une entreprise [ISO/CEI 13335-1:2004]
Audit	Examen méthodique d'une situation relative à un produit, un processus, une organisation, réalisé en coopération avec les intéressés en vue de vérifier la conformité de cette situation aux dispositions préétablies, et l'adéquation de ces dernières à l'objectif recherché [définition ISO, d'après la norme AFNOR Z61-102]
Authentification / identification	L'authentification a pour but de vérifier l'identité dont une entité se réclame. Généralement l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté. En résumé, s'identifier c'est communiquer son identité, s'authentifier c'est apporter la preuve de son identité. [D 530]
Besoin de sécurité	Expression à priori des niveaux requis de disponibilité, d'intégrité et de confidentialité associés aux informations, fonctions ou sous-fonctions étudiées.
Besoin d'en connaître	Expression qui signifie la nécessité d'avoir accès à des Informations classifiées dans le cadre d'une fonction officielle déterminée et pour l'exécution d'une mission spécifique.
Biens sensibles	Éléments du système qu'il est indispensable de protéger pour satisfaire les objectifs de sécurité. Ils sont identifiés par une analyse propre à chaque système, qui prend en compte en particulier les conditions d'environnement et les menaces auxquelles celui-ci est soumis. Les résultats de cette analyse sont consignés dans le dossier de sécurité et doivent préciser si les biens sensibles font l'objet d'une classification. Dans le cas présent, les biens sensibles incluent au minimum les données d'enregistrement. [IGI 1310]
Confidentialité	Propriété d'une information qui n'est ni disponible, ni divulguée aux

	personnes, entités ou processus non autorisés. [ISO 7498-2]
Disponibilité	Propriété d'un système informatique capable d'assurer ses fonctions sans interruption, délai ou dégradation, au moment même où la sollicitation en est faite par une personne autorisée. Note(s) La fiabilité fait référence à la capacité d'un système de se conformer à ses spécifications sur une période donnée, alors que la disponibilité a trait à la capacité d'un système de répondre à une demande à un moment précis. Les termes utilisés pour rendre compte de ces deux concepts ne doivent pas être confondus.
Donnée	Représentation d'une information sous une forme conventionnelle destinée à faciliter son traitement. [901/DISSI/DCSSI]
Intégrité	Propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée. [ISO 7498-2]
Bien	Toute ressource qui a de la valeur pour l'organisme et qui est nécessaire à la réalisation de ses objectifs.
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité. Il s'agit non seulement d'une méthode d'appréciation des risques SSI, mais aussi d'un véritable outil d'assistance à la maîtrise d'ouvrage (définition d'un périmètre d'étude, expression de besoins, responsabilisation des acteurs…). Associée aux Critères Communs et aux avancées dans le domaine de la gestion de la sécurité de l'information (par exemple la norme [ISO 17799]), EBIOS devient aussi une méthode de traitement des risques SSI.
Élément essentiel	Information ou fonction ayant au moins un besoin de sécurité non nul.
Élément menaçant	Action humaine, élément naturel ou environnemental qui a des conséquences potentielles négatives sur le système. Elle peut être caractérisée par son type (naturel, humain, ou environnemental) et par sa cause (accidentelle ou délibérée). Dans le cas d'une cause accidentelle, elle est aussi caractérisée par une exposition et des ressources disponibles. Dans le cas d'une cause délibérée, elle est aussi caractérisée par une expertise, des ressources disponibles et une motivation.
Événement de sécurité de l'information	Présence d'un état identifié d'un système, service ou réseau dénotant une violation possible de la politique de sécurité de l'information, une défaillance des sécurités ou une situation inconnue jusque-là et susceptible de concerner la sécurité. [ISO/CEI TR 18044 :2004]
Homologation de sécurité	Démarche formalisée permettant d'identifier, d'atteindre puis de maintenir un niveau de risque de sécurité acceptable pour un SI, compte tenu du besoin de sécurité préalablement exprimé.
Impact	Conséquence sur l'organisme de la réalisation d'une menace.
Incident informatique	Un incident informatique est indiqué par un ou plusieurs événements de sécurité de l'information indésirables ou inopinés risquant fort de compromettre les activités de l'entreprise et de menacer la sécurité de l'information. [ISO/CEI, TR 18044 :2004]
Menace	Cause potentielle d'un événement indésirable susceptible d'endommager un système ou une entreprise. [ISO/CEI 13335-1 :2004]

Mesure de sécurité	Moyen destiné à améliorer la sécurité, spécifié par une exigence de sécurité et à mettre en œuvre pour la satisfaire. Il peut s'agir de mesures de prévision ou de préparation, de dissuasion, de protection, de détection, de confinement, de « lutte », de récupération, de restauration, de compensation…
Propriétaire	Personne désignée qui possède la responsabilité de création, de traitement, de diffusion d'une information ou d'utilisation d'un service applicatif.
Référentiel général de sécurité	Référentiel entré en vigueur suite à un décret du 6 mai 2010 qui fixe les règles contribuant à la sécurité des informations. Outre des règles sur les dispositifs de signature électronique, authentification, confidentialité ou horodatage, il contient des bonnes pratiques en matière de SSI ainsi que des dispositions visant à mettre en place la procédure d'homologation de sécurité. La version initiale du RGS (v.1.0) a été rendue officielle par arrêté du Premier ministre en date du 6 mai 2010. Une version 2.0 a été publiée par arrêté du Premier ministre du 13 juin 2014. Elle est applicable à partir du 1er juillet 2014.
Risque	Combinaison d'une menace et des pertes qu'elle peut engendrer, c'est-à-dire : de l'opportunité de l'exploitation d'une ou plusieurs vulnérabilités d'une ou plusieurs entités par un élément menaçant employant une méthode d'attaque ; et de l'impact sur les éléments essentiels et sur l'organisme.
Risque résiduel	Risque subsistant après le traitement du risque. [ISO Guide 73]
Sécurité de l'information	Protection de la confidentialité, de l'intégrité et de la disponibilité de l'information ; peut également porter sur d'autres propriétés, comme l'authenticité, l'imputabilité, la non-répudiation et la fiabilité.
Sécurité des systèmes d'information	Protection des systèmes d'information, et en particulier des éléments essentiels, contre toute atteinte des critères de sécurité non autorisée, qu'elle soit accidentelle ou délibérée.
ISO / CEI	L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) constituent le système spécialisé de normalisation à l'échelle mondiale. Une famille de normes internationales relatives aux systèmes de gestion de la sécurité de l'information (ISMS) est en cours d'élaboration au JTC 1 ISO/CEI, SC 27. Cette famille comprend des normes internationales sur les critères, la gestion des risques et les mesures des systèmes de gestion de la sécurité de l'information, ainsi que des conseils sur la mise en œuvre de ces systèmes. Elle adoptera une formule de numérotation utilisant la série de nombres 27000 et suivants. A partir de 2007, il est envisagé d'intégrer la nouvelle édition d'ISO/CEI 17799 dans cette nouvelle formule de numérotation sous la référence ISO/CEI 27002.
ISO 17799	NORME INTERNATIONALE - Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la gestion de la sécurité de l'information La présente norme internationale établit une guide et des principes généraux pour l'introduction, la mise en œuvre, l'entretien et l'amélioration de la gestion de la sécurité de l'information dans les entreprises. Les objectifs qui y sont décrits donnent une orientation générale sur les buts généralement admis de la gestion de la sécurité de l'information. Les objectifs des contrôles et les contrôles figurant dans cette norme internationale sont destinés à être appliqués pour répondre aux besoins déterminés par une appréciation des risques. Cette norme internationale peut

	servir de guide pratique pour l'élaboration de normes de sécurité des entreprises et de pratiques de gestion de la sécurité efficaces, mais aussi pour permettre de susciter la confiance dans les activités inter-entreprise.
Vulnérabilité	Faiblesse ou faille d'un élément d'actif ou d'un ensemble d'actifs qui peut être exploitée par une ou plusieurs menaces. [ISO/CEI 13335-1:2004]

Acronymes

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information (anciennement Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI))
CERT-FR	Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (anciennement CERTA)
DAAF	Direction Départementale de l'Alimentation, de l'Agriculture et de la Forêt
DRAAF	Direction Régionale de l'Alimentation, de l'Agriculture et de la Forêt
FSSI	Fonctionnaire de Sécurité des Systèmes d'Information
HFDS	Haut Fonctionnaire de Défense et de Sécurité
ISP	Intégration de la Sécurité dans les Projets
MAAF	Ministère de l'Agriculture, de l'Agroalimentaire et de la Forêt
MOA	Maîtrise D'ouvrage
MOE	Maîtrise D'œuvre
MSSI	Mission Sécurité des Systèmes d'Information
PDA	Personal Digital Assistant / Assistant numérique personnel
PCA	Plan de Continuité d'Activité (idem Plan de Reprise d'Activité)
POS	Pôle Opérationnel de Sécurité
PSSI	Politique de Sécurité des Systèmes d'Information
PSSIE	PSSI de l'État
PSSI-DDI /Préfec-tures	PSSI-Réforme de l'Administration Territoriale de l'État (PSSI concernant les Directions départementales interministérielles (DDI) et les préfectures)
RGS	Référentiel Général de Sécurité
SAJ	Service des Affaires Juridiques du Ministère de l'Agriculture
SG	Secrétariat général du Ministère de l'Agriculture
SI	Système d'Information

SSI	Sécurité des Systèmes d'Information

4 Annexe B : Nomenclature des exigences de sécurité

Les chapitres de la norme ISO ont été renommés en domaines pour des besoins de lisibilité.

Chacune des exigences de sécurité définies au sein de ces domaines principaux doit être unique impliquant une numérotation spécifique qui respecte le modèle suivant :

Domaine	Trigramme	Nomenclature
Politique de sécurité	PDS	***EXG_PDS_XX***
Organisation de la sécurité	ORG	***EXG_ORS_XX***
Classification des Informations	GDA	***EXG_CLA_XX***
Ressources humaines	SRH	***EXG_SRH_XX***
Gestion des prestataires	PRE	***EXG_PRE_XX***
Sécurité physique des locaux et matériels	SPE	***EXG_PHY_XX***
Exploitation des systèmes	GCO	***EXG_EXP_XX***
Identification et contrôle d'accès logique	CAC	***EXG_CAC_XX***
Homologation de sécurité des systèmes	HOM	***EXG_HOM_XX***
Développement et maintenance des systèmes	ADM	***EXG_DEV_XX***
Gestion des incidents	GDI	***EXG_GDI_XX***
Gestion de la continuité d'activité	GCA	***EXG_GCA_XX***
Assurance de conformité	ADC	***EXG_ADC_XX***

Il est à noter que **« XX »** représente la numérotation de l'exigence, symbolisée par une série de deux chiffres.

CHARTE INFORMATIQUE

Document public – Confidentialité C0

définie et approuvée le 06 Juillet 2015 par le

Service du Haut-Fonctionnaire de Défense et de Sécurité

et le

Secrétariat Général

Préambule

La présente Charte définit et fixe les conditions générales d'utilisation et les mesures de sécurité-applicables à tous les systèmes d'information et de communication présents au sein de l'administration centrale et des services déconcentrés du ministère de l'agriculture.

L'utilisation du matériel informatique, des moyens de télécommunications, des réseaux et de l'accès à Internet y est détaillée afin de permettre une exploitation optimale et sécurisée du système d'information pour l'ensemble des intervenants au sein du ministère de l'agriculture, qu'il s'agisse de ses utilisateurs habituels tels que ses agents ou de ses utilisateurs temporaires tels que les prestataires externes ou les stagiaires.

La charte informatique, comme le règlement intérieur, a une valeur juridique opposable devant les juridictions, ainsi sa violation pourra entraîner en plus des sanctions disciplinaire, des sanctions administratives, civiles ou pénales.

Une lecture attentive des dispositions de la charte est conseillée afin d'assurer l'intégrité des ressources informatiques et notamment celles mises à votre disposition.

Table des matières

1 Définitions des termes techniques utilisés

Les **administrateurs** sont les personnes en charge de la gestion du système d'information, que ce soit au niveau de sa sécurité, de son fonctionnement, de son exploitation et d'un point de vue opérationnel.

Les **utilisateurs** sont toutes les personnes identifiées et spécifiquement autorisées à utiliser le matériel informatique. Ce sont les agents, les stagiaires et le cas échéant les prestataires informatiques et les visiteurs autorisés à se connecter au réseau de manière dérogatoire.

L'internet se définit comme étant le réseau mondial associant des ressources de télécommunication et des ordinateurs serveurs et clients, destiné à l'échange de messages électroniques, d'informations multimédia et de fichiers.

Un **logiciel** est entendu comme un ensemble de programmes, procédés et règles, et éventuellement de la documentation, relatifs au fonctionnement d'un ensemble de traitement de données. Il a pour but de faire accomplir des fonctions par un ordinateur ou un équipement de communication électronique.

Le **réseau** est un ensemble permettant la connexion d'équipement au sein du système d'information. Il prend en compte les prises RJ45, les concentrateurs (*hubs*) et commutateurs réseau (*switches*) et autres moyens de connexion mis à disposition par le Ministère (clef 3G, Wi-Fi).

Le **système d'information** est considéré comme un ensemble de ressources regroupant à la fois le réseau, les applications, le matériel informatique, les moyens de communication et d'échange de même que les procédures associées et les ressources humaines afférentes.

Le **matériel informatique fixe** comprend les éléments physiques employés pour le traitement de données et destinés à rester dans les locaux du ministère de l'agriculture et à ne pas être transportés facilement par l'utilisateur. Par exemple, un ordinateur fixe ou une imprimante entrent dans cette catégorie.

Le **matériel informatique portable** peut être utilisé hors des locaux du ministère de l'agriculture et transporté facilement par l'utilisateur. Par exemple, un ordinateur portable, un téléphone, ou une clef USB entrent dans cette catégorie.

Les **données personnelles** sont toutes les données permettant d'identifier directement ou indirectement une personne physique. Par exemple, les noms, prénom, numéro de sécurité sociale sont des données personnelles.

Le **RMSI** est le Responsable de la Mission des systèmes d'information c'est-à-dire le responsable informatique de proximité de l'utilisateur.

L'**AQSSI** est l'Autorité Qualifiée de Sécurité des Systèmes d'Information qui est responsable pour sa structure, de la sécurité des systèmes d'information. Elle veille à l'application des dispositions ministérielles.

Les **ASSI** sont les Agents chargés de la Sécurité des Systèmes d'Information, ils aident notamment l'AQSSI à veiller à la bonne application de la PSSIA.

Le **FSSI**, Fonctionnaire Sécurité des Systèmes d'Information, assiste le Haut Fonctionnaire de Défense et de Sécurité (**HFDS**) qui est responsable de l'application des dispositions relatives à la sécurité de la défense nationale.

Le **SDSI** est le Sous-Directeur des Systèmes d'Information, il est garant de la cohérence technique des dispositifs de protection pour l'ensemble des applications ainsi que de la cohérence des politiques de sécurité techniques des applications métiers ou transverses.

La **MSSI**, Mission Sécurité des Systèmes d'Information, assure la cohérence du niveau de protection sur l'ensemble du SI et représente le SDSI dans les instances où elle intervient.

L'**ANSSI** assure la fonction de l'Autorité Nationale de Sécurité et de défense des Systèmes d'Information afin de coordonner l'action gouvernementale pour la gestion des menaces et des crises affectant la sécurité des systèmes d'information des autorités publiques.

2 Dispositions de la charte Informatique

2.1 La sécurité du Système d'Informations

2.1.1 Les règles d'établissement et d'utilisation des mots de passe

Tout utilisateur des systèmes d'information du ministère doit disposer d'un **identifiant unique**. Cet identifiant est assorti obligatoirement d'un mot de passe, qui, pour des raisons de sécurité se doit d'être robuste.

Pour cela, il doit remplir les conditions suivantes :

- Le mot de passe est composé d'au minimum **huit caractères** avec au moins trois des types de caractères suivants : lettres majuscules, lettres minuscules, chiffres, caractères spéciaux.
- Le mot de passe est **unique**. En cas de pluralité de comptes, il est fortement conseillé qu'un mot de passe différent soit utilisé pour chacun d'eux.
- Le mot de passe doit être **difficile à deviner et facile à retenir**. Ainsi, il faut impérativement éviter la répétition de termes ou de caractères, les mots communs (par exemple du dictionnaire), les prénoms et noms de personnes (l'utilisateur, ses relations ou des personnalités connues) et les informations personnelles (dates, numéros de carte bancaire, informations sensibles).

Tout appareil mobile (téléphone, tablette, etc.) doit être sécurisé, lorsque c'est possible, par un verrouillage système (mot de passe ou schéma de déverrouillage) ainsi que par un code PIN.

Le mot de passe de chaque utilisateur doit être personnel, unique et non partagé.

2.1.2 Les règles de connexion de matériels et d'installations de logiciels

Il est strictement **interdit de connecter tous types de matériel personnel (ordinateur portable, smartphone, tablette, etc.) sur le réseau du ministère.** On entend par réseau du ministère à la fois les équipements filaires (prises réseau RJ45 notamment) ainsi que le réseau Wi-Fi du ministère.

La **connexion de tout autre type de matériel personnel** tel que appareils photos, disques dur externe, clefs USB, carte mémoire à un autre matériel du ministère **est tolérée dès lors que sa sécurité a été préalablement expertisée par un agent de l'informatique de proximité.**

L'utilisateur souhaitant se servir de son matériel personnel pour un travail professionnel devra toutefois respecter certaines conditions cumulatives :

- **exclure** les connexions au réseau du ministère,

- **proscrire** le traitement d'information atteignant un niveau C4[1] ou supérieur,
- **autoriser** le ministère de l'agriculture, en cas d'incident, à auditer son poste personnel,
- **exclure** le recours à des services en ligne tiers pour travailler sur des sujets professionnels.

2.1.3 Les règles générales d'utilisation

Il est strictement interdit sur le matériel informatique du ministère de :

- **télécharger** des logiciels et des contenus non autorisés,
- **masquer** sa véritable identité, usurper l'identité d'autrui,
- **tenter d'obtenir** des droits et prérogatives que l'on ne possède pas (par exemple obtenir des droits d'administrateurs),
- **détruire**, modifier, altérer des données appartenant à d'autres utilisateurs, sans leur autorisation,
- **interrompre ou perturber** le fonctionnement normal du matériel informatique,
- **introduire** toute forme de virus informatique volontairement.

Et plus généralement, **il est interdit d'avoir un comportement manifestement contraire aux principes et dispositions énoncés dans la présente Charte.**

En cas de nécessité absolue de déroger aux règles de sécurité dans le cadre de l'activité professionnelle, cette dérogation doit obtenir l'accord préalable de l'AQSSI, de l'ASSI ou du SDSI. U**ne demande écrite et motivée doit être présentée en ce sens.**

Une vérification antivirus par une personne qualifiée SSI (ASSI, MSSI, FSSI) **doit être effectuée avant toute connexion au matériel professionnel des périphériques tiers** (en particulier les périphériques de stockage). Cette exigence comprend également les cadeaux et objets promotionnels reçus par un utilisateur.

2.1.4 Les règles concernant les échanges d'informations

Toute **transmission d'information de niveau C3[2] ou plus sera chiffrée** en privilégiant un produit certifié ou qualifié par l'ANSSI. Pour le niveau C4 ou plus, le chiffrement sera obligatoirement effectué avec un produit certifié ou qualifié par

[1]Le niveau C4 est le niveau de stratégique dans la classification des informations, il concerne tous les documents comportant des informations très sensibles mais non classifiées de défense, à diffusion strictement limitée à une liste fermée et contrôlée de destinataire ayant droit d'en connaître.
[2]Le niveau C4 est le niveau de stratégique dans la classification des informations, il concerne tous les documents comportant des informations très sensibles mais non classifiées de défense, à diffusion strictement limitée à une liste fermée et contrôlée de destinataire ayant droit d'en connaître.

l'ANSSI.

Les **supports amovibles ou mobiles** (supports USB, CD, DVD, disquettes, téléphones, tablettes, etc.) pourront servir de média d'échange sous conditions qu'ils respectent les mesures de protection adaptées au niveau de classification correspondant.

Il est interdit de laisser des documents, physiques ou non, à proximité des appareils d'impression (photocopieurs multifonction (EMF), imprimantes, télécopieurs, etc.). Il convient donc de les retirer dès que possible, à savoir dès la fin de l'impression ou de l'utilisation du matériel. Par exemple, il convient de retirer les documents imprimés, de déconnecter les périphériques de stockage ou encore d'effacer volontairement la mémoire interne de l'appareil d'impression.

2.1.5 La gestion des alertes

En cas de perte ou vol de matériel même lorsqu'il s'agit d'un support de stockage (clef USB par exemple), l'utilisateur doit informer, sans délai, l'AQSSI, l'ASSI ou l'agent d'informatique de proximité qui en informera la chaîne SSI afin qu'elle puisse apprécier les risques qu'engendrent cette perte et prendre les mesures nécessaires à limiter son impact.

Les mêmes précautions doivent être prises par les utilisateurs en cas de **suspicion de vol d'information ou de tout incident (intrusion présumée dans une chambre d'hôtel par exemple)** ou encore d'**usurpation ou de perte de certificat**.

2.2 L'utilisation des outils informatiques

2.2.1 L'internet

L'utilisateur visitant un site est conscient que ses données de connexion sont enregistrées par le site visité ainsi que par les systèmes du ministère. Il doit donc s'abstenir de toute action susceptible de porter atteinte à l'image du ministère de l'agriculture.

L'utilisation de l'internet ne requiert que de simples droits d'utilisateur. Il est fortement recommandé de ne pas utiliser les droits d'administrateur d'un poste ou du domaine pour se connecter à l'internet.

Les données de connexion sont, conformément à la réglementation, conservées par le ministère pendant une année[3].

Du fait que leur consultation nuit à l'intégrité, à la sécurité et au bon fonctionnement du système d'information du Ministère, l'accès à certains sites est bloqué par un dispositif de filtrage.

L'utilisateur ne doit pas s'identifier sur des sites internet ni participer à des forums ou blogs par le biais d'une **adresse de messagerie professionnelle** comprenant le nom de domaine du ministère (prénom.nom@agriculture. gouv. fr). Il ne doit pas,

[3]Délai légal fixé par la loi LCEN du 21 juin 2004 et son décret d'application n°2011-219 du 25 février 2011.

non plus publier cette adresse dans le cadre d'une utilisation personnelle sur internet.

L'utilisateur doit lire et respecter les conditions régissant l'utilisation des sites internet qu'il visite.

En cas d'absence, **il est formellement interdit de transférer la messagerie professionnelle sur une messagerie personnelle.** L'usage de l'application de messagerie en ligne (web-mail), de droit pour l'ensemble des agents du ministère doit être substitué à cette pratique.

Afin de **respecter la vie privée d'autrui,** l'utilisateur ne doit pas diffuser des informations portant atteinte à l'intérêt de quiconque ou des images sans l'autorisation des personnes concernées, ni enregistrer ou diffuser des enregistrements de tiers sans leur accord préalable.

2.2.2 Le matériel informatique portable

L'utilisateur se doit d'être **vigilant** quant au matériel portable dont il dispose pour limiter les risques de perte, d'accès à l'information par des tiers non autorisés et donc d'atteinte au principe de confidentialité.

L'utilisateur ne doit pas laisser son matériel portable sans surveillance.

Quel que soit le lieu où l'utilisateur travaille, au sein ou à l'extérieur des locaux du ministère, il doit **veiller à ce que les tiers ne puissent pas avoir connaissance des communications échangées ni avoir accès aux données et documents stockés dans le matériel.** Par exemples un filtre de confidentialité pour écran doit être utilisé lors de l'usage du matériel dans les transports en commun ainsi qu'un câble antivol est fortement conseillé pour les bureaux ne fermant pas à clef.

Il doit aussi s'assurer d'appliquer un **niveau de sécurité approprié** concernant toutes les données confidentielles dont il prend possession ou connaissance par le biais de son travail.

Tout matériel de stockage (ordinateur portable, clef USB, disque dur, tablette, téléphone) contenant des données sensibles doit obligatoirement être chiffré.

L'utilisateur doit être vigilant, notamment en déconnectant ses réseaux sans fil vulnérables (Bluetooth, Wi-Fi, NFC, etc.) lors de ses déplacements hors de l'enceinte du site du ministère et en se souciant de la sécurité de son matériel.

En cas de vol du matériel portable, il est indispensable d'en référer à un responsable informatique de proximité ou le cas échéant à l'AQSSI dont il dépend afin que ceux-ci puissent prendre les mesures nécessaires.

En cas de doute sur la sécurité du matériel et sur le contenu de ses informations, se référer au paragraphe 2.1.4 sur la gestion des alertes.

En voyage, il est conseillé de conserver les appareils et les fichiers sur soi. Il convient de ne jamais laisser ces appareils et fichiers sans surveillance dans un hôtel ou un bureau visité. Les informations transportées doivent être réduites au minimum nécessaire et être stockées sur une clef USB chiffrée. L'utilisation de matériel tiers (clefs USB offertes, bornes de chargement en libre service, borne Wi-Fi dans un hôtel, etc.) est fortement déconseillé; au besoin, ce matériel devra être confié, au retour, aux services informatiques de proximité pour expertise.

2.2.3 Le courrier électronique

Le courrier électronique peut valablement **prouver** un fait (courriel sans signature électronique certifiée) ou un acte juridique (courriel avec une signature électronique : à valeur de contrat par exemple) devant les juridictions judiciaires ou administratives. À ce titre, **il peut engager la responsabilité du ministère et celle de son auteur.**

Les risques d'altération non perceptible des contenus des courriers électroniques exigent certaines **précautions si l'on souhaite en garantir leur opposabilité** :les conseils, avis et opinions ne doivent pas être formulés dans le courrier lui-même mais dans un courrier signé annexé en pièce jointe en format PDF.

L'usage de la messagerie personnelle à titre professionnel est prohibé.

L'utilisateur doit être **prudent** en cas de réception de messages tendant à obtenir de lui des informations personnelles, sensibles ou professionnelles qui pourraient ensuite être exploitées par un tiers malveillant. Ces techniques d'hameçonnage (filoutage ou encore *phishing*) doivent immédiatement être signalées à l'ASSI, la MSSI ou le FSSI.

Il ne doit en aucun cas donner ses identifiants et mots de passe par courrier électronique.

Avant toute ouverture de pièce jointe, l'utilisateur doit faire preuve de vigilance en contrôlant sa provenance et sa légitimité. Les pièces jointes peuvent contenir du code malveillant.

2.2.4 Les usages de services extérieurs

L'utilisation de services extérieurs à l'administration pour déporter sur un serveur distant des données ou des ressources, notamment au moyen de services en nuage informatique (*cloud computing*), est **interdit**.

Par exception, l'utilisation d'un service de stockage en ligne est autorisée si son utilisation respecte les caractéristiques minimales de sécurité posées par la PSSIA, et notamment l'authentification via un certificat électronique, le chiffrement des flux et des données ainsi que des garanties de stockage sur le territoire national.

2.2.5 L'image et la réputation du ministère de l'agriculture

L'utilisateur visitant un site est conscient que ses **données de connexion** sont enregistrées par le site visité. Il doit donc s'abstenir de toute action susceptible de porter atteinte à l'image du ministère de l'agriculture ou de ses agents.

L'utilisateur doit respecter **les obligations de réserve, de discrétion et de secret professionnel** conformément aux droits et obligations des agents publics[4] afin de ne pas causer de préjudice aux activités du ministère de l'agriculture ni porter atteinte à son image ou à sa réputation.

2.3 L'usage des réseaux sociaux

[4]Lois des 13 juillet 1983 et 26 janvier 1984.

L'utilisation de certains réseaux sociaux depuis le ministère est autorisée à titre personnel. Cependant, elle ne doit pas porter atteinte à la qualité du travail de l'agent.

Tout agent du ministère est tenu à une obligation de loyauté envers son employeur, ce qui s'apparente à un devoir de discrétion et de non-dénigrement.

Il est donc interdit de publier sur les réseaux sociaux ou sur tout autre forme de publication en ligne (blog, forums, etc.) des informations concernant le ministère et qui seraient de nature à porter atteinte à sa réputation ou qui pourraient entraîner la mise en jeu de la responsabilité du ministère et par conséquent celle de l'utilisateur à l'origine de cette publication.

Sur les réseaux sociaux ou ailleurs, l'utilisateur doit faire preuve de **vigilance face aux tentatives d'ingénierie sociale**. Des personnes malveillantes peuvent en effet essayer de récolter des informations personnelles afin d'usurper des identités et entrer dans un système d'information.

2.4 Le respect de la propriété intellectuelle et incorporelle

2.4.1 L'utilisation de logiciels

Les logiciels doivent être **utilisés en conformité** avec les dispositions du Code de la propriété intellectuelle ainsi qu'avec leur licence. Cette exigence est particulièrement importante pour les logiciels dont les licences sont non libres.

L'utilisateur ne doit pas télécharger, installer ou lancer des logiciels sur son poste de travail sans avoir obtenu au préalable l'autorisation de l'ASSI et du RMSI.

2.4.2 Les bases de données

L'utilisateur peut exploiter les informations contenues dans les bases de données pour exécuter ses obligations professionnelles au sein du ministère. Cette exploitation est exclusivement limitée à cette fin.

L'utilisateur ne doit ni utiliser, ni copier, ni diffuser ces informations dans un autre but. Cet usage est sanctionné par la loi[5].

La divulgation ou la destruction, non autorisée, d'une base de donnée ou de ses informations est interdite, car elle peut entraîner un grave préjudice pour le ministère de l'agriculture.

2.4.3 Les droits d'auteur

L'utilisateur doit être **vigilant** quant au respect du droit d'auteur en ne reproduisant pas une œuvre protégée sans l'**accord express de son titulaire**[6]. Il est rappelé

[5]Loi n° 98-536 du 1er juillet 1998.

[6]Lois des 11 mars 1957 et 3 juillet 1985.

que les logiciels sont en France protégés par le droit d'auteur[7].

Ainsi, pour tout document, photo, logo, texte et contenus éditoriaux publié sur des sites Internet, l'utilisateur doit vérifier avant tout emploi, s'il bénéficie de l'autorisation de l'auteur à cette fin.

Il est rappelé que **la violation des droits d'auteurs est constitutive du délit de contrefaçon** puni d'une peine d'amende de 300 000 euros et d'une peine de 3 ans d'emprisonnement[8].

2.4.4 Autres éléments de propriété industrielle

Dans le même sens l'utilisateur ne devra pas utiliser ou reproduire les **marques**, **logos** ou **inventions brevetées** sans avoir obtenu les **autorisations** ou **licences** nécessaires à de telles exploitations sous peines de poursuites civiles et pénales risquant d'entraîner la responsabilité ou entachant la réputation du ministère de l'agriculture.

2.5 La protection des données

2.5.1 Les données professionnelles et personnelles

Toute donnée à caractère personnel, c'est-à-dire « ***toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres*** » selon l'article 2 de la Loi Informatique et Libertés, doit être traitée en conformité avec cette loi.

Si, dans l'accomplissement de son travail ou de ses missions, l'utilisateur est amené à constituer des fichiers contenant des données personnelles, il doit veiller à ce que lesdits fichiers soient constitués dans le **respect** de la Loi Informatique et Libertés et s'abstenir d'y faire figurer des remarques personnelles et inappropriées sur les personnes citées (collègues, clients, etc.).

2.5.2 Les droits des utilisateurs

L'utilisateur, en application de la Loi Informatique et Libertés, dispose d'un **droit d'accès et de rectification** des données le concernant. Il peut exercer ce droit à tout moment en s'adressant à la MSSI qui redirigera la demande vers le service en charge.

En application du **droit à l'oubli**, l'utilisateur peut demander la suppression des données le concernant détenues par le ministère de l'agriculture. Cependant, ce dernier pourra lui refuser la suppression de certaines données dans le cas où celles-ci sont nécessaires à la finalité pour laquelle elles ont été collectées.

[7]Code de la Propriété Intellectuelle, Partie 1, Livre 1er.

[8]Article L. 335-2 du Code de la propriété intellectuelle.

2.6 La procédure de suppression des comptes utilisateurs

2.6.1 Les opérations à la charge de l'utilisateur

À la fin des relations contractuelles entre l'utilisateur et le ministère de l'agriculture, **une procédure automatique de fin d'utilisation des outils informatiques** est mise en place.

Préalablement à son départ, l'utilisateur doit **effacer** toutes ses données à caractère privé stockées dans sa boîte à lettre et ses dossiers (courrier électronique, pièces jointes, photos et autres documents).

À son départ, les données restantes seront **conservées** par le ministère de l'agriculture selon si elles sont considérées comme des données professionnelles.

L'utilisateur doit **restituer** ou laisser les matériels fixes et/ou portables mis à sa disposition par le ministère de l'agriculture, le jour de son départ. **La restitution du badge d'accès-agent au ministère est également obligatoire.**

2.6.2 La suppression du compte utilisateur par les administrateurs

Le compte utilisateur permettant l'accès au système d'information est **verrouillé** suite au départ de l'utilisateur.

L'utilisateur ne peut plus alors accéder aux différentes ressources mises à sa disposition ni aux données stockées dans les différents espaces numériques qui ont été fournis (boite de messagerie, documents personnels hébergés et stockés sur les serveurs, etc.).

La boite de messagerie est verrouillée après le départ de l'utilisateur, que celui-ci constitue un départ de l'administration ou un transfert vers une autre administration. La correspondance électronique de l'utilisateur ne sera pas conservée.

La redirection du contenu de la boîte aux lettres de l'utilisateur peut être effectuée à son départ par dérogation vers une autre boite aux lettres professionnelles pendant une période courte et définie par le SDSI.

Les certificats électroniques sont révoqués lors du départ de l'utilisateur du ministère. Ils sont également supprimés du poste (navigateur et messagerie).

2.7 Les contrôles et audits

2.7.1 Les conditions d'exécution des contrôles

L'utilisateur est informé que différents dispositifs du système d'information, liés à la gestion de la sécurité et à la recherche des pannes et incidents, **enregistrent** des informations le concernant, tel que par exemple des données de connexion.

Ces dispositifs permettent des analyses systématiques de volumétrie, la détection de comportements anormaux et l'identification d'utilisations contraires aux dispositions de la présente charte.

L'utilisateur a conscience que ces dispositifs peuvent garder une trace d'activités le

concernant ou de fichiers qu'il a supprimé. Les informations ainsi collectées sont conservées pendant une durée maximum de un an sauf en cas de poursuites disciplinaires ou de nécessité d'opérer des investigations complémentaires.

Avant toute prise de main à distance d'un ordinateur, l'administrateur doit demander à l'utilisateur son accord.

2.7.2 L'accès aux contenus

Le ministère a accès aux **contenus professionnels** de l'utilisateur, incluant la messagerie électronique.

Aucun contrôle de contenus à caractère privé ne sera en principe effectué par le Ministère en vertu du respect à la vie privée. Ces contenus doivent toutefois être **expressément identifiés** par l'utilisateur (par exemple avec le nom « dossier personnel »).

Le ministère pourra néanmoins opérer des investigations en cas de risque avéré, urgent ou de non-respect de la présente charte.

Les administrateurs disposent de **moyens d'investigation** pour remplir leur mission à partir de fichiers portant sur des données professionnelles, sur les traces de connexion et des communications électroniques.

Annexe – Contexte normatif

Les textes législatifs

- **Loi n° 78-17 du 6 janvier 1978** relative à l'informatique, aux fichiers et aux libertés et modifié par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. Les libertés individuelles susceptibles d'être menacées par l'utilisation des systèmes d'information et de communication sont protégées par ces lois.
- **Loi n° 78-753 du 17 juillet 1978** portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.
- **Loi n° 83-634 du 13 juillet 1983** détaille les droits et les obligations des fonctionnaires notamment en matière d'obligations morales telles que le secret professionnel et la discrétion professionnelle dont découle l'obligation de réserve.
- **Loi n° 84-16 du 11 janvier 1984** sur les dispositions statutaires relatives à la fonction publique de l'État et qui donne les sanctions disciplinaires en cas de manquements aux devoirs et obligations des agents.
- **Loi n° 85-660 du 3 juillet 1985** relative aux droits d'auteur et aux droits des artistes-interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle. Elle protège les auteurs de création et de logiciel contre toutes reproductions illicites.
- **Loi n° 88-19 du 5 janvier 1988** est relative à la fraude informatique. Elle va venir sanctionner les accès ou les maintiens frauduleux dans les systèmes d'information ainsi que les atteintes accidentelles ou volontaires à son bon fonctionnement mais aussi la falsification des documents informatiques et leur usage illicite.
- **Loi n° 91-646 du 10 juillet 1991** relative aux correspondances électroniques. Elle va étendre le principe du secret des correspondances à celles émises par la voie des communications électroniques.
- **Loi n° 2004-575 du 21 juin 2004** (LCEN) pour la confiance dans l'économie numérique. Elle va étendre la reconnaissance de l'écrit électronique à titre de validité d'un acte juridique s'il est assorti d'une signature électronique sécurisée.
- **Loi n° 2006-961 du 1 août 2006** (DADVSI), Titre II relatif au droit d'auteur des agents de l'État, des collectivités territoriales et des établissements publics à caractère administratif.

Les textes codifiés

- **Article 9 du Code civil** sur le respect de la vie privée, pour tous et par tous.
- **Articles 1315 et suivants du Code civil codifié** par la loi n° 2000-230 du 13 mars 2000 relatives à la preuve et à la signature électronique. Elle va adapter le droit de la preuve aux technologies de l'information en consacrant l'écrit électronique comme mode de preuve et en admettant la signature électronique.
- **Articles 226-1 à 226-7 du Code pénal** sur la répression des crimes et délits contre les personnes (d'après la loi n° 92-684 du 22 juillet 1992) qui viennent sanctionner les atteintes à la vie privée d'autrui.
- **Articles 226-16 et suivant du Code pénal** sur les dispositions pénales de la loi informatique et liberté contre les atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques.
- **Articles 323-1 à 323-7 du Code pénal** sur les atteintes aux systèmes de traitement automatisé de données afin de protéger les infrastructures vitales contre la Cybermenace (d'après la loi n°2013-1168 du 18 décembre 2013).

Les documents et réglementations de l'État

- **Instruction Interministérielle n° 901** du 28 janvier 2015, émise par le SGDSN/ANSSI et relative à la protection des systèmes d'informations sensibles.
- **Instruction Interministérielle 920 du 12 janvier 2005**, émise par le SGDN/DCSSI et relative aux systèmes traitant des informations classifiées de défense de niveau Confidentiel Défense.
- **Instruction Générale Interministérielle 1300** du 30 novembre 2011, émise par le SGDN/PSE/SSD relative à la protection du secret et des informations concernant la défense nationale et la sûreté de l'État.
- **La politique de sécurité des systèmes d'information de l'État** du 17 juillet 2014.
- **La politique de sécurité des systèmes d'information du Ministère de l'agriculture** du 06 Juillet 2015.