Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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

Secrétariat général **Service de la modernisation** **Sous-direction des systèmes d'information** **78, rue de Varenne** **75349 PARIS 07 SP** **0149554955**	**Instruction technique** **SG/SM/SDSI/2015-482** **29/05/2015**

Date de mise en application : Immédiate
Diffusion : Tout public

Cette instruction n'abroge aucune instruction.
Cette instruction ne modifie aucune instruction.
Nombre d'annexes : 1

Objet : Règles techniques applicables au poste de travail micro-informatique.

Destinataires d'exécution
Secrétariat général Directions d'administrtaion centrale DRAAF DAAF

Résumé : Cette instruction technique doit permettre de rappeler et, dans certains cas, de préciser les règles techniques et d'usage applicables aux postes de travail micro-informatiques au sein des services du ministère
Certaines de ces règles doivent faire l'objet d'une déclinaison locale, documentée au travers du dossier d'exploitation du service.

Table des matières

Contexte, enjeux et applicabilité

Le poste de travail constitue un élément essentiel de l'environnement professionnel de l'agent.

La présente instruction technique a pour objet de préciser les éléments essentiels présents sur le poste de travail standard, ainsi que les règles d'usage applicables. Elle s'inscrit dans le cadre du schéma directeur national des systèmes d'information (SDNSI) du ministère et du cadre de cohérence technique associé d'une part, dans celui de la politique de sécurité des systèmes d'information d'autre part. Elle est destinée :

- aux utilisateurs finaux – l'ensemble des agents du ministère,
- aux responsables d'unités,
- aux équipes techniques compétentes sur les sujets d'informatique de proximité (BIP en administration centrale, MSI en DRAAF/DAAF).

L'objectif est de regrouper en un document unique, lisible et compréhensible par tous, les préceptes principaux fondant la gestion opérationnelle du poste de travail au sein des services centraux et déconcentrés du ministère.

Certaines dispositions, signalées dans le texte, sont susceptibles de faire l'objet d'une déclinaison locale (ensemble de l'administration centrale, DRAAF/DAAF) élaborée sous la responsabilité de l'équipe de proximité compétente.

Quelle stratégie technique guide la gestion des postes utilisateurs ?

Le ministère de l'agriculture, de l'agroalimentaire et de la forêt s'inscrit dans la démarche engagée par le Gouvernement autour de la rationalisation et de l'ouverture (au sens des normes techniques applicables) du poste de travail.

Cet engagement se manifeste notamment par le choix d'appliquer aussi largement que possible le socle interministériel logiciels libres (SILL) conçu sous le pilotage du ministère de la culture et de la communication sous mandat de la direction interministérielle des systèmes d'information et de communication (DISIC).

Le SILL est présenté en détail sur le site du secrétariat général pour la modernisation de l'action publique : http://references.modernisation.gouv.fr/socle-logiciels-libres.

Plusieurs idées fortes structurent cette stratégie, et notamment :

- Disposer d'une stratégie interministérielle claire, partagée et lisible afin de faciliter l'interopérabilité et les échanges en interne de l'État et avec l'ensemble des opérateurs, des administrations publiques et des acteurs économiques et professionnels.
- Appliquer systématiquement des normes et standards ouverts, libres de droits, n'induisant aucune possibilité de discrimination entre les acteurs économiques susceptibles de participer ou d'appuyer l'action de l'État, et permettant de garantir dans la durée la possibilité d'utiliser des documents : norme ISO 26300 OpenDocument pour les textes, tableaux et présentations révisables, norme ISO 32000 PDF ou ISO 19005-1 PDF/A pour les documents non révisables ou devant être archivés, etc.
- Mettre en œuvre les orientations de la circulaire du Premier ministre du 19 septembre 2012 fixant les orientations pour l'usage des logiciels libres dans l'administration, en privilégiant, chaque fois que cela est pertinent, des ressources libres, et en facilitant ainsi le recours à des acteurs économiques implantés localement.

La stratégie de l'État et sa déclinaison ministérielle se sont construites progressivement depuis la fin des années 90 et disposent désormais d'une légitimité et d'une visibilité fortes. Chaque agent est invité à se l'approprier pour la promouvoir dans son cadre professionnel.

De quel matériel puis-je disposer ?

Le poste de travail peut être :

1. Un micro-ordinateur fixe, dans le cas général
2. Un micro-ordinateur portable, solution bien adaptée aux agents se trouvant fréquemment en situation de mobilité (techniciens, inspecteurs et contrôleurs de terrain, managers)
3. Une tablette hybride (micro-ordinateur portable pouvant être utilisé sans clavier physique), cas particulier de portable, adapté à des agents effectuant une part significative de leur temps de travail en situation de réunion hors bureau

Les tablettes sous Microsoft Windows 8.x sont considérées comme des postes de travail à part entière. Les autres tablettes, en particulier celles sous Androïd, sont considérées comme des équipements périphériques.

Pour les micro-ordinateurs portables et les tablettes hybrides, le poste de travail est associé à un réplicateur de port ou une station d'accueil, équipement de bureau permettant de faciliter l'utilisation du poste de travail en situation de travail posté.

Le recours à des équipements privés (propriété des agents) est interdit par la politique de sécurité des systèmes d'information Agriculture. Dans des cas où une équipe technique du ministère serait amenée, pour des raisons liées à une obligation de service, à intervenir sur un équipement qui n'est pas propriété de l'État, le propriétaire de l'équipement doit, en préalable, signer une décharge dégageant la responsabilité du ministère (ou de la DRAAF/DAAF) en cas de problème – sécurité, matériel, logiciel, portant sur les données – sur l'équipement considéré.

Comment mon poste est il installé ?

Le système d'exploitation de référence est :

- Microsoft Windows 7 si les écrans associés au poste de travail ne sont pas tactiles,
- Microsoft Windows 8.1 si au moins un écran associé est tactile.

Le système d'exploitation de référence précédent était Microsoft Windows XP. Aucun nouveau poste ne doit cependant être déployé sous ce système d'exploitation depuis le début de l'année 2014. Les postes existant seront progressivement migrés ou remplacés par des postes sous Microsoft Windows 7 ou 8.1.

À titre dérogatoire, sur demande du service, après visa du responsable des affaires générales si la demande concerne un poste bureautique et avis conforme SDSI, il est possible de déployer des postes de travail sous MacOS. Ces postes, limités à certaines applications particulières (graphisme) ne font pas l'objet d'une garantie de support de la part du ministère et les services qui y recourent sont fortement encouragés à étudier leur renouvellement par des PC en fin de vie des équipements existants.

Quels sont les logiciels installés sur mon poste de travail ?

Bureautique

La suite bureautique **LibreOffice** est la suite de référence du ministère.

LibreOffice est désormais installé par défaut sur les nouveaux postes de travail en lieu et place d'OpenOffice.org et sera progressivement généralisé, y compris sur les postes de travail plus anciens, à partir du second semestre 2014.

Outils de communication

Le ministère appuie ses communications électroniques sur le système national de travail collaboratif Agricoll. Ce système comporte plusieurs composants parmi lesquels le système national de messagerie électronique, l'annuaire, le système de gestion d'agenda, le système de gestion des listes de diffusion/discussion et de forums...

Sur le poste de travail, l'accès à ce système se fait par l'intermédiaire :

- du courrielleur **Mozilla Thunderbird** (messagerie) associé aux greffons OBM-Sync (synchronisation) et Lightning (agenda intégré au logiciel de messagerie),
- du navigateur **Mozilla Firefox**.

Navigateur Internet

Les applications métier du ministère sont testées avec Mozilla Firefox. Ce navigateur est donc à privilégier ; c'est aussi celui qui assure la meilleure protection des données.

Un second navigateur, Microsoft Internet Explorer, est cependant également systématiquement installé sur les postes de travail.

Il ne doit être utilisé que dans les cas suivants :

- pour l'accès à quelques applications anciennes (Gestor),
- sur instruction des équipes en charge de la sécurité des systèmes d'information, en cas de faille critique détectée sur le navigateur de référence Mozilla Firefox.

Accessoires complémentaires

- Le logiciel **Peazip** pour la compression (ce logiciel supporte notamment les formats de compression les plus utilisés, dont le .zip, le .7z et le .rar),
- Le logiciel **SyncBack** pour la gestion individuelle des sauvegardes (y compris de la sauvegarde messagerie). Ce sujet fera l'objet ultérieurement d'une instruction technique dédiée,
- Le logiciel **VLC** pour la lecture des flux audio/vidéo.

A quel outillage ai-je accès en situation de mobilité ?

Pour l'ensemble des agents

L'accès au système national de travail collaboratif Agricoll est possible en mode web (messagerie, agenda, annuaire) depuis tout poste de travail – y compris privé/personnel – raccordé à internet à l'adresse : https://portail.agricoll.agriculture.gouv.fr.

Pour les agents bénéficiant d'un ordinateur portable

Les micro-ordinateurs portables sont équipés du composant **Mercure VPN.** Ce composant permet, en situation de mobilité et sous réserve de disposer d'une connexion internet (WiFi ou réseau privé, clé 3G) et d'un certificat d'authentification Agricoll, un accès sécurisé à l'intranet du ministère et aux applications métier.

En pratique, tous les services sont accessibles sauf l'accès aux serveurs bureautiques et l'accès aux applications client-serveur dont le serveur n'est pas hébergé au centre de production informatique du ministère, à Auzeville.

Sur demande au responsable des affaires générales dont il relève, l'utilisateur peut disposer d'une clé 3G (marché Mobiles 2014). Les règles d'attribution sont établies par direction ou service.

Synchronisation avec un ordiphone

Si l'agent dispose d'un ordiphone professionnel et d'un certificat Agricoll, l'ordiphone peut bénéficier d'une synchronisation avec le système national de travail collaboratif Agricoll. Il permet alors d'accéder à la messagerie (*boîte aux lettres personnelle de l'agent et boîtes aux lettres fonctionnelles auxquelles l'agent est abonné)*, à l'agenda personnel de l'agent, et aux contacts.

J'ai besoin d'autres logiciels que ceux présents sur mon poste de travail

Les logiciels de l'installation standard ne sont jamais désinstallés et doivent impérativement être utilisés pour la satisfaction des besoins correspondant aux tâches standards. C'est en particulier le cas de l'outillage bureautique.

En application des règles de la politique de sécurité des systèmes d'information (PSSI), les agents ne disposent pas de droits d'administration de leur poste de travail et ne peuvent donc procéder seuls à l'ajout de logiciels ou au changement du paramétrage de leur poste de travail.

Pour répondre à des besoins supplémentaires, il est toutefois possible de demander des compléments d'installation. Ces demandes sont à adresser à l'équipe informatique de proximité (BIP ou MSI suivant le cas), qui prendra contact :

- Soit directement avec le demandeur si aucune instruction particulière n'est nécessaire (par exemple, cas des logiciels SILL non présents dans la matrice standard ministère).
- Soit avec le responsable des affaires générales du demandeur (cas des logiciels nécessitant une acquisition),
- Soit, uniquement en administration centrale, avec l'encadrement SDSI dans le cas où une dérogation spécifique est indispensable (cf. infra).

Les deux derniers cas ne sont pas exclusifs l'un de l'autre.

En fonction des procédures locales, la demande devra être effectuée par le biais du responsable des affaires générales ou pourra être transmise directement par l'agent.

Suite bureautique : MS Office

Dans certains cas, il peut être nécessaire d'installer des éléments de la suite bureautique privative Microsoft Office.

Ces cas doivent être justifiés par des arguments techniques et, pour en simplifier l'instruction par l'équipe informatique de proximité (MSI en DRAAF/DAAF, BIP en administration centrale), les demandeurs sont encouragés à fournir tous les éléments permettant d'illustrer les difficultés rencontrées.

Les demandes font l'objet d'un avis formel du SDSI (en administration centrale) ou du directeur/directeur régional (en service déconcentré). Cet avis indique le composant (Microsoft Word, Excel, Powerpoint) pour lequel la dérogation est acceptée.

La version de l'outillage Microsoft installée par défaut est la v2003. Si l'instruction technique montre le caractère indispensable d'une version supérieure, la v2007, dont le ministère ne dispose que d'un stock de licences très limité, est alors préférée. Cette version, ainsi que les suivantes, offre néanmoins un niveau de compatibilité moindre avec Libre Office que les versions précédentes.

Les adhérences techniques entre certaines applications nationales (majoritairement conçues dans la première partie des années 2000) sont coûteuses à supprimer. Elles disparaissent cependant progressivement, à l'occasion d'une modernisation significative de ces applications ou de leur remplacement par une nouvelle application. Ces adhérences techniques constituent des motifs admissibles de dérogation.

En administration centrale, la demande de dérogation fait l'objet d'un formulaire à remplir sous forme électronique ; la demande doit être validée par l'autorité hiérarchique du demandeur et par la MAG compétente avant d'être envoyée par messagerie électronique au BIP. Le traitement de la demande est assuré par la SDSI dans un délai de 5 jours ouvrés, les actions d'instruction technique interrompant le calcul de ce délai. La décision de dérogation n'est jamais tacite (processus de type « silence vaut refus »). Seul l'accord est motivé : le motif implicite de refus est la non satisfaction des critères d'accord.

En service déconcentré, le dossier d'exploitation précise le processus mis en place pour la conduite de l'instruction technique. Ce processus peut inclure, pour les cas délicats, une demande d'avis auprès de la SDSI.

En administration centrale comme en service déconcentré, les bénéficiaires d'une dérogation doivent être particulièrement exemplaires dans le respect des règles concernant les formats d'échange : en particulier, les logiciels privateurs ne doivent être utilisés que pour contourner les difficultés techniques ayant justifié leur installation. L'exemplarité constitue une valeur forte du ministère, qui s'applique très directement à l'utilisation des outils bureautiques.

En raison des restrictions ci-dessus, le ministère n'assure pas les montées en version des logiciels Microsoft installés par dérogation. Le risque technique résiduel est assumé, mais justifié par le caractère très limité des dérogations acceptées.

Gestion de projet

Le logiciel standard est **ProjectLibre**.

Cependant, pour la gestion de projets informatiques, c'est le logiciel MS Project qui est utilisé en raison des adhérences techniques associées à l'outillage de gestion de portefeuille (SteeringProject) : la SDSI gère à cette fin un pool de licences.

En dehors de la gestion de projets informatiques, si des licences MS Project doivent être acquises (avis préalable SDSI requis), elles doivent être financées sur les crédits de fonctionnement de la direction utilisatrice.

Logiciel de dessin vectoriel

La suite bureautique LibreOffice dispose du module Draw, compatible avec le logiciel Microsoft Visio et apportant les mêmes fonctionnalités.

Logiciel de dessin en mode point (bitmap)

Le logiciel standard est **The Gimp**.

Grapheur d'idées

Le logiciel standard est **Freeplane**.

Base de données

La suite bureautique LibreOffice dispose du module **Base**, satisfaisant l'essentiel des besoins pour une petite base de données personnelle ou pour un groupe de travail.

Microsoft Access peut être installé sur demande (en v2003) pour assurer la continuité d'un développement existant : il est cependant formellement proscrit de développer de nouvelles applications dans cet environnement (préférer Base, dont le périmètre fonctionnel est globalement équivalent).

La demande d'installation de Microsoft Access ne s'inscrit pas dans la démarche dérogatoire pour une suite bureautique. Elle est validée au niveau de l'équipe informatique de proximité après examen de la réalité du développement préalable et de l'examen du pool de licences disponibles.

Publication assistée par ordinateur (PAO)

Le logiciel standard est **Scribus**.

Pour les services de communication, l'utilisation d'autres logiciels (par exemple QuarkXPress ou Adobe InDesign) doit faire l'objet, en administration centrale, d'un avis conforme de la SDSI et de la DICOM. Ces logiciels sont normalement réservés aux services dont la communication est la fonction principale.

Information géographique

En application des recommandations de la commission consultative de l'information géographique (CCIG), le logiciel **QGis** est utilisé. Ce logiciel est désormais recommandé pour remplacer, dans le cas général, le logiciel privateur MapInfo.

Visioconférence à partir du poste de travail utilisateur

Le logiciel **CMA Desktop** s’appuyant sur l’infrastructure de visioconférence du ministère est le seul autorisé.

J’ai besoin d’accéder à des « logiciels métier »

La terminologie « logiciel métier » vise les applications et systèmes utilisés dans le cadre spécifique du poste occupé par chaque agent. On classe ainsi dans cette catégorie les applications et systèmes relavant des grands programmes métiers (RESYTAL, SIRENA, Cassis...) ou support (Chorus, Agorha, Découverte...).

L’accès aux logiciels métiers s’effectue en deux étapes :

- L'installation technique sur le poste de travail : pour les systèmes les plus récents, cette installation se résume souvent à la transmission d'un simple lien, l'accès se faisant au travers du navigateur Firefox.

  Pour les applications les plus anciennes, une installation technique (installation de l’application, configuration du navigateur) peut encore se révéler nécessaire.

  Dans ce cas, la demande doit être formulée à l'équipe informatique de proximité, qui appliquera les consignes techniques établies par les équipes maîtres d'œuvre des systèmes demandés.

  En fonction des procédures locales, la demande devra être effectuée par le biais du responsable des affaires générales ou pourra être transmise directement par l’agent.

  En administration centrale, l'attribution d'un nouveau poste de travail est l'occasion d'une revue systématique des logiciels installés, y compris métiers.

- L'attribution d'un rôle ou profil utilisateur au sein de l'application (habilitation) : cette attribution est opérée en application des règles établies par la maîtrise d'usage (ou, en son absence, par la maîtrise d'ouvrage) de l'application ou du système considéré.

  Dans le cas général, l'équipe informatique de proximité n'a ni rôle ni responsabilité dans ce processus, mais peut souvent donner des informations sur la procédure à mettre en œuvre, qui varie d'une application à l'autre.

Comment mon poste de travail est-il maintenu à jour ?

Pour les logiciels standards

À partir de septembre 2014, la nouvelle stratégie de montée de versions en administration centrale prévoit désormais une montée en version annuelle sur l'ensemble des postes. La montée en version s'effectuera logiciel par logiciel, et chaque montée en version sera – au moins pour les logiciels principaux, suite bureautique, navigateur, courrielleur, anti-virus – accompagnée d'une fiche pédagogique exposant les principales différences entre versions successives.

Les services déconcentrés sont encouragés à établir une stratégie de montée en version dérivée de celle-ci.

Pour les logiciels complémentaires

Pour les logiciels libres : la montée de version s’effectue à la demande de l'utilisateur. Pour les logiciels largement déployés, la montée de version est faite de manière simultanée pour l’ensemble des postes équipés.

Pour les logiciels éditeurs : une étude doit être faite au cas par cas en fonction des conditions de la licence d'utilisation.

Pour les logiciels métiers

La stratégie de mise à jour et d’évolution des logiciels métier est sous responsabilité de la maîtrise d'usage (ou, en son absence, par la maîtrise d'ouvrage) de l'application ou du système considéré. Elle varie d'une application à l'autre.

A quels services communs ai-je accès ?

Services d'impression et de numérisation

La circulaire SG/SAFSL/SDLP/N2009-1510 du 18 mars 2009 rappelle la stratégie poursuivie par le ministère, stratégie qui s'inscrit dans le cadre du Plan Administration Exemplaire (PAE). Cette stratégie prévoit notamment :

- la suppression des imprimantes à jet d'encre ;
- le non remplacement des imprimantes individuelles;
- le développement des copieurs multifonctions ;

- 100% des cartouches laser ayant des caractéristiques équivalentes à celle de l'écolabel NFE ;
- 100% des cartouches d'impression usagées reprises par les prestataires ou par des entreprises adaptées (EA) ou des établissements et services d’aide par le travail (ESAT).

Cette stratégie a conduit le ministère à s'inscrire dans le dispositif mis en œuvre sous l'égide du service des achats de l'État (SAE) qui a permis de conclure un accord cadre interministériel relatif à la location et le support d'équipements multi-fonctions (EMF).

Les EMF ainsi mis en place ont vocation à assurer :

- un service d'impression, depuis les postes de travail. Ce service est en mesure, pour les équipements les plus puissants, d'assurer une impression couleur A3 et des volumes pouvant aller jusqu'à 100 000 pages/mois.
- un service de numérisation, les fichiers générés pouvant être mis à disposition sur une ressource bureautique locale ou transmis par courrier électronique.
- un service de copie.

Pour leur fonctionnement, les EMF s'appuient sur l'infrastructure technique du ministère : réseau local du site, serveurs de messagerie nationaux, serveurs d'impression dédiés en administration centrale, intégrés au sein de l'infrastructure Milux en DRAAF/DAAF.

Les pilotes d'impression mis en œuvre disposent de fonctions de sécurité avancées. En particulier, il est possible de demander une impression différée, ou une impression protégée (nécessitant la saisie d'un code personnel sur l'EMF cible). Ces fonctions permettent de limiter la mise en œuvre d'imprimantes individuelles aux seuls cas où cette mise en œuvre est indispensable au regard de la proportion de documents confidentiels devant être imprimés.

Il est en effet nécessaire de rappeler que les imprimantes individuelles ont un coût moyen à la page très supérieur à celui des EMF : sans constituer un dogme, la mutualisation présente, dans la très grande majorité des cas, des avantages significatifs, y compris sur des plans aussi basiques que la communication au sein des équipes.

Espaces bureautiques

Des espaces communs, régulièrement sauvegardés, sont mis à disposition des utilisateurs. Ces espaces peuvent notamment servir :

- Au stockage de documents bureautiques ou de données métiers,
- À la collaboration et au partage de documents,
- À la sauvegarde de documents ou de données.

Ces espaces sont associés à des droits d'accès. Trois types de droits peuvent être attribués :

- Un droit individuel et exclusif, afin de disposer d'un espace destiné à la sauvegarde de données et documents professionnels personnels.
- Un droit collectif donné à une équipe (service, département, bureau…) dans le but de constituer un espace collaboratif pérenne.
- Une combinaison de droits individuels et/ou collectifs, afin de constituer un espace collaboratif dans le cadre d'un programme ou projet : ces espaces, dans le cas général, ont alors une durée de vie corrélée à celle du programme ou projet support.

Deux technologies sont utilisées à la date d'établissement de la présente instruction :

- Des espaces bureautiques, uniquement accessible au travers du réseau local par le biais de l'explorateur, désignés sous forme d'unité logique (G:\, P:\, et U:\ en administration centrale).

  Cette technologie est simple d'utilisation, et permet en particulier une utilisation sans rupture entre la gestion des fichiers sur le poste de travail et sur le réseau. Elle n’est en revanche pas utilisable en situation de mobilité.
- Des espaces documentaires sur un serveur de gestion électronique de document (**GEDSI**), accessibles au travers du navigateur (Firefox).

L'accès à ces espaces nécessite une habilitation et une authentification Agricoll. Cet accès est possible en situation de mobilité, mais induit une rupture dans le client utilisé. Elle peut présenter une performance inférieure à celle des espaces bureautiques mais permet de disposer de fonctions de recherche et de contrôle de flux beaucoup plus évoluées que dans le cas des espaces bureautiques.

Comment est assurée la sécurité de mon poste de travail ?

Chaque agent est responsable de la sécurité de son poste de travail. Il doit respecter les règles d'hygiène informatique et ne doit pas entraver le fonctionnement de l'outillage de sécurité.

Règles d'hygiène informatique

Chaque poste de travail dispose d'un ensemble d'outils destiné à améliorer la sécurité d'ensemble du système d'information en général, de l'environnement de travail de chaque agent en particulier.

Ceci étant, le principal acteur de la sécurité est... l'utilisateur : soyez prudents !

Le ministère a élaboré une politique de sécurité des systèmes d'information, elle-même dérivée de la stratégie gouvernementale en la matière. Il importe de s'y conformer strictement, en toutes circonstances. C'est bien la sécurité de l'ensemble du système d'information du ministère qui est mise en cause à chaque imprudence commise par l'un des agents du ministère.

Chaque agent est donc encouragé à respecter strictement Les 10 commandements de la sécurité sur internet (voir annexe) tels qu'établis par l'agence nationale pour la sécurité des systèmes d'information.

Anti-virus

Un logiciel anti-virus est en permanence actif sur le poste de travail. Il s'agit actuellement du logiciel **McAfee**, retenu dans un cadre interministériel (ministères de l'agriculture, de l'écologie, de l'intérieur, des finances, de la santé).

Ce logiciel est paramétré pour procéder à une analyse hebdomadaire systématique, dont le jour et heure de déclenchement varie d'un poste à l'autre de l'ensemble du poste de travail.

Certificats logiciels

Un certificat logiciel est un fichier installé sur le poste de travail de l'agent. Il correspond à son identité numérique et peut ainsi s'apparenter à une « carte d'identité électronique » de l'agent.

Tous les agents en administration centrale, DRAAF et DAAF peuvent se voir attribuer un certificat logiciel. L'agent doit pour cela disposer d'un compte Agricoll.

Les certificats du MAAF sont délivrés, dans chaque structure, par des agents qui ont été désignés comme autorité d'enregistrement locale (AEL). La liste de l'ensemble des agents qui exercent cette fonction est accessible à l'adresse suivante : *http://igc.agriculture.gouv.fr/liste_ael.php*

Au sein du ministère, 3 classes de certificats personnels sont délivrés :

- Les certificats d'authentification : ils servent à s'authentifier auprès de la plupart des applications informatiques du ministère (voire d'autres, comme Chorus, Salsa ou le site communautaire Alfresco du MEDDE/MLET/DISIC...) ;
- Les certificats de signature : ils servent à signer électroniquement les documents bureautiques (sous LibreOffice ou sur la place de marché *www.marches-publics.gouv.fr,* par exemple) ;
- Les certificats de chiffrement : ils permettent notamment de chiffrer les échanges par messagerie (cf. infra).

La durée de vie de ces certificats est de 3 ans. L'utilisation de certificats simplifie la vie quotidienne des agents (limitation de l'usage des mots de passe,...) tout en améliorant le niveau global de sécurité : elle doit donc être encouragée.

Les directions et services sont, de fait, encouragés à systématiser la certification de l'ensemble de leurs agents. Les équipes informatiques de proximité et les équipes en charge de la délivrance des certificats (AEL) assurent la promotion de ce dispositif.

Attention, un certificat est personnel et doit être protégé. Toute suspicion de compromission (perte, vol, usurpation) doit être immédiatement signalée auprès de l'AEL de la structure qui rendra le certificat inutilisable en procédant à sa révocation.

Chiffrement des données du poste de travail

Le chiffrement permet de répondre au risque de divulgation d'informations confidentielles.

Plusieurs solutions de chiffrement peuvent être mises à disposition :

- La partition disque principale des micro-ordinateurs portables doit être chiffrée en s'appuyant sur le logiciel **TrueCrypt**. *Note : ce chiffrement impose la saisie d'un mot de passe supplémentaire au lancement de la machine.*
- Le logiciel **TrueCrypt**, présent sur tous les postes, peut également être utilisé, en mode manuel, pour chiffrer des dossiers sur des supports amovibles (disques durs externes, clés USB), des espaces réseau (espace sur des serveurs bureautiques) ou sur le poste de travail.

  L'utilisation de TrueCrypt est personnelle : il n'est pas recommandé de procéder à des accès concurrents de partitions ainsi chiffrées (par exemple, des partitions partagées sur un serveur bureautique).
- Le logiciel **AxCrypt,** également installé sur tous les postes de travail, peut être utilisé pour sécuriser l'échange ou le stockage de documents sensibles. L'utilisation de ce logiciel nécessite de partager, avec les destinataires du document, un mot de passe : celui-ci doit alors impérativement être transmis par un moyen différent de celui utilisé pour la transmission du document protégé. Ainsi, si ce dernier est échangé par messagerie, le mot de passe associé peut, par exemple, être partagé par SMS.

  AxCrypt est assez largement utilisé au sein des services de l'État, voire des autorités publiques. Il s'agit par ailleurs d'un logiciel libre que les destinataires hors ministère peuvent, en tant que de besoin, installer par leurs propres moyens.

Attention, les mécanismes de chiffrement s'appuient sur la connaissance d'un mot de passe, connu seulement de l'utilisateur. Il n'est pas possible, pour une équipe informatique de proximité de déchiffrer des données qui auraient été chiffrées et dont le mot de passe aurait été perdu.

Chiffrement des messages électroniques

Lorsque les correspondants sont tous utilisateurs du système national de travail collaboratif Agricoll, et qu'ils disposent tous d'un certificat de chiffrement Agricoll, il est possible de demander le chiffrement du message au niveau du client de messagerie Thunderbird. Le message est alors automatiquement chiffré en émission, et déchiffré lors de la consultation en réception.

Les restrictions suivantes s'appliquent cependant :

- Le message ne peut être soumis et lu que depuis un client Mozilla Thunderbird convenablement paramétré avec la référence du certificat de chiffrement de l'utilisateur ; les messages ne peuvent être ni chiffrés ni déchiffrés depuis le client webmail ou depuis un autre client de messagerie que Mozilla Thunderbird.
- En cas d'envoi à plusieurs destinataires, le message ne sera chiffré que si tous les destinataires disposent bien d'un certificat de chiffrement Agricoll. Le chiffrement vers une liste de diffusion n'est pas possible.
- Avant de recevoir un message chiffré de la part d'un émetteur, il est indispensable de lui avoir envoyé, en clair, un message *signé* (avec un certificat d'authentification Agricoll).
- Seul le corps des messages est chiffré, pas leur enveloppe (en particulier, ni les destinataires ni le sujet ne sont chiffrés).

En dépit de ces restrictions, le service ainsi offert est sûr et simple d'utilisation, Thunderbird indiquant si il est, ou pas, en mesure de chiffrer le message.

Sauvegarde des données du poste de travail

Chaque utilisateur reste responsable de la sécurité des documents qu'il est amené à rédiger ou à utiliser. Les espaces bureautiques personnels peuvent être utilisés à cette fin dans la limite des quotas techniques mis en place. En cas de besoin, et sous réserve de l'accord des structures, des disques durs individuels peuvent également être utilisés. L'outil SyncBack doit alors être utilisé pour automatiser les actions de sauvegarde ou de restauration.

Le ministère prévoit d'engager courant 2015 une projet autour de la sauvegarde des données du poste de travail utilisateur (documents et messagerie).

Pourquoi n'ai-je pas accès à tous les sites Internet depuis le réseau du MAAF ?

La sécurité du système d'information du ministère impose la mise en place de fonctions de filtrage du trafic internet pour trois motifs principaux :

- La lutte contre les sites malveillants, par exemple connus pour abriter des espiogiciels (*malware*).

  Dans cette catégorie sont également placés les sites de partage de données personnelles (dropbox, dlFREE ou WeTransfer). Ces sites, en tant que tels, ne sont pas malveillants, mais leur utilisation pour échanger des données sensibles est fermement déconseillée, aucune garantie de sécurité ne pouvant être apportée.
- La lutte contre les sites illégaux (pédopornographie, racisme, anti-sémitisme, terrorisme...). Il s'agit en particulier d'éviter que le nom du ministère soit associé à une enquête construite sur les traces des sites illégaux démantelés. Si l'accès à un site exposant du contenu illégal est indispensable dans le cadre d'une enquête, alors l'accès doit être réalisé à partir d'un poste de travail raccordé directement à internet, et l'utilisation du poste de travail à cette fin doit être documentée.
- Le maintien des performances du réseau. Cet aspect vise notamment tout ce qui est flux vidéo, particulièrement consommateur de bande passante. Pour illustrer ce risque, les équipes réseau évoquent l' « effet Tour de France » : la bande passante à l'interconnexion entre le réseau interne et internet s'effondre si, par exemple, les flux vidéo associés aux télévisions publiques ne sont pas filtrés lors des étapes emblématiques de ce type d'événement sportif.

Mise en liste blanche : levée du filtrage pour l'ensemble du ministère

Le filtrage mis en place s'appuie sur des listes établies par un partenaire du ministère. Ces listes peuvent comporter des erreurs, conduisant par exemple à filtrer indûment un site légitime du point de vue professionnel.

Dans ce cas, une signalisation peut être faite à l'adresse mssi.sg@agriculture.gouv.fr. Après analyse, la demande d'inscription en liste blanche est alors transmise à l'opérateur en charge de la plate-forme de service (point d'interconnexion entre l'intranet du ministère et internet). Le demandeur est toujours informé du résultat de sa demande. Le délai moyen de traitement de celle-ci est d'une semaine.

Attention : cette procédure ne permet pas de défiltrer ni des sites fournissant des flux audio/vidéo présentant un risque de congestion pour le réseau du ministère, ni des sites de partage de données personnelles. Elle vise essentiellement à corriger les erreurs de classements induites par le partenaire du ministère (erreurs essentiellement inévitables en raison du nombre désormais colossal de sites internet à classifier).

Levée individuelle du filtrage

Dans certaines conditions, le filtrage peut s'avérer contre-productif et la mise en liste blanche insuffisante ou impossible à mettre en œuvre. Il est alors possible de demander la levée du filtrage ce qui permet alors d'accéder sans contrainte à l'ensemble d'internet, au prix d'un abaissement global du niveau de sécurité.

La demande de levée de filtrage s'effectue en ligne : http://proxyvip.national.agri/faire_demande.php. Elle nécessite un certificat d'authentification Agricoll et une validation hiérarchique et SDSI (accordée après instruction technique pour cette dernière validation). Si les justifications sont insuffisantes pour une décision immédiate, l'instruction est conduite sous la forme de questions/réponses avec le demandeur ou le valideur.

La levée de filtrage est accordée par défaut pour un an et doit, à l'issue de cette période, être renouvelée en respectant la même procédure (pas de renouvellement tacite).

Dans certains cas, l'instruction peut conduire à une levée de filtrage accordée pour une période réduite : tel est notamment le cas des levées de filtrage accordées à des stagiaires ou des vacataires (durée limitée à la période travaillée), dans le cas de sessions de formation (durée limitée à celle de la formation) ou pour accéder à des sites de partage d'information personnelle fléchés dans le cadre d'organisations tierces (durée limitée par défaut à 6 semaines, afin de permettre la recherche d'autres solutions de type partage Agricoll ou site ftp).

Comment accéder au support informatique de proximité ?

Le support représente l'ensemble des activités d'assistance aux utilisateurs des systèmes d'information.

Au ministère – administration centrale, DRAAF, DAAF – et, sauf exception limitées, cette activité est assurée par des **agents de l'État**, fonctionnaires ou agents contractuels. Les moyens consacrés au support ont fait l'objet, ces dernières années, d'actions de rationalisation significatives, induisant, en administration centrale comme en DRAAF/DAAF, une mutualisation des agents sur l'ensemble des métiers du ministère.

Demande de support

La demande de support s'effectue, dans le cas général, en situation d'urgence pour le demandeur, que la demande soit en relation avec une demande de travail (prévision de déménagement par exemple), d'information (« comment puis-je faire ceci ? ») ou une signalisation d'incident (« l'imprimante refuse de fonctionner alors que j'ai un dossier urgent à rendre »). Il est cependant important, quels que soient la demande et le niveau de stress associé, de conserver la courtoisie compatible avec la vie en collectivité dans le cadre professionnel.

La demande de support doit être établie en ayant le souci de fournir aux techniciens qui la traiteront le maximum d'information utile. À titre d'illustration, l'indication 'tel composant ne fonctionne pas' n'apporte aucune information pouvant être exploitée en vue de la résolution d'un potentiel dysfonctionnement. Il convient, par exemple, d'indiquer 'ce jour vers telle heure, j'ai tenté d'utiliser tel composant. Cette tentative s'est traduite par tel message d'erreur'. Si l'outillage proposé pour signaler une demande le permet, il est conseillé de joindre une copie d'écran.

Chaque demande de support fait l'objet, par l'équipe technique qui la reçoit, de la délivrance d'un numéro de référence (on parle souvent de numéro de ticket). En administration centrale, ces demandes d'assistance sont à soumettre par le biais de l'outil SOS-BIP. En DRAAF/DAAF, la MSI précise les conditions d'accès (dans l'espace *ad hoc* sur le site intranet du service).

Recours hiérarchique

Si, après dépôt de la demande de support, le demandeur considère que le niveau de priorité affecté au traitement de sa demande est inférieur au niveau auquel cette demande devrait être traitée, il peut effectuer un recours hiérarchique (« escalade »). Ce recours est préférentiellement assuré sous forme de courrier électronique, mais peut, en cas de crise opérationnelle, être doublée par appel téléphonique.

Pour être valable, une montée en escalade doit impérativement comprendre la référence du ticket initial. Effectuer un recours avant d'avoir ouvert un incident auprès du support n'est pas une pratique admise.

En administration centrale, le premier niveau d'escalade est le chef du bureau de l'informatique de proximité et son adjoint ; le second est le sous-directeur des systèmes d'information et son adjoint. Chaque DRAAF/DAAF précise les règles d'escalade applicables et les diffuse au niveau de son comité de direction.

Comment être formé à l’utilisation de mon poste de travail ?

Les services sont invités à encourager la formation continue des agents sur les sujets suivants, pour lesquels des offres de formations nationales et locales existent :

- maîtrise du fonctionnement du poste de travail
- maîtrise des outils bureautiques
- applications métier du MAAF

Dispositions transitoires et conclusion

La présente instruction technique rassemble, sous forme compacte et cohérente, des éléments auparavant présentés au sein de documents et de sites intranet disparates. À l'exception de la stratégie de montée en version, elle n'introduit aucune nouveauté, mais a l'ambition de donner une vision globale des problématiques associées à l'utilisation de la micro-informatique dans le contexte du système d'information du ministère.

Je vous remercie de bien vouloir me faire part, sous le présent timbre, des difficultés que vous pourriez être amenés à rencontrer dans le cadre de la mise en œuvre des présentes instructions.

La secrétaire générale,

Valérie MÉTRICH-HECQUET

Annexe

Quelques recommandations sur le choix du format d'échange de fichiers bureautiques

Le format de référence est celui issu de la norme internationale ISO 26300 OpenDocument : extensions odt (texte), ods (tableau), odp (présentation), odg (dessin), ot× (modèle de document). Ce format doit être utilisé pour les échanges de documents avec les autres services de l'État – une instruction des services du Premier ministre l'impose en particulier pour tous les envois vers les préfectures et les directions départementales interministérielles – et peut être utilisé pour tous les autres échanges. Néanmoins, pour les documents n'ayant pas vocation à être modifiés, le recours au format PDF est préférable – y compris pour les présentations.

La plaquette de présentation LibreOffice au MAAF précise les recommandations sur les formats à utiliser, recommandations applicables dans la plupart des situations de travail.

Une documentation, très complète et pédagogique, a été mise en ligne par les équipes SI du ministère chargé de l'écologie : http://bureautique.info.application.i2/libreoffice-libo-r204.html.

Les 10 commandements de la sécurité sur l'internet

http://www.securite-informatique.gouv.fr/gp_rubrique34.html

Utiliser des mots de passe de qualité. Le dictionnaire définit un mot de passe "comme une formule convenue destinée à se faire reconnaître comme ami, à se faire ouvrir un passage gardé". Le mot de passe informatique permet d'accéder à l'ordinateur et aux données qu'il contient. Il est donc essentiel de savoir choisir des mots de passe de qualité, c'est-à-dire difficiles à retrouver à l'aide d'outils automatisés, et difficiles à deviner par une tierce personne.

Avoir un système d'exploitation et des logiciels à jour : navigateur, antivirus, bureautique, pare-feu personnel, etc.

La plupart des attaques tentent d'utiliser les failles d'un ordinateur (failles du système d'exploitation ou des logiciels). En général, les agresseurs recherchent les ordinateurs dont les logiciels n'ont pas été mis à jour afin d'utiliser la faille non corrigée et ainsi parviennent à s'y introduire. C'est pourquoi il est fondamental de mettre à jour tous ses logiciels afin de corriger ces failles.

Effectuer des sauvegardes régulières

Un des premiers principes de défense est de conserver une copie de ses données afin de pouvoir réagir à une attaque ou un dysfonctionnement. La sauvegarde de vos données est une condition de la continuité de votre activité.

Désactiver par défaut les composants ActiveX et JavaScript

Les composants ActiveX ou JavaScript permettent des fonctionnalités intéressantes mais ils présentent aussi des risques de sécurité pouvant aller jusqu'à la prise de contrôle par un intrus d'une machine vulnérable. En dépit de la gêne que cela peut occasionner, il est conseillé de désactiver leur interprétation par défaut et de choisir de ne les activer que lorsque cela est nécessaire et si l'on estime être sur un site de confiance.

Ne pas cliquer trop vite sur des liens

Une des attaques classiques visant à tromper l'internaute pour lui voler des informations personnelles, consiste à l'inciter à cliquer sur un lien placé dans un message. Ce lien peut-être trompeur et malveillant. Plutôt que de cliquer sur celui-ci, il vaut mieux saisir soi-même l'adresse du site dans la barre d'adresse du navigateur. De nombreux problèmes seront ainsi évités.

Ne jamais utiliser un compte administrateur pour naviguer

L'utilisateur d'un ordinateur dispose de privilèges ou de droits sur celui-ci. Ces droits permettent ou non de conduire certaines actions et d'accéder à certains fichiers d'un ordinateur. On distingue généralement les droits dits d'administrateur et les droits dits de simple utilisateur. Dans la majorité des cas, les droits d'un simple utilisateur sont suffisants pour envoyer des messages ou surfer sur l'internet. En limitant les droits d'un utilisateur on limite aussi les risques d'infection ou de compromission de l'ordinateur.

Contrôler la diffusion d'informations personnelles

L'internet n'est pas le lieu de l'anonymat et les informations que l'on y laisse échappent instantanément ! Dans ce contexte, une bonne pratique consiste à ne jamais laisser de données personnelles dans des forums, à ne jamais saisir de coordonnées personnelles et sensibles (comme des coordonnées bancaires) sur des sites qui n'offrent pas toutes les garanties requises. Dans le doute, mieux vaut s'abstenir…

Ne jamais relayer des canulars

Ne jamais relayer des messages de type chaînes de lettres, porte-bonheur ou pyramides financières, appel à solidarité, alertes virales, etc. Quel que soit l'expéditeur, rediffuser ces messages risque d'induire des confusions et de saturer les réseaux.

Soyez prudent : l'internet est une rue peuplée d'inconnus !

Il faut rester vigilant ! Si par exemple un correspondant bien connu et avec qui l'on échange régulièrement du courrier en français, fait parvenir un message avec un titre en anglais (ou tout autre langue) il convient de ne pas l'ouvrir. En cas de doute, il est toujours possible de confirmer le message en téléphonant. D'une façon générale, il ne faut pas faire confiance machinalement au nom de l'expéditeur qui apparaît dans le message et ne jamais répondre à un inconnu sans un minimum de précaution.

Soyez vigilant avant d'ouvrir des pièces jointes à un courriel : elles colportent souvent des codes malveillants

Une des méthodes les plus efficaces pour diffuser des codes malveillants est d'utiliser des fichiers joints aux courriels. Pour se protéger, ne jamais ouvrir les pièces jointes dont les extensions sont les suivantes : .pif (comme par exemple une pièce jointe appelée "photos.pif) ; .com ; .bat ; .exe ; .vbs ; .lnk. A l'inverse quand vous envoyez des fichiers en pièces jointes à des courriels privilégiez l'envoi de pièces jointes au format le plus "inerte" possible, comme RTF ou PDF par exemple. Cela limite les risques de fuites d'informations