

Directive sécurité de l'environnement de travail V2

FEVRIER 2016



SOMMAIRE

1 - PRÉSENTATION DE LA POLITIQUE.....	4
1.1 - Contexte.....	4
1.2 - Objectif de ce document.....	4
1.3 - Périmètre d'application.....	4
1.4 - Conventions.....	4
2 - ENJEUX RELATIFS AUX POSTES DE TRAVAIL.....	6
2.1 - Typologie de postes de travail.....	6
2.2 - Typologie d'usage en sensibilité des postes.....	7
3 - ACTEURS DE LA SÉCURITÉ DE L'ENVIRONNEMENT DE TRAVAIL.....	9
3.1 - Responsable de la Sécurité des Systèmes d'Information.....	9
3.2 - Encadrants.....	9
3.3 - Utilisateurs.....	10
3.4 - Équipe support chargée des Systèmes d'Information.....	10
3.5 - Maîtrises d'ouvrage et maîtrises d'œuvre.....	11
4 - RÈGLES DE SÉCURITÉ.....	12
4.1 - Sécurité physique.....	12
4.1.1 - Sécurité physique de l'environnement de travail.....	12
4.1.2 - Sécurité physique des postes de travail.....	12
4.2 - Cycle de vie et usage des postes de travail.....	13
4.2.1 - Politique d'attribution des postes de travail.....	13
4.2.2 - Gestion du parc informatique.....	14
4.2.3 - Installation et configuration du poste.....	15
4.2.4 - Réaffectation du poste et récupération d'informations.....	16
4.2.5 - Envoi en maintenance et mise au rebut du poste.....	16
4.3 - Protection des informations.....	17
4.3.1 - Protection en termes de disponibilité.....	17
4.3.2 - Protection en termes de confidentialité.....	18
4.3.3 - Gestion des postes nomades.....	21
4.3.4 - Gestion des supports amovibles.....	22

4.4 - Exploitation.....	23
4.4.1 - Administration des systèmes.....	23
4.4.2 - Contrôle d'accès au poste de travail.....	24
4.4.3 - Gestion des droits.....	26
4.4.4 - Durcissement des configurations.....	28
4.4.5 - Gestion locale des réseaux.....	29
4.4.6 - Lutte contre les codes malveillants.....	30
4.4.6.1 - Protection contre les codes malveillants.....	30
4.4.6.2 - Protection contre les codes mobiles.....	32
4.4.7 - Mises à jour systèmes et logicielles.....	32
4.4.8 - Journalisation des événements.....	33
4.4.9 - Contrôles de conformité avec le référentiel national.....	34
4.5 - Nomadisme.....	34
4.5.1 - Principes de gestion.....	34
4.5.2 - BYOD (Bring You Own Device).....	35
4.5.3 - Connexions distantes (hors réseau du ministère).....	35
4.6 - Sécurisation des imprimantes et scanners / fax.....	37
 ANNEXES TECHNIQUES.....	 38

1 - Présentation de la politique

1.1 - Contexte

Les informations et données, ainsi que les systèmes informatiques qui permettent de les collecter, traiter, transmettre et stocker, constituent une part essentielle du patrimoine de notre ministère.

Alors que les besoins d'ouverture, de mutualisation, d'harmonisation et de flexibilité font croître l'exposition et la complexité des systèmes d'information, ils l'exposent à de multiples menaces qui évoluent en permanence et qui peuvent nuire gravement à notre activité.

Les postes de travail constituent l'interface entre les utilisateurs et les Systèmes d'Information et doivent faire l'objet d'une attention toute particulière.

1.2 - Objectif de ce document

La présente **directive de Sécurité de l'environnement de travail** s'inscrit dans la démarche de sécurisation des systèmes d'information placés sous la responsabilité du RSSI. Elle définit les règles que doivent appliquer les équipes supports en charge des postes de travail et à leur environnement.

Elle vise à protéger le matériel (postes de travail des agents) et surtout les informations qui sont traitées sur ces postes, et tous les périphériques de stockage numériques (y compris les postes de personnels externes comme ceux des prestataires intervenant dans le périmètre).

1.3 - Périmètre d'application

Cette directive s'applique à l'ensemble des postes de travail des différents services du ministère aussi bien en administration centrale qu'en services déconcentrés.

Le terme « Poste de travail » couvre dans ce document **l'ensemble des terminaux** permettant aux utilisateurs de collecter, de traiter, de supprimer, de copier et de stocker les informations sous forme numérique. Il regroupe donc les ordinateurs affectés aux utilisateurs (fixe ou portable), les téléphones fixes et téléphones intelligents (ordiphones), les tablettes, les terminaux légers ou virtuels, etc.

1.4 - Conventions

Les conventions suivantes sont adoptées dans ce document :

- Toutes les exigences de sécurité édictées dans le présent document sont numérotées et précédées de la mention « EDT » pour Environnement de travail suivi d'un indicatif de trois lettres faisant référence au chapitre dans lesquelles elles figurent.
Par exemple, la deuxième exigence du chapitre *Sécurité physique* sera précédée de l'indicatif « EDT-PHY-02 ».

- L'indicatif est complété de la lettre D ou R selon que les exigences de sécurité sont qualifiées en **Directives** ou **Recommandations**.

- ◆ Une **Directive** est **impérative** et **doit être appliquée conformément à son contenu et aux conditions d'application** sur l'ensemble du périmètre de la directive. La non-conformité à une directive doit avoir pour corollaire l'existence d'une dérogation.

La référence des exigences de sécurité considérées comme des directives est suffixée par la lettre « D ».

- ◆ Une **Recommandation** s'applique le plus largement possible sur l'ensemble du périmètre. Des contraintes spécifiques peuvent nécessiter d'y déroger. Dans ce cas, les conséquences techniques sont pleinement assumées par l'entité responsable de sa non-application. L'entité sera néanmoins amenée, dans le cadre des opérations de contrôle, à rendre compte de la raison pour laquelle elle n'applique pas une recommandation.

La référence des exigences de sécurité considérées comme des Recommandations est suffixée par la lettre « R ».

2 - Enjeux relatifs aux postes de travail

Le poste de travail constitue l'outil de travail principal de la grande majorité des agents du ministère. Ce poste de travail leur permet en particulier :

- De collecter, traiter, supprimer, recopier et stocker **des informations** dans le cadre de leur mission ;
- D'accéder aux applications métier (locales ou nationales) nécessaires à leur activité ;
- D'accéder aux ressources partagées (serveurs bureautiques, imprimantes, scanners, etc.).

Les postes de travail doivent répondre aux enjeux de sécurité du ministère, liés à ses missions :

- Des **enjeux financiers et économiques** par exemple lors de la gestion des subventions pour le logement et l'habitat ;
- Des **enjeux politiques et d'image**, par exemple en cas de fuite d'information ou de sanction prononcée par l'Union européenne, etc. ;
- Des **enjeux d'organisation**, par exemple lors de la gestion de ressources, de la comptabilité, du système d'information local, etc.

Ils doivent de plus s'adapter aux évolutions des modes de fonctionnement :

- **Mobilité accrue** : les activités des agents nécessitent de plus en plus régulièrement la connexion distante des postes de travail aux ressources de leur ministère dans le cadre de nomadisme, télétravail ;
- **Evolution des matériels** : face à la banalisation de certains matériels comme les média amovibles (clés USB, DVD, etc.) ou de terminaux mobiles légers (ordiphones, tablettes, etc.), les règles de sécurité doivent s'adapter et permettre une utilisation sécurisée de ces dispositifs.

Un poste de travail constitue un **point d'accès à l'ensemble du Système d'Information du ministère** : sa sécurité s'avère être par conséquent un élément incontournable.

2.1 - Typologie de postes de travail

La typologie de postes de travail distingue quatre catégories :

- Le **poste de travail fixe**, poste classique non destiné à être déplacé dans le cadre normal du travail de l'utilisateur et disposant à la fois d'un écran, d'une unité centrale et de périphériques de saisie (clavier, souris, écran tactile...) ;
- Le **poste de travail nomade**, poste pouvant être déplacé et utilisé dans les différents bureaux et sites géographiques du service ou à l'extérieur des locaux du service ou du ministère (domicile, lieux publics, etc.) ;
- La **tablette tactile** et l'**ordiphone**, qui se distinguent des postes nomades par leur format ultra-portable et par leurs spécificités en matière de systèmes d'exploitation, de connectique (USB, sans fil, etc.), de fonctions (agenda, mail, téléphone, etc.), de connectivité et qui permettent d'accéder à des contenus multimédias.

Sont exclus de cette catégorie les téléphones mobiles classiques.

- Le **terminal téléphonique fixe**, outil de communication de l'environnement de travail, utilisant les infrastructures réseau du ministère.

Pour chacune de ces catégories de poste de travail, trois modes d'utilisation sont distingués :

- **Poste mono-utilisateur** : le poste de travail n'est l'outil que d'un unique utilisateur ;
- **Poste multi-utilisateurs** : le poste de travail est l'outil de plusieurs utilisateurs dans son fonctionnement quotidien (par exemple, même poste utilisé par plusieurs agents) ;
- **Poste de prêt** : le poste de travail de prêt n'est généralement utilisé que par un seul utilisateur simultanément, mais cet utilisateur change régulièrement.

Les règles présentées dans cette politique s'appliquent à une ou plusieurs catégories de postes de travail et à un ou plusieurs modes d'utilisation.

Des indications précisent clairement à quelles catégories et modes d'utilisation chaque règle s'applique, son caractère obligatoire ou recommandé.

2.2 - Typologie d'usage en sensibilité des postes

L'identification des postes de travail repose sur les missions de l'utilisateur ainsi que sur la sensibilité des informations qu'il manipule. Deux catégories de sensibilité sont identifiées :

- Les **informations sensibles en disponibilité** sont les informations nécessaires au fonctionnement du service. Une perte ou une inaccessibilité temporaire à ces informations pourrait avoir des impacts importants sur la réalisation des missions du service concerné (par exemple, la gestion de crises ou la sûreté maritime peuvent être considérées comme sensibles en disponibilité) ;
- Les **informations sensibles en confidentialité** sont les informations dont la diffusion doit être limitée à certaines personnes autorisées, au sein du service ou du ministère, ou externes. Une fuite de ces informations (vers des personnes non autorisées) pourrait avoir des impacts importants sur le service concerné, ou le ministère, en termes d'image, financiers, de réalisation des missions, de santé publique, etc.

Les informations ou données personnelles au sens de la CNIL, les informations non transmissibles définies par la Commission d'Accès aux Documents Administratifs, ou les informations identifiées comme confidentielles selon d'autres réglementations peuvent notamment entrer dans cette catégorie.

Les **informations non classifiées, de niveau « diffusion restreinte »** ou supérieures doivent répondre à des règles de sécurité propres à leur niveau de classification complétant le dispositif de sécurisation (réseau physiquement distinct du réseau habituel). Le RSSI est garant de la bonne protection de ces informations conformément aux textes en vigueur.

Cette classification d'information permet aux équipes support d'adapter la configuration des postes de travail en fonction de leur niveau de sensibilité:

- **Postes standards** ;
- **Postes sensibles en disponibilité** ;
- **Postes sensibles en confidentialité.**

Ces règles constituent un référentiel de sécurité déclinable en mesures opérationnelles pouvant être mises en œuvre par les équipes support chargées des systèmes d'information.

Elles précisent un niveau minimum applicable qui peut être complété par des mesures complémentaires lorsque cela est jugé nécessaire par les personnes responsables de l'utilisation des postes de travail concernés et après avis du RSSI.

3 - Acteurs de la sécurité de l'environnement de travail

La sécurité des postes de travail implique l'ensemble des agents du ministère à différents niveaux selon leur activité.

3.1 - Responsable de la Sécurité des Systèmes d'Information

Le Responsable de la Sécurité des Systèmes d'Information (RSSI) est chargé de la Sécurité des Systèmes d'Information du service, suivant les directives exprimées par le directeur dans sa lettre de mission.

EDT-ORG-1 : Responsabilité de l'identification des postes sensibles

Le **RSSI** est responsable de la détermination et de la révision annuelle des postes sensibles en disponibilité ou en confidentialité dans son service. Il établit une liste exhaustive de ces postes sensibles et la revoit au minimum une fois par an et aussi souvent que nécessaire.

Il se base notamment sur la présente Politique et sur l'inventaire des SI sensibles réalisé au sein du service.

EDT-ORG-2 : Contrôle de l'application de la politique

Le **RSSI** est responsable de la mise en conformité des postes de travail avec la présente politique.

Il définit les contrôles annuels et effectue un rapport régulier auprès de son Directeur (AQSSI) sur le niveau de conformité, les actions en cours, et les incidents importants relatifs aux postes de travail.

3.2 - Encadrants

Les encadrants possèdent de par leur fonction hiérarchique des responsabilités en matière de sécurité des postes de travail des agents de leur service.

EDT-ORG-3 : Sensibilisation des agents

L'**encadrant** est responsable de la conduite de la sensibilisation à la sécurité des systèmes d'information des agents sous sa responsabilité.

Les utilisateurs doivent être sensibilisés régulièrement à la sécurité des systèmes d'information et plus particulièrement à la sécurité du poste de travail et de ses périphériques.

Pour les utilisateurs de postes nomades ou d'ordiphones, des sensibilisations spécifiques doivent être conduites afin de leur communiquer les risques additionnels liés à l'utilisation de ces équipements.

Les encadrants peuvent faire appel à l'équipe support chargée des systèmes d'information pour l'animation de la sensibilisation.

EDT-ORG-4 : Contrôle et remontée d'information par l'encadrant

L'**encadrant** est responsable de la communication à l'équipe support chargée des systèmes d'information des arrivées, départs ou mutations des agents de son service.

Il possède un devoir de contrôle et de remontée hiérarchique d'information en cas de détection ou de suspicion de comportement non conforme aux règles.

Il doit saisir officiellement le RSSI et l'équipe support chargée des systèmes d'Information en cas d'incident.

3.3 - Utilisateurs

L'utilisateur est impliqué à différents niveaux dans la sécurité de son poste de travail.

EDT-ORG-5 : Usage du poste de travail

L'**utilisateur** est responsable de l'usage qu'il fait de son poste de travail et de l'application des règles qui lui ont été communiquées à travers des documents spécifiques ¹.

Il doit être formé à l'utilisation de son outil de travail.

Il doit suivre l'ensemble des consignes émises par l'équipe support chargée des systèmes d'Information et ne doit pas modifier la configuration de son poste de travail.

EDT-ORG-6 : Remontée d'information par l'utilisateur

L'**utilisateur** doit signaler à l'équipe support chargée des systèmes d'information tout incident de sécurité, comportement anormal, ou vulnérabilité suspectée ou détectée sur son poste de travail.

3.4 - Équipe support chargée des Systèmes d'Information

L'équipe support chargée des systèmes d'information est responsable de l'ensemble des systèmes d'information du service. En particulier, elle a pour responsabilité la gestion des postes de travail des utilisateurs.

EDT-ORG-7 : Mise à disposition et maintien en conditions opérationnelles

L'**équipe support chargée des systèmes d'information** est responsable de la mise à disposition des utilisateurs d'un poste de travail configuré selon les règles de sécurité et du maintien en condition opérationnelle du poste de travail, notamment en ce qui concerne les règles de sécurité tant pour le poste que pour les données qui y sont stockées.

1 Livret d'accueil de l'utilisateur du SI par exemple

Cette règle inclut notamment sa responsabilité envers les utilisateurs sur la disponibilité des informations et la mise à disposition des services aux utilisateurs dans la limite des règles énoncées dans cette directive.

EDT-ORG-8 : Respect de la propriété intellectuelle (logiciels et matériels)

L'équipe support chargée des systèmes d'information est responsable du respect de la réglementation relative à la propriété intellectuelle afférente aux logiciels et matériels utilisés sur les postes de travail.

L'équipe support chargée des systèmes d'information peut organiser des sensibilisations destinées aux utilisateurs afin de leur communiquer des règles de bon usage, ou de les sensibiliser « par l'exemple », etc.

Ces sensibilisations peuvent être menées à son initiative propre ou bien à la demande du RSSI, de la direction ou de l'encadrement.

3.5 - Maîtrises d'ouvrage et maîtrises d'œuvre

Les maîtrises d'ouvrage interviennent au niveau de la définition des applications métier (étude amont, analyse fonctionnelle). Les maîtrises d'œuvre en charge de leur conception et mise en production définissent les caractéristiques de leur mise en œuvre sur postes « métier ».

EDT-ORG-9 : Sécurité des applications sur postes « métier »

Les **maîtrises d'ouvrage** sont responsables de la définition des règles relatives à la sécurisation des applications sous leur responsabilité.

Les **maîtrises d'ouvrage** sont responsables de la définition des règles de sécurité spécifiques applicables à certains postes de travail « métier » nécessitant un niveau de sécurité supérieur à ceux définis dans la politique.

4 - Règles de sécurité

4.1 - Sécurité physique

La sécurité physique des services vise à assurer un contrôle des accès aux locaux et aux infrastructures du Système d'Information en vue de pallier les intrusions physiques de tiers non autorisés ou les dangers liés aux événements naturels.

4.1.1 - Sécurité physique de l'environnement de travail

Postes sensibles en confidentialité

EDT-PHY-1-D : Protection des bureaux

Les bureaux contenant des postes sensibles en confidentialité doivent être **fermés de manière sécurisée** (clé, badge, code...) lorsqu'aucun utilisateur n'est présent.

Dans la mesure du possible, les postes sensibles en confidentialité doivent être isolés dans des bureaux particuliers (et non mélangés avec des postes de sensibilité moindre).

4.1.2 - Sécurité physique des postes de travail

La sécurisation physique des postes de travail vise à réduire les risques de vol et de destruction de matériel ou d'information.

Règles communes

EDT-PHY-2-R : Verrouillage de l'unité centrale des postes fixes

Le boîtier des unités centrales des postes de travail doit être scellé ou verrouillé par une clé. A défaut, le local dans lequel l'unité centrale est installée doit être sécurisé.

Postes nomades et postes sensibles en confidentialité

EDT-PHY-3-D : Câble de sécurité

Un **câble physique de sécurité** doit être fourni avec chaque poste sensible en confidentialité et chaque poste nomade. Les utilisateurs doivent être sensibilisés à son utilisation.

Plus généralement, il est recommandé que tout poste de travail soit équipé d'un câble de sécurité.

EDT-PHY-4-D : Continuité de fonctionnement

Les postes sensibles en disponibilité doivent faire l'objet a minima de mesures particulières destinées à assurer la continuité de fonctionnement, accès restreint et contrôlé au minimum par une porte fermée à clé et identification de toutes les personnes pouvant accéder aux postes.

4.2 - Cycle de vie et usage des postes de travail

Le processus de gestion du cycle de vie des postes de travail doit permettre une identification de la fonction de l'utilisateur afin de lui fournir un poste de travail lui permettant de mener à bien sa mission.

Le processus doit ensuite garantir une récupération et réaffectation du poste de travail par l'équipe support chargée des systèmes d'Information en cas de départ ou mutation de l'utilisateur ou changement d'usage du poste.

4.2.1 - Politique d'attribution des postes de travail

Des mesures de protection particulière doivent être mises en œuvre par les équipes de proximité pour les postes sensibles. Le service support en charge des systèmes d'information en lien avec le RSSI et les encadrants doit élaborer une politique d'attribution des postes de travail qui tiendra compte de leur usage et de leur sensibilité validée par le RSSI.

EDT-CYC-1-D : Déclaration des usages possibles des postes de travail

Le RSSI valide les usages possibles pour chaque type de poste de travail (fixe, nomade, ordiphone, etc.) et distingue ceux qui traitent des données sensibles.

Les usages non explicitement autorisés sont interdits.

EDT-CYC-2-D : Qualification des postes de travail

La sensibilité des postes doit être évaluée. La sensibilité (en disponibilité ou confidentialité) et la typologie des postes doivent être répertoriées dans l'inventaire des ressources informatiques du service.

EDT-CYC-3-D : Politique d'attribution basée sur les arrivées, mutations et départs

Le processus d'attribution des postes de travail aux utilisateurs qu'ils soient internes (titulaires, stagiaires, vacataires) ou externes (prestataires), doit s'appuyer sur le processus de gestion des arrivées, des mutations et des départs des agents du ministère.

EDT-CYC-4-D : Attribution des postes de travail et affectation

Le processus d'attribution des postes de travail aux utilisateurs doit être formalisé

Ce processus doit inclure :

- Une **demande officielle validée** par le chef de service de l'utilisateur faisant apparaître le type de poste souhaité (fixe, nomade, ordiphone) et justifiant le besoin professionnel dans le cadre d'un poste nomade ou d'un ordiphone ;
- La vérification que l'utilisateur a été **sensibilisé** aux règles de bonne utilisation de son poste de travail (notamment par la remise de documents spécifiques²).

EDT-CYC-5-R : Maîtrise de la téléphonie

Il est recommandé d'attribuer des postes téléphoniques filaires aux utilisateurs dont les échanges sont les plus sensibles et de limiter l'utilisation du protocole DECT.

EDT-CYC-6-R : Achat des matériels

Les services doivent respecter les accords-cadre interministériels pour l'achat de leur matériel sur tous les domaines sur lesquels ces accords existent.

4.2.2 - Gestion du parc informatique

La gestion du parc informatique doit permettre d'une part d'identifier les postes de travail présents sur le parc informatique et leur utilisateur, d'autre part, de suivre les logiciels, versions, et correctifs déployés.

EDT-CYC-7-D : Inventaire du parc informatique

En tant que ressources informatiques, les matériels et leur configuration doivent être répertoriés conformément aux règles édictées au sein de la *Directive de l'Hébergement informatique*.

Le RSSI doit vérifier régulièrement que l'inventaire est tenu à jour.

EDT-CYC-8-D : Fourniture et gestion maîtrisée des postes de travail

Les postes de travail utilisés dans le cadre professionnel sont fournis, configurés et gérés par l'équipe locale chargée des Systèmes d'Information.

Est interdite, la connexion d'équipements non maîtrisés, non administrés ou non mis à jour par l'équipe locale chargée des Systèmes d'Information (qu'il s'agisse d'ordiphones, d'équipements informatiques nomades et fixes ou de supports de stockage amovibles) sur des équipements et des réseaux professionnels internes.

2 Dont livret d'accueil de l'utilisateur du SI ou CGU ou messagerie

4.2.3 - Installation et configuration du poste

Un **référentiel national** recense les composants logiciels et matériels utilisés au sein des services.

EDT-CYC-9-R : Recours au référentiel national

Les composants pour la configuration des postes de travail sont ceux inscrits au référentiel national.

Ce référentiel est défini et maintenu à jour au niveau national (bureau des infrastructures), et communiqué aux équipes support chargées des systèmes d'information des différents services.

Les équipes support chargées des systèmes d'information peuvent proposer l'ajout de nouveaux composants logiciels et matériels au référentiel ; une étude est alors menée par le niveau national, qui peut ensuite valider l'insertion de ces nouveaux composants au référentiel.

EDT-CYC-10-D : Référentiel des composants logiciels et matériels

En dehors de toute interdiction, l'installation d'un **composant non inscrit** au référentiel national et hors des directives des maîtrises d'ouvrage engage la responsabilité du directeur du service et transfère la responsabilité de la gestion de ces composants (mises à jour de sécurité, support, gestion des droits d'acquisition, etc.) au niveau de l'équipe support chargée du système d'information du service.

Dans le cas où elle s'avère nécessaire, elle est effectuée sous réserve de la production

- d'une déclaration obligatoire au niveau national auprès de l'entité en charge du référentiel national et du bureau de la sécurité.
- d'une grille d'analyse de risques établie par la maîtrise d'ouvrage locale et si besoin d'une analyse de risque.

L'entité en charge des systèmes d'information au niveau national peut **interdire a posteriori** l'installation d'un logiciel ou sa mise à jour et demander sa désinstallation, notamment en cas de problèmes de compatibilité avec les autres composants du référentiel ou pour des raisons de sécurité.

EDT-CYC-11-D : Formalisation et documentation des configurations

Une procédure formalisée et documentée de configuration des postes de travail est établie par chaque entité, conformément aux directives nationales existantes.

Elle doit permettre de disposer des informations pour la configuration initiale, les mises à jour à chaque changement majeur, ainsi que les mises à jour de sécurité lors de l'installation.

4.2.4 - Réaffectation du poste et récupération d'informations

Les postes de travail peuvent être amenés à changer d'utilisateur lors d'un départ ou d'une mutation. Il convient alors de s'assurer que ces changements n'exposent pas des informations confidentielles ayant été stockées ou manipulées sur ces postes.

EDT-CYC-12-D : Réaffectation de poste de travail

En cas de réaffectation d'un poste de travail à un nouvel utilisateur, le disque dur doit être au minimum **formaté** au préalable.

Dans le cas d'un poste de travail sensible en confidentialité, le disque dur doit être **effacé de manière sécurisée**.

EDT-CYC-13-D : Récupération de données

En cas de départ ou de mutation d'un utilisateur, les données professionnelles (données stockées sur le poste de travail, présentes sur les espaces individuels réseau ou des supports amovibles) doivent être conservées par le service.

La récupération de ces données par un tiers extérieur au ministère est interdite, sauf dans les cas exceptionnels prévus par la Loi.

Les données privées de l'utilisateur ne peuvent en aucun cas être récupérées sans l'accord de ce dernier, sauf dans les cas exceptionnels prévus par la Loi.

Les données professionnelles présentes sur les postes de travail et espaces réseau individuels des utilisateurs quittant le service peuvent être conservées (par exemple sur un serveur de fichiers) pendant un délai fixé par les équipes afin d'assurer que les informations nécessaires ont été récupérées par le service « métier ».

4.2.5 - Envoi en maintenance et mise au rebut du poste

Les opérations de maintenance et la mise au rebut des supports engendrent des risques liés à la sortie d'informations hors du domaine contrôlé par le ministère.

Ces opérations doivent par conséquent être réglementées afin d'éviter les fuites d'informations appartenant aux services.

EDT-CYC-14-D : Maintenance externe

Les données **non chiffrées** stockées sur un poste de travail doivent être **effacées de manière sécurisée** avant toute opération de maintenance nécessitant le déplacement du poste hors du service.

Si ces données ne peuvent être effacées en totalité (par exemple : disque dur défectueux sous garantie), l'envoi en maintenance ne peut se faire que **sous couvert d'un engagement contractuel de confidentialité** de la part du mainteneur, ou bien dans le cadre d'une réparation sur site en présence d'un membre de l'équipe support chargée des systèmes d'Information.

EDT-CYC-15-D : Mise au rebut et recyclage

Lorsqu'un poste de travail est amené à quitter définitivement le service, les données présentes sur les disques durs ou la mémoire intégrée du poste doivent être **effacées de manière sécurisée**.

Dans le cas d'une impossibilité de procéder à un effacement sécurisé sur tout ou partie des disques ou de la mémoire (par exemple pour raison de panne ou dysfonctionnement), le support de stockage **doit être détruit(e) physiquement** avant de quitter définitivement le service.

Dans le cas où la mise au rebut ou le recyclage des postes de travail est effectué par le biais de **tiers**, un **engagement contractuel de confidentialité** entre le ministère et ces sociétés doit exister.

4.3 - Protection des informations

Les informations gérées au sein des services sont généralement stockées sur des serveurs de fichiers ou applicatifs. Certaines informations doivent néanmoins être stockées en local par exemple pour permettre une utilisation hors connexion, notamment pour les postes nomades ou les ordiphones.

4.3.1 - Protection en termes de disponibilité

Les informations stockées sur les postes de travail sont produites et traitées par les utilisateurs dans le cadre de leur mission. Il est par conséquent nécessaire de se prémunir contre leur perte : suppression involontaire ou résultant d'un acte malveillant, corruption des données, vol, etc.

Règles communes

EDT-PRO-1-R : Stockage des informations

En règle générale, les données traitées par les utilisateurs doivent être stockées sur des espaces réseau, eux-mêmes sauvegardés selon les exigences des services et en accord avec les règles de sécurité en vigueur.

EDT-PRO-2-D : Sauvegarde/synchronisation des données locales

Dans le cas où des données doivent être stockées en local, des moyens de synchronisation ou de sauvegarde doivent être fournis aux utilisateurs.

Les utilisateurs doivent par ailleurs être informés des principes retenus et des moyens mis à leur disposition.

EDT-PRO-3-D : Synchronisation automatique

Les postes sensibles en disponibilité doivent disposer d'une solution de synchronisation automatique sur les serveurs de fichiers pour les informations sensibles en disponibilité stockées en local.

Gestion des données sur les serveurs de fichiers

Les serveurs de fichiers sont utilisés par les utilisateurs pour stocker leurs données afin de travailler de manière collaborative. La gestion des serveurs de fichiers (mise à disposition, sauvegarde, nettoyage) doit par conséquent être réglementée afin de garantir le service mis à disposition des utilisateurs.

EDT-PRO-4-D : Répertoires sur les serveurs

Des répertoires adéquats doivent être mis à disposition des utilisateurs sur les serveurs de fichiers afin qu'ils puissent déposer les fichiers professionnels qu'ils gèrent et échanger des informations avec d'autres agents ou services.

Chaque utilisateur doit également disposer d'un espace individuel sur les serveurs de fichiers (par exemple pour y sauvegarder ses archives de messagerie).

L'équipe support chargée des systèmes d'Information est responsable de la disponibilité des informations stockées sur les espaces réseau partagés qu'elle met à disposition des utilisateurs.

EDT-PRO-5-D : Récupération de données locales sauvegardées

Les demandes de récupération de données à partir des sauvegardes doivent faire l'objet d'une procédure de contrôle stricte afin de s'assurer que la demande est réalisée sous contrôle du propriétaire de l'information et que cette demande est justifiée et autorisée.

4.3.2 - Protection en termes de confidentialité

Toute information traitée par le ministère possède un niveau minimum de protection d'accès. À ce titre, des mesures s'appliquent à l'ensemble des informations stockées sur chaque poste de travail.

EDT-PRO-6-D : Liste de contrôle d'accès aux données

Un système de **liste de contrôle d'accès** aux données stockées sur les postes de travail ou sur les serveurs doit être mis en place afin de garantir qu'un autre utilisateur se connectant sur le poste ne peut pas voir les données qui ne lui appartiennent pas.

Par défaut, un utilisateur n'a aucun droit d'accès aux données, quelles qu'elles soient.

Cette règle s'applique en particulier sur les postes de travail multi-utilisateurs pour lesquels un utilisateur se connectant sur le poste ne doit pas pouvoir accéder aux données ou au profil Windows d'un autre utilisateur du même poste.

Cette règle doit protéger également les données temporaires d'un utilisateur (répertoires temporaires, cache local des pages Web consultées...) et les données de configuration (registre sous Windows, etc.).

EDT-PRO-7-D : Sortie de matériel du ministère

La sortie hors du ministère de postes de travail du service doit être justifiée par un besoin de service et formalisée.

EDT-PRO-8-D : Partage de fichiers

Le partage de répertoires ou de données entre postes de travail n'est pas autorisé. L'échange de données par des plate-formes de stockage publiques (cloud public de type Dropbox, Google Drive, etc.) est formellement interdit.

Tout partage de fichiers doit être effectué de préférence à travers un dossier d'échange réseau ou un outil de travail collaboratif mis en place spécifiquement à cet usage. Il peut également être effectué par échange de media amovible (clé USB) ou par messagerie électronique.

EDT-PRO-9-D : Suppression des données du répertoire d'échange de fichiers

Les données inutiles présentes dans le répertoire d'échange de fichiers mis à disposition des utilisateurs sur un serveur de fichiers doivent être supprimées régulièrement.

EDT-PRO-10-D : Sécurité des périphériques sans fil

L'utilisation de périphériques sans fil d'entrées / sorties (clavier, écran, casque, etc.) est interdite.

L'utilisation de périphériques dont l'écoute ne permettrait pas de voler des informations (notamment souris sans fil) peut être cependant tolérée.

L'écoute d'un clavier ou d'un casque pourrait permettre le vol d'informations métier sensibles.

Tout matériel sans fil ajouté au référentiel national après une étude technique et une analyse de risques par les équipes centrales déroge implicitement à cette règle.

Postes partagés

EDT-PRO-11-D : Suppression des données sur les postes partagés

Les données présentes sur les postes partagés (par exemple portable de prêt) doivent être supprimées entre deux utilisateurs.

Les données temporaires (données en cache par exemple) doivent être supprimées à chaque reconnexion.

Postes sensibles en confidentialité

EDT-PRO-12-D : Chiffrement sur les postes sensibles en confidentialité

Les postes sensibles en confidentialité (PC portables entre autres) doivent bénéficier d'une solution de chiffrement protégeant les informations stockées. Les moyens de chiffrement sont adaptés au support (postes et serveurs, espaces de travail, données temporaires et fichiers cache/échange du système).

Les informations sensibles en confidentialité doivent être chiffrées quel que soit le support.

La solution de chiffrement est déterminée au niveau central et incluse au référentiel national. Dans la mesure du possible, cette solution doit être transparente pour l'utilisateur.

EDT-PRO-13-D : Sauvegarde des informations chiffrées

Lors des opérations de stockage de fichiers chiffrés sur des espaces réseau ou pour les sauvegardes et les archivages, la confidentialité des données doit être assurée par des dispositifs de robustesse équivalente à ceux qui protègent les données stockées sur les postes de travail.

En particulier, dans le cas où des données sont chiffrées sur un poste de travail, les sauvegardes de ces données sont elles aussi chiffrées ; par conséquent un administrateur réseau ne peut avoir accès à ces informations.

EDT-PRO-14-D : Recouvrement des données chiffrées

La solution de chiffrement sur espace partagé préconisée par le niveau national définit une organisation et des droits de recouvrement propres.

En dehors de cette solution, l'équipe support chargée des systèmes d'Information doit formaliser son niveau d'engagement vis-à-vis du recouvrement des informations chiffrées en cas de perte ou d'indisponibilité des secrets assurant le chiffrement (mots de passe, certificats, etc.).

Elle doit ensuite mettre en place et contrôler régulièrement les procédures nécessaires au recouvrement des informations chiffrées en cohérence avec son engagement.

4.3.3 - Gestion des postes nomades

Le stockage local d'informations sur les postes nomades est souvent nécessaire pour assurer une continuité de l'activité en dehors du service, par exemple dans le cadre de déplacements professionnels. Les informations stockées doivent par conséquent être contrôlées afin d'éviter leur perte ou leur fuite en cas de perte ou de vol du poste.

EDT-PRO-15-D : Stockage local d'information

Le stockage local d'information sur les postes de travail nomades et ordiphones doit être limité au strict nécessaire.

Les données stockées sur ces types de postes doivent être soumises aux règles de sécurité correspondant à leur niveau de sensibilité (non sensible, sensible en disponibilité, sensible en confidentialité).

Les informations sensibles en disponibilité ne doivent pas être stockées exclusivement sur un poste nomade ou un ordiphone. Des copies de ces informations doivent être disponibles (sur un serveur, sur un autre poste, sous la forme de documents papiers, etc.).

L'utilisation de postes de travail nomades sensibles en confidentialité doit être évitée dans des lieux publics

EDT-PRO-16-D : Mot de passe BIOS

Un mot de passe BIOS doit être implémenté sur chaque poste de travail nomade.

EDT-PRO-17-D : Chiffrement des disques durs

Les postes de travail nomades doivent comporter une solution de chiffrement des disques durs afin de protéger les informations stockées localement.

EDT-PRO-18-D : Filtre de confidentialité

Pour les postes de travail nomades sensibles en confidentialité, un filtre de confidentialité doit être fourni. Il est obligatoirement positionné sur l'écran dès lors que le poste est utilisé en dehors des locaux du service.

Un filtre de confidentialité est un dispositif optique à placer devant l'écran du portable limitant les angles de vision de l'écran notamment sur les côtés et vers le haut afin d'éviter à un tiers de pouvoir voir l'écran. Ces filtres sont disponibles pour tous les postes portables et pour les ordiphones.

4.3.4 - Gestion des supports amovibles

Les supports amovibles sont par définition les supports de type clé USB, disque dur externe, CD-ROM, DVD-ROM, etc. De par leur format et leur utilisation, ils sont davantage exposés aux pertes, vols ou indiscretions.

Règles communes

EDT-PRO-19-R : Fourniture de clés USB et disques externes

Autant que possible, les clés USB et disques durs externes doivent être fournis aux utilisateurs par l'équipe support chargée des systèmes d'Information.

Ces supports amovibles doivent être récupérés par l'équipe support chargée des systèmes d'information lorsqu'ils ne sont plus utiles ou s'ils sont défectueux.

L'utilisation de clés USB à connexion sans fil est interdite (par exemple clé USB *Bluetooth*).

Les clés USB constituent un des principaux vecteurs des infections virales.

L'utilisateur s'engage à n'utiliser que des clés professionnelles dans l'environnement informatique du ministère (pas de connexion sur son ordinateur personnel notamment).

EDT-PRO-20-D : Confidentialité des informations stockées

La confidentialité des données stockées sur des supports amovibles (CD, DVD, clé USB, disque dur externe) doit être assurée par des dispositifs de robustesse équivalente à ceux qui protègent les mêmes données stockées sur les postes de travail.

Notamment, une solution de chiffrement doit être proposée pour des données confidentielles stockées sur de tels supports amovibles. Des mesures supplémentaires de protection physique de ces supports peuvent être mises en place (stockage en coffre, surveillance continue pendant l'utilisation, remise en main propre en cas d'échange, traces des copies et des échanges, etc.).

EDT-PRO-21-D : Stockage d'information sur des media amovibles

Les clés USB ne doivent pas servir de media de stockage permanent mais uniquement de moyen d'échange.

EDT-PRO-22-D : Analyse automatique des supports amovibles

À la connexion d'un support amovible, son contenu doit être automatiquement analysé par l'antivirus avant utilisation afin de se prémunir contre les codes malveillants.

En cas de détection d'une anomalie, le code malveillant doit être supprimé par l'antivirus, ou au minimum, mis en quarantaine. Dans ce dernier cas, le support amovible ne doit plus être utilisé et doit être remis au service de proximité pour analyse.

EDT-PRO-23-D : Exécution automatique à partir des supports amovibles

L'exécution automatique à la connexion d'un support amovible (« autorun ») doit être désactivée.

Cette règle permet d'éviter des infections ou des vols d'information par des supports amovibles « piégés ». Une communication devra néanmoins être adressée aux utilisateurs pour expliquer comment accéder au contenu stocké sur ce type de support.

EDT-PRO-24-D : Mise au rebut de supports amovibles

Tout support amovible devant être mis au rebut (fin de vie, défectueux...) doit être préalablement effacé de manière sécurisée ou si cela n'est pas possible³, détruit (cf. règles 4.2.5).

Cas spécifiques des disques durs externes sans fil

EDT-PRO-25-D : Interdiction des disques durs sans fil

L'utilisation de disques durs externes à connexion sans fil est interdite (par exemple disques durs *Wi-fi* ou *Bluetooth*).

4.4 - Exploitation

L'exploitation et l'administration des postes de travail nécessitent des privilèges et des outils spécifiques pour les membres de l'équipe en charge des Systèmes d'Information. Ces outils ou privilèges permettent généralement de nombreux paramétrages sur le parc et engendrent notamment des risques d'erreur ou d'accès par une personne non autorisée.

4.4.1 - Administration des systèmes

EDT-EXP-1-D : Restriction des droits d'administration

Sauf exception dûment motivée et validée par le RSSI, les utilisateurs n'ont pas de droits d'administration.

EDT-EXP-2-D : Procédures de gestion des incidents et des demandes

La gestion des incidents et des demandes concernant les postes de travail doit faire l'objet d'un processus formalisé et outillé dans le respect des règles en vigueur définies dans la Politique Générale de Sécurité des Systèmes d'Information du ministère.

Cela signifie notamment qu'un outil de gestion des incidents et des demandes doit être mis en place par l'équipe support chargée des systèmes d'Information de chaque service concerné. Cet outil doit être déterminé au niveau national et inscrit dans le référentiel national.

³ Media non effaçables, media défectueux...

EDT-EXP-3-D : Utilisation exceptionnelle du compte de l'utilisateur

L'utilisation du compte de l'utilisateur par un membre de l'équipe en charge des Systèmes d'Information est proscrite.

Dans des cas très exceptionnels, il est possible à condition que l'utilisateur l'accepte explicitement, que l'opération s'effectue sous surveillance de l'utilisateur et que le changement de mot de passe intervienne immédiatement après.

Cette utilisation ne doit pas aller à l'encontre des règles de sécurité présentées dans cette politique.

EDT-EXP-4-D : Gestion de la prise en main à distance

La prise en main à distance d'un poste de travail ne doit être réalisable que par les agents de l'équipe support chargée des systèmes d'Information, sur les postes de travail de leur périmètre et à condition que l'utilisateur l'accepte explicitement.

En particulier, la télémaintenance de postes de travail par un tiers extérieur au ministère est interdite, sauf en cas d'un raccordement au niveau national soumis préalablement à une analyse de risque et à la signature d'un engagement de confidentialité.

EDT-EXP-5-D : Protection des prises en main à distance

Les outils de prise en main à distance doivent faire l'objet de mesures de durcissement et figurer dans le référentiel national.

Toute solution utilisant le déport ou transit de données sur un serveur externe est interdit.

La prise en main à distance sur un poste de travail ne peut se faire qu'après acceptation de l'utilisateur : la simple indication téléphonique ne suffit pas, elle doit correspondre à une action sur le poste de travail (validation sur une fenêtre *pop-up* par exemple). L'utilisateur doit également pouvoir mettre fin à la session à tout moment.

4.4.2 - Contrôle d'accès au poste de travail

Toute action conduite sur ou à partir d'un poste de travail ou d'un terminal téléphonique fixe doit être soumise à une authentification préalable de l'utilisateur.

Postes de travail fixes et nomades

EDT-EXP-6-D : Identification de l'utilisateur

Chaque utilisateur doit disposer d'un **identifiant** (login) individuel pour ouvrir une session sur son poste de travail et sur un terminal téléphonique fixe.

Le libellé de l'identifiant ne doit révéler aucune information sur le niveau de privilèges ou de droits d'accès de l'utilisateur.

EDT-EXP-7-D : Authentification de l'utilisateur

L'authentification d'un utilisateur par mot de passe individuel doit être nécessaire pour accéder à un poste de travail et à un terminal téléphonique fixe.

Les paramétrages et secrets permettant l'authentification ne doivent pas être visibles en clair par les utilisateurs.

Des mesures doivent être prévues pour limiter le nombre de tentatives de connexion, telles que la mise en place d'un blocage après un trop grand nombre d'échecs.

L'activation de l'écran de veille doit être systématique et comporter un verrouillage en cas d'inactivité (préconisé : supérieur à 5 mn)

EDT-EXP-8-D : Politique de mot de passe

Les mots de passe doivent respecter la **politique de mot de passe** communiquée par le ministère. Des moyens techniques doivent être mis en place à cet effet.

Les règles devant être respectées par les mots de passe des postes de travail et des terminaux téléphoniques fixes sont rappelées en annexe.

EDT-EXP-9-D : Initialisation des mots de passe

Chaque compte utilisateur doit être créé avec un **mot de passe initial aléatoire unique**.

Il doit être transmis de manière sécurisée à l'utilisateur (le transfert ne doit pas pouvoir être intercepté et l'identité de l'utilisateur doit être assurée au moment du transfert).

L'utilisateur doit être contraint de le modifier lors de sa première connexion.

EDT-EXP-10-D : Gestion des mots de passe

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

Les mots de passe ne doivent pas apparaître en clair à l'écran lors de leur saisie.

Les utilisateurs doivent conserver la possibilité de changer leurs mots de passe à tout moment, mais dans la mesure du possible ne doivent pas pouvoir changer de mot de passe plusieurs fois dans un intervalle de temps réduit.

Après installation d'une application ou d'un système, les mots de passe par défaut doivent immédiatement être modifiés.

Les mots de passe doivent obligatoirement être renouvelés tous les 6 mois.

EDT-EXP-11-D : Coffre-fort de mots de passe / de secrets

Des coffres-forts de mots de passe ou de secrets (clés privées / certificats) peuvent être mis en place afin de faciliter l'utilisation des logiciels en évitant aux utilisateurs d'avoir à se souvenir de tous leurs mots de passe.

Seuls les composants validés par les équipes nationales dans le cadre d'une étude

de sécurité peuvent être utilisés.

EDT-EXP-12-D : Comptes utilisateur génériques

L'utilisation de comptes utilisateur génériques est interdite.

EDT-EXP-13-D : Désactivation des comptes

Les comptes des utilisateurs quittant le service (départ ou mutation) doivent être **désactivés** dès leur départ.

Les comptes inactifs pendant plus de trois mois doivent automatiquement être **désactivés**.

Les comptes des utilisateurs externes (prestataires, etc.) doivent être **désactivés** automatiquement à la date de fin de leur contrat.

Postes sensibles en disponibilité

EDT-EXP-14-D : Mots de passe des postes sensibles en disponibilité

Un mécanisme de **recouvrement** permettant de retrouver dans un délai acceptable par le service l'accès à un poste de travail sensible en disponibilité en cas de perte de cet accès doit être mis en place.

Un tel mécanisme peut inclure notamment une enveloppe scellée gardée dans un coffre sécurisé et contenant des informations sur un identifiant et un mot de passe d'un compte de recouvrement.

4.4.3 - Gestion des droits

Une gestion rigoureuse des privilèges systèmes et des droits d'accès locaux permet de limiter les risques d'erreurs des utilisateurs et participe à la lutte contre les codes malveillants et les attaques sur les postes.

Règles communes

EDT-EXP-15-D : Droits des utilisateurs

La gestion des droits des utilisateurs sur leur poste de travail doit suivre le principe du « **moindre privilège** » : chaque utilisateur ne doit disposer que des droits nécessaires pour lui permettre de conduire les actions relevant de sa mission ; ainsi que le principe du « **besoin d'en connaître** » : chaque utilisateur n'est autorisé à accéder qu'aux ressources pour lesquelles on lui accorde le bénéfice de l'accès.

Les comptes privilégiés doivent être utilisés uniquement pour les opérations le nécessitant (par exemple opérations de support et d'administration technique).

Les applications ou composants logiciels utilisé(e)s sur les postes rendant nécessaire l'attribution de privilèges élevés (« utilisateur avec pouvoir » ou « administrateur local ») à des utilisateurs doivent être identifiés.

La liste de ces applications et postes de travail doit être identifiée au niveau national qui peut prendre, le cas échéant, les dispositions souhaitées (par exemple plan de remplacement de ces applications, procédure de paramétrage spécifique du système⁴, etc.).

EDT-EXP-16-D : Droits d'accès locaux

Des droits d'accès locaux doivent être mis en place pour s'assurer que les utilisateurs n'ont pas d'accès :

- Aux paramétrages et fichiers système et notamment à la configuration sécurité du poste sauf besoin spécifique (mise à jour avec compte utilisateur par ex) ;
- Aux profils d'autres utilisateurs stockés en local ;
- Aux répertoires de stockage nominatifs locaux d'autres utilisateurs, y compris répertoires temporaires ou cache (exemple : navigateur).

EDT-EXP-17-D : Revue des comptes utilisateurs

Les comptes des utilisateurs présents dans l'annuaire bureautique doivent être revus au minimum de façon annuelle par l'équipe support chargée des systèmes d'Information du service qui en informe le RSSI.

Les comptes inactifs depuis plus de trois mois doivent être supprimés sauf cas particuliers examinés par le RSSI.

La désactivation des comptes inactifs permet d'interdire l'accès au compte tout en conservant la traçabilité des actions effectuées par le propriétaire du compte. Au-delà de la durée prévue dans la règle « EDT-EXP-41-D : Journalisation des événements », les comptes peuvent être supprimés.

EDT-EXP-18-D : Activités nécessitant une élévation des privilèges

Les activités particulières nécessitant une élévation des droits de l'utilisateur ou un changement de la configuration système ou sécurité du poste de travail (développement, tests, etc.) doivent être menées à partir de **postes spécifiques** mis à disposition des utilisateurs pour ces activités (autres que leurs postes de travail bureautiques). Ces postes doivent être **soumis à des règles de sécurité particulières** et notamment isolés sur des réseaux contrôlés. Ils doivent de plus être référencés afin de permettre une réaction rapide en cas d'incident (par exemple en cas d'infection virale sur un poste de test).

L'utilisation de données sensibles sur ces postes spécifiques doit être explicitée, motivée et soumise à une analyse de risque préalable.

Les agents de l'équipe support chargée des systèmes d'Information nécessitant **une élévation ponctuelle des privilèges** sur leur poste de travail peuvent utiliser une fonction de type « Exécuter en tant que » (par exemple pour des activités d'administration).

Le RSSI du service doit détenir une liste à jour de ces postes

4 Par exemple : modification de droits NTFS sur des fichiers systèmes ou de droits sur les clés de registre

Les activités de développement ou de tests ne demandant pas de privilèges particuliers sur les postes (par exemple développement de bases de données) ne sont pas concernées par cette règle.

L'isolement d'un poste du réseau bureautique pourra être réalisé par une séparation physique ou logique des réseaux

La mise en place de postes virtuels (sur un serveur ou poste de travail) peut également être réalisée pour fournir un environnement sécurisé pour les activités nécessitant une élévation des privilèges uniquement si ces postes virtuels sont segmentés du reste du réseau bureautique (y compris du système hôte).

Dans le cas où le cloisonnement est difficile à mettre en place, et sous couvert d'une acceptation du risque par le RSSI, un mécanisme de cloisonnement logique/physique d'urgence en cas d'incident ou de crise uniquement peut se substituer à un cloisonnement permanent.

4.4.4 - Durcissement des configurations

Afin d'éviter les modifications accidentelles ou intentionnelles des configurations du poste de travail pouvant nuire à son fonctionnement, des règles de configuration strictes des postes doivent être mises en œuvre.

EDT-EXP-19-D : Durcissement des configurations

La configuration des systèmes d'exploitation et des applications sur les postes de travail doit être durcie afin de limiter les droits des utilisateurs sur des fonctions systèmes et de renforcer la sécurité du poste par rapport à des attaques externes.

Un délai de verrouillage de l'accès du poste en cas d'inactivité de 5 à 15 minutes est recommandé sur l'ensemble des postes de travail.

EDT-EXP-20-R : Mot de passe disque dur

Un mot de passe disque dur doit être mis en place sur l'ensemble des postes de travail.

Le mot de passe peut être identique sur l'ensemble des postes du parc informatique. Il permet de limiter les risques liés au vol de poste par un tiers extérieur au service. La gestion de ce mot de passe peut rapidement devenir complexe : peu de solutions de recouvrement en cas de perte, aucune solution de modification du mot de passe sur l'ensemble des postes, etc.

EDT-EXP-21-R : Installation de plusieurs systèmes d'exploitation

Dans la mesure du possible, chaque poste de travail doit être installé avec un seul système d'exploitation (absence de multiboot).

Dans le cas où plusieurs systèmes d'exploitation doivent être installés sur un même poste de travail, chaque système doit être conforme à l'ensemble des règles énoncées dans cette politique.

Par ailleurs, les utilisateurs doivent être sensibilisés aux risques spécifiques liés à l'utilisation de plusieurs systèmes d'exploitation sur un même poste de travail.

Les systèmes multiboot doivent donc assurer au minimum la mise à jour régulière des composants et permettre une gestion centralisée des configurations. Ils doivent être installés sous la responsabilité de l'équipe support chargée des systèmes d'information.

EDT-EXP-22-D : Utilisation de systèmes virtuels

Dans le cas où plusieurs systèmes d'exploitation virtuels sont utilisés et/ou stockés sur un poste de travail, chaque système virtuel doit être conforme à l'ensemble des règles énoncées dans cette politique.

Cette règle peut cependant ne pas s'appliquer si le système virtuel est complètement isolé du système hôte et du réseau bureautique.

Par ailleurs, les utilisateurs doivent être sensibilisés aux risques spécifiques liés à l'installation de différents systèmes d'exploitation sur un même poste de travail.

Les systèmes virtuels doivent donc assurer au minimum la mise à jour régulière des composants et permettre une gestion centralisée des configurations. Ils doivent être installés sous la responsabilité de l'équipe support chargée des systèmes d'Information.

4.4.5 - Gestion locale des réseaux

Une identification des postes présents sur le réseau permet de garantir l'absence d'intrusion de postes non maîtrisés pouvant engendrer un risque pour la sécurité de l'ensemble du Système d'Information du service.

EDT-EXP-23-D : Postes autorisés sur le réseau

Seuls les postes de travail **maîtrisés** par l'équipe support chargée des systèmes d'Information du service et **conformes au niveau de l'application des règles** de sécurité peuvent être reliés au réseau local du service.

Les ordiphones ou tablettes non fournis par l'équipe support chargée du SI ne doivent pas être connectés au réseau ou à un poste de travail du ministère ni synchronisés avec les ressources du ministère, sauf exceptions explicitement autorisées et documentées (par exemple la messagerie qui est un service accessible depuis n'importe quel poste banalisé).

EDT-EXP-24-D : Services réseau

Les postes de travail ne doivent pas mettre en œuvre de services réseau tels que le routage (entre deux interfaces réseau physiques ou entre machines virtuelles) ou la résolution locale des noms de machines (l'utilisation de DNS réseau est obligatoire)

EDT-EXP-25-D : Connexion à plusieurs réseaux, accès à Internet

La connexion d'un poste de travail à **plus d'un réseau** simultanément est formellement interdite. Ceci inclut les réseaux filaires et sans fil (wi-fi, Bluetooth...).

Les accès spécifiques à Internet nécessitant des droits particuliers pour un usage métier ne peuvent être mis en place que sur dérogation dûment justifiée, et sur des machines isolées physiquement et séparées du réseau de l'entité, après validation préalable du RSSI.

EDT-EXP-26-D : Connexion sans fil des postes fixes

Les postes de travail fixes ne doivent pas utiliser les interfaces réseau sans fil en dehors des cas prévus par l'équipe support chargée des systèmes d'Information et identifiés dans le cadre d'une étude sécurité.

Si les postes de travail fixes disposent d'interfaces réseau sans fil (wi-fi, Bluetooth...), ces interfaces doivent être désactivées.

La désactivation des interfaces se fera de préférence physiquement (débranchement des interfaces / suppression des cartes filles), ou si nécessaire le plus bas possible dans les couches de gestion matérielles (BIOS).

4.4.6 - Lutte contre les codes malveillants

Face à l'apparition de nouveaux virus sur Internet et la détection régulière de nouvelles failles de sécurité sur les systèmes d'exploitation et applications utilisés, un ensemble de règles de sécurité doit protéger les postes de travail et les informations contre les codes mobiles et malveillants.

La lutte contre ces codes s'effectue au niveau du réseau pour les accès vers des réseaux publics (Internet) ou non maîtrisés (partenaires), ainsi qu'au niveau des postes de travail et serveurs.

4.4.6.1 - Protection contre les codes malveillants

Postes fixes et postes nomades

EDT-EXP-27-D : Installation d'un antivirus

Un antivirus doit être installé sur l'ensemble des postes de travail des utilisateurs.

EDT-EXP-28-D : Protection des paramètres de configuration

L'utilisateur ne doit pas pouvoir désactiver l'antivirus de son poste ni modifier ses paramètres.

L'accès au menu de l'antivirus par l'utilisateur doit être limité au lancement d'un scan d'une zone définie (fichier, répertoire, partition, etc.), à la vérification des bases de signatures et du moteur installés, et à une demande de mise à jour de ces bases de signatures ou du moteur.

EDT-EXP-29-D : Analyse des postes de travail

L'antivirus présent sur les postes de travail doit être configuré pour réaliser une analyse complète des disques locaux au moins de façon hebdomadaire.

Les médias amovibles doivent être scannés a minima à l'accès aux fichiers, l'utilisateur doit pouvoir lancer un scan à volonté.

La programmation de cette analyse est placée sous la responsabilité de l'équipe chargée du SI de manière à perturber au minimum le fonctionnement du service :

- Soit en heures ouvrées en cherchant à limiter les perturbations utilisateurs (heures creuses, limitation de la charge système allouée à l'analyse) ;
- Soit en heures non ouvrées dans le respect des règles liées au développement durable (extinctions des ordinateurs ...).

EDT-EXP-30-D : Gestion des événements

Les événements de sécurité de l'antivirus doivent être remontés sur un serveur national pour analyse statistique et gestion des problèmes *a posteriori* (exemples : poste constamment infecté, virus détecté et non éradiqué par l'antivirus, etc.).

Cette remontée pourra s'appuyer sur des serveurs locaux suivant les recommandations émises par les services en charge de la sécurité.

EDT-EXP-31-D : Mesures en cas de contamination avérée

Lorsque la pollution d'un système est confirmée, il doit être isolé physiquement (débranchement réseau et électrique). Aucune action n'est ensuite autorisée sur le système et une alerte est remontée.

EDT-EXP-32-D : Mise à jour de la base de signatures

Les mises à jour de bases antivirales et de moteurs d'antivirus doivent être mises à disposition par les services nationaux en charge de la sécurité et déployées automatiquement sur les postes de travail par un dispositif prescrit par ce même service.

Une mise à jour d'urgence doit également pouvoir être programmée par les équipes nationales ou locales sur l'ensemble des postes de travail.

Ordiphones

EDT-EXP-33-R : Antivirus sur les ordiphones

Dans la mesure du possible un antivirus devrait être installé sur l'ensemble des ordiphones.

L'antivirus doit assurer une **analyse en temps réel des** fichiers lus ou écrits à partir du poste, des pages Web visitées (Internet ou Intranet) et des composants associés, ainsi que des téléchargements effectués depuis le Web, des courriels reçus et envoyés depuis le poste.

La base de signatures antivirales doit être mise à jour régulièrement.

Dans la mesure du possible, l'utilisateur ne doit pas pouvoir désactiver l'antivirus ni modifier ses paramètres.

4.4.6.2 - Protection contre les codes mobiles

Les codes mobiles sont des codes s'exécutant à travers le navigateur Web et présentant des risques au même titre que les autres exécutables. La protection contre ces codes implique la mise en place d'une configuration spécifique du navigateur.

EDT-EXP-34-D : Configuration du navigateur

Une configuration sécurisée du navigateur doit être déployée sur l'ensemble des postes de travail par l'équipe support chargée des systèmes d'Information.

Cette configuration doit être définie, formalisée et maintenue à jour au niveau national.

EDT-EXP-35-R : Protection de la configuration du navigateur

L'utilisateur ne doit pas être autorisé à modifier la configuration du navigateur ou installer des extensions.

Les extensions installées doivent être validées au niveau national et déployées sur les postes de travail par l'équipe support chargée des systèmes d'Information du service.

4.4.7 - Mises à jour systèmes et logicielles

Afin de maintenir le niveau de sécurité face à l'apparition régulière de nouvelles menaces, une veille sécurité performante permet d'assurer d'une part l'analyse des alertes recensées et d'autre part l'application de mesures nécessaires pour pallier ces menaces.

EDT-EXP-36-D : Veille sécurité

Une veille sécurité doit être mise en place au niveau national pour qualifier les failles de sécurité sur l'ensemble des composants présents au référentiel national.

L'équipe support chargée des systèmes d'Information du service est responsable de la veille sécurité des composants utilisés non-inscrits au référentiel national.

EDT-EXP-37-D : Déploiement des correctifs de sécurité

Les correctifs à déployer sur les postes de travail, concernant les composants du référentiel national, sont prescrits et mis à disposition par les services nationaux en charge de la sécurité. Ils sont déployés sous la responsabilité du niveau national puis local en fonction des dispositifs disponibles.

Le déploiement sur les postes de travail de correctifs concernant des composants hors référentiel national est fait sous la responsabilité de l'équipe locale chargée des SI.

EDT-EXP-38-D : Télédistribution de logiciels et mises à jour

La gestion des correctifs de sécurité et leurs mises à jour sur les postes de travail doit faire l'objet d'une procédure formalisée et outillée.

Un outil de télédistribution permettant de déployer les logiciels et les mises à jour doit être mis en place.

EDT-EXP-39-D : Procédure de crise

En cas d'alerte émise par le niveau national pour l'application urgente d'un correctif de sécurité, l'équipe support chargée des systèmes d'Information du service suit les recommandations qui lui ont été communiquées dans l'alerte.

EDT-EXP-40-D : Évolutions majeures

Les évolutions majeures (service pack, nouvelle version logicielle, etc.) doivent faire l'objet d'un processus spécifique de qualification avant déploiement, selon les consignes des services nationaux.

4.4.8 - Journalisation des événements

La journalisation des événements importants permet d'identifier les responsabilités des différents acteurs en cas d'incident, ou d'enquête administratives.

EDT-EXP-41-D : Journalisation des événements

Les événements importants des postes de travail et les serveurs assurant la connexion de ces postes aux ressources du réseau doivent être conservés durant une durée conforme à la réglementation en vigueur :

- Accès système acceptés ou refusés ;
- Modification des configurations ou des paramètres de protection, intervention de maintenance ;
- Utilisation de privilèges ou accès aux utilitaires systèmes/applications ;
- Alertes systèmes critiques ou majeures ;
- Alertes de sécurité (antivirus, pare-feu...).

Une durée de conservation d'une année est recommandée.

EDT-EXP-42-D : Collecte et analyse des traces

Les journaux d'événements relatifs aux postes de travail et stockés sur les serveurs doivent être collectés et analysés régulièrement avec les outils appropriés selon une procédure validée par le RSSI.

EDT-EXP-43-D : Cadre légal

Les contraintes légales en matière de journalisation doivent être respectées. En particulier, les utilisateurs doivent être prévenus de l'existence et du contenu des traces informatiques les concernant afin d'assurer leur exploitabilité en cas de litige.

EDT-EXP-44-D : Protection des informations journalisées

Les informations journalisées doivent être protégées selon les règles explicitées dans la Politique Générale de Sécurité des Systèmes d'Information du ministère.

4.4.9 - Contrôles de conformité avec le référentiel national

EDT-EXP-45-D : Vérification automatique de la conformité

Afin de maintenir dans le temps les éléments de configuration des postes de travail, l'outil national de vérification régulière de la conformité de ces éléments doit être mis en place.

Cet outil permet une remontée centralisée.

4.5 - Nomadisme

Les postes nomades et ordiphones sont exposés à davantage de menaces que les postes de travail fixes en raison de leur utilisation hors du domaine contrôlé par le ministère.

L'utilisation notamment d'ordiphones amplifie les risques liés à l'utilisation de postes nomades : les vols ou pertes d'ordiphones sont plus courants et se détectent tardivement (en particulier en raison de leur taille réduite) la complexité des mots de passe utilisés est moindre, les solutions de sécurité sont moins matures que sur les autres types de postes de travail (antivirus, pare-feu), offrant par exemple des possibilités d'interception des communications sans fil de ces postes facilitées par rapport aux postes nomades classiques.

4.5.1 - Principes de gestion

EDT-NOM-1-D : Connexion des postes pour mise à jour

Les postes nomades doivent être connectés au réseau local à raison d'une journée par mois au minimum afin de réaliser les mises à jour nécessaires.

EDT-NOM-2-D : Usage professionnel des postes nomades

Les besoins exprimés en vue de l'acquisition de postes nomades correspondent à des usages professionnels. En conséquence, seuls les dispositifs agréés et installés par le ministère sont autorisés.

4.5.2 - BYOD (Bring You Own Device)

Le “Bring You Own Device” est une pratique qui consiste à utiliser ses équipements personnels (téléphone, ordinateur portable, tablette électronique) dans un contexte professionnel. Cette pratique pose des questions relatives à la sécurité de l'information et à la protection des données, ainsi que sociales et juridiques.

EDT-NOM-3-D : Interdiction des usages BYOD

L'usage d'un poste de travail ou ordiphone personnel dans le cadre professionnel est interdit.

EDT-NOM-4-D : Usages tolérés

Les usages professionnels suivants sont cependant tolérés sur les équipements personnels : consultation de la messagerie, du calendrier, des contacts.

Les équipements personnels sont interdits dans l'usage de données sensibles.

Des moyens techniques et organisationnels doivent être mis en place par les services pour limiter la synchronisation de la messagerie sur les équipements personnels.

La synchronisation de la messagerie ne doit être possible qu'après la mise en place d'un code de verrouillage à 6 chiffres et la signature des conditions générales d'utilisation.

EDT-NOM-5-D : Protection des données sensibles

Il est interdit d'ouvrir des pièces jointes sensibles à partir d'un équipement personnel.

4.5.3 - Connexions distantes (hors réseau du ministère)

Les postes nomades peuvent potentiellement être davantage confrontés aux menaces de par leur utilisation en dehors du service et leur raccordement à des Systèmes d'Information non contrôlés ne présentant aucune des protections présentes sur le réseau du ministère.

Postes nomades

EDT-NOM-6-D : Mise à disposition d'une solution VPN

Une solution VPN (« Virtual Private Network », ou réseau privé virtuel) doit être mise en œuvre pour autoriser la connexion à distance des postes nomades au Système d'Information des services.

Une solution VPN permet aux utilisateurs d'accéder à distance à certaines ressources disponibles sur le Système d'Information et de travailler directement de façon nomade. Cette solution permet également de réduire la quantité de fichiers stockés sur les postes nomades et limite ainsi les conséquences d'un vol ou d'une perte du poste.

EDT-NOM-7-D : Ressources disponibles via la connexion VPN

Les ressources accessibles aux postes nomades et ordiphones en utilisation VPN sont identifiées au niveau national.

Une procédure de mise à disposition d'une nouvelle ressource, comprenant notamment une analyse de risque, devra être formalisée.

EDT-NOM-8-D : Accès réseau en situation de nomadisme

Un dispositif de sécurité de type pare-feu personnel, prescrit par le niveau national, doit permettre de filtrer les échanges réseau sur le poste de travail en situation de nomadisme.

Ces accès doivent être autorisés à travers :

- Les connexions Ethernet et points d'accès Wi-fi permettant un accès direct à Internet (sans authentification préalable sur un portail opérateur ou local) ;
- Les bornes Wi-fi spécifiquement mises en place au Ministère et sécurisées par les équipes nationales (exemple : bornes implantées dans les locaux du ministère offrant des solutions de mobilité) ;
- *(pour les utilisateurs nomades intensifs uniquement)* Les réseaux de données radio des opérateurs agréés par l'entité chargée du service national à travers une carte de communication remise spécifiquement.

Les accès autres en situation de nomadisme (itinérance téléphonique à l'international, accès à travers des accès Wifi opérateurs ou nécessitant une authentification par portail, etc.) doivent être étudiés spécifiquement et seront attribués uniquement sur dérogation.

EDT-NOM-9-D : Authentification d'accès

Les connexions de postes nomades au réseau du ministère *via* l'accès VPN doivent être soumises à une authentification forte.

L'authentification forte consiste en un mode d'authentification d'une entité qui requiert au minimum deux éléments d'authentification permettant de prouver l'identité de l'entité. Il s'agit d'éléments de deux types distincts parmi les éléments :

- Qu'elle connaît (mot de passe, etc.) ;
- Qu'elle possède (certificat logiciel, carte à puce, etc.) ;
- Qui prouve son identité (éléments biométriques, etc.).

Les postes de travail sont soumis à un contrôle de conformité. Si la date de dernière mise à jour du système d'exploitation ou de la base de signatures antivirales est trop ancienne, le poste ne doit pas être autorisé à se connecter au réseau local via l'accès VPN avant d'être mis à jour.

4.6 - Sécurisation des imprimantes et scanners / fax

EDT-IMP-1-D : Impression des informations sensibles

Les impressions d'informations sensibles doivent être effectuées selon une procédure prédéfinie, garantissant le contrôle de l'utilisateur, du déclenchement de l'impression jusqu'à la récupération du support imprimé.

EDT-IMP-2-D : Sécurisation des imprimantes et copieurs multifonctions

Les imprimantes et copieurs multifonctions sont des ressources informatiques à part entière qui doivent être gérées en tant que telles.

Elles ne doivent pas pouvoir communiquer avec l'extérieur.

Elles doivent faire l'objet d'un durcissement en termes de sécurité :

- Changement des mots de passe initialement fixés par le « constructeur » ;
- Désactivation des interfaces réseau inutiles ;
- Suppression des services inutiles ;
- Chiffrement des données sur le disque dur lorsque cette fonctionnalité est disponible ;
- Configuration réseau statique.

EDT-IMP-3-D : Sécurisation de la fonction de numérisation

La fonction de numérisation sur les copieurs multifonctions doit être sécurisée. Les mesures de sécurité suivantes doivent notamment être appliquées :

- Envoi de documents à destination d'une adresse de messagerie interne à l'entité uniquement ;
- Envoi à une unique adresse de messagerie.

EDT-IMP-4-D : Sécurisation de la fonction fax des équipements multifonctions

Le principe de séparation des réseaux doit être appliqué pour les équipements multifonctions. La fonction fax sur ces copieurs doit être sécurisée. En particulier, deux protocoles sont autorisés :

- Par réseau télécom analogique ou
- Par Ethernet sécurisé.

Ces deux protocoles ne peuvent coexister.

Annexes techniques

Sauvegarde/synchronisation des données locales

Des moyens de sauvegarde ou de synchronisation peuvent notamment inclure :

- La mise à disposition d'espaces individuels sur les serveurs de fichiers et un plan de classement explicite à tous les utilisateurs ;
- Des scripts automatiques de copie de dossiers locaux ;
- Des outils de synchronisation automatique (gérés par l'équipe support chargée des systèmes d'Information) ;
- Etc.

La solution de synchronisation automatique doit être autant que possible transparente pour l'utilisateur (par exemple, synchronisation quotidienne d'un répertoire à heure fixe). La solution mise à disposition de l'utilisateur doit lui être communiquée.

Protection des prises en main à distance

Les outils de prise en main à distance doivent respecter les règles suivantes :

- L'authentification doit au minimum être protégée par un mot de passe respectant les règles applicable ;
- Les flux d'authentification lors de la prise en main à distance doivent être sécurisés (aucun mot de passe en clair, séquence non rejouable...) ;
- La prise en main à distance ne doit pas être techniquement réalisable à l'insu de l'utilisateur (l'utilisateur doit explicitement accepter la prise en main) ;
- Les utilisateurs ne doivent pas pouvoir modifier le paramétrage de sécurité de l'outil, ou visualiser les mots de passe ou secrets utilisés ;
- Les secrets utilisés pour établir la connexion ne doivent pas pouvoir être récupérés à partir d'un poste de travail⁵.

Par ailleurs :

- Dans la mesure du possible, l'ensemble des échanges doivent être chiffrés ;
- Dans la mesure du possible, l'outil doit signaler la fin de la prise en main à l'utilisateur ou verrouiller sa session si l'utilisateur n'est pas présent devant son poste à ce moment.

Coffre-fort de mots de passe / de secrets

Ces coffres-forts doivent inclure :

- Un contrôle d'accès constitué au minimum par un mot de passe maître respectant la politique de mot de passe et les règles de gestion explicités dans ce chapitre ;

⁵ Notamment, le risque principal est qu'un même mot de passe soit utilisé sur tous les postes, et qu'un tiers récupère ce mot de passe après le vol d'un ordinateur par exemple.

- Le stockage sécurisé des mots de passe garantissant que les mots de passe protégés ne peuvent être récupérés sans connaissance du secret (chiffrement, masquage...) ;
- L'affichage sécurisé des mots de passe (masquage des mots de passe dans les boîtes de connexion, etc.) ;
- Une résistance aux attaques (déchiffrement, force brute, etc.) ;
- Une fermeture ou un blocage automatique (après une certaine durée, lors de la mise en veille sécurisée, etc.).

Durcissement des configurations

Le durcissement des configurations doit notamment concerner les points suivants :

- Démarrage uniquement sur le disque local ou la mémoire locale ;
- Protection de la configuration système bas niveau (exemple : BIOS) par mot de passe ;
- Renommage des comptes locaux disposant de privilèges élevés nécessaires pour la gestion du poste (exemple : administrateur local) ;
- Désactivation ou suppression des comptes inutiles ;
- Changement des mots de passe / codes secrets par défaut ;
- Désactivation ou suppression des services inutiles ;
- Limitation des droits d'écriture de l'utilisateur sur les zones système et applicatives ;
- Verrouillage de l'accès au poste de travail par un écran de veille protégé par mot de passe se déclenchant au bout d'un délai d'inactivité maximum.

Un script automatique de démarrage permet de corriger les interventions de l'utilisateur sur la dernière règle (modification de la minuterie, suppression de la veille, etc.).

Installation d'un antivirus

L'antivirus doit assurer une analyse en temps réel :

- Des fichiers lus ou écrits, y compris depuis ou vers des disques amovibles ou des partages réseau ;
- Des media externes (CD-ROM, DVD-ROM, clés USB, etc.) connectés sur le poste ;
- Des pages Web visitées (Internet ou Intranet) et des composants associés, ainsi que des téléchargements effectués depuis le Web ;
- Des courriels reçus et envoyés depuis le poste ;
- Des programmes en mémoire vive du poste ;
- Il doit également permettre une analyse d'un disque, lecteur, media, répertoire ou fichier à la demande de l'utilisateur.

Mise à disposition d'une solution VPN

Cette solution VPN doit assurer :

- Une authentification et un chiffrement des communications conformes avec les règles en vigueur de raccordement distant ;
- La non-possibilité de raccordement simultané à Internet et au Système d'Information à travers le tunnel VPN (absence de « split tunneling ») ;
- La protection des moyens d'authentification sur le poste de travail (notamment l'absence de stockage ou de mise en cache des mots de passe et la protection par mot de passe complexe des certificats logiciels ou matériels) ;
- Il doit en outre s'agir d'un système français.

