


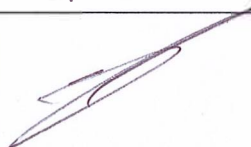




CHARTE DU BON USAGE DES MOYENS INFORMATIQUES DE L'ONERA

	Rédacteur	Vérificateur(s)		Approbateur
Fonction	OCSSI	DSI	OCS	Président de l'ONERA
Nom	Laurent GALLIANO	Pierre MALECKI	Denis Strasser	Bruno SAINJON
Date	04/02/2019	15/02/2019	29.03.19	28.07
Signature				

04/02/2019

Propriété de l'ONERA - Reproduction, communication, utilisation
même partielles interdites sans accord écrit préalable



SOMMAIRE

1	OBJET	3
2	DOMAINE D'APPLICATION.....	3
3	DEFINITIONS	3
4	RESPONSABILITES GENERALES	4
4.1	MISE EN ŒUVRE DES SYSTEMES D'INFORMATION	4
4.2	LA SECURITE DES SYSTEMES D'INFORMATION	4
5	REGLES D'UTILISATION	5
5.1	CONDITIONS GENERALES D'UTILISATION	5
5.1.1	Finalité d'utilisation des moyens informatiques de l'ONERA	5
5.1.2	Respect de l'intégrité des moyens	5
5.1.3	Conditions d'accès aux réseaux de l'ONERA	6
5.2	REGLES DE CONFIDENTIALITE	6
5.2.1	Comptes d'accès individuels et dispositifs associés	6
5.2.2	Données professionnelles	6
5.2.3	Données privées	7
5.2.4	Données syndicales	7
5.3	CONDITIONS PARTICULIERES D'UTILISATION	7
5.3.1	Messagerie et services Internet (réseaux sociaux, blog, forum, ...)	7
5.3.2	Imprimantes multifonctions	8
5.3.3	Supports de stockage amovibles	8
5.3.4	Postes de travail nomades	8
5.3.5	Respect de la propriété intellectuelle et usage licite de logiciels	8
5.4	RESPONSABILITES DE L'ADMINISTRATEUR	8
5.4.1	Devoir d'assistance technique	9
5.4.2	Devoir d'intervention	9
5.4.3	Devoir de gestion des moyens de supervision	9
5.4.4	Devoir de confidentialité	9
5.4.5	L'administrateur local	9
6	MESURES ET SANCTIONS APPLICABLES	10
6.1	SUPERVISION DES MOYENS INFORMATIQUES	10
6.2	AUDIT ET SENSIBILISATION	10
6.3	MESURES PRISES EN CAS D'INCIDENT DE SECURITE OU DE NON-RESPECT DE LA CHARTE	10
6.4	SANCTIONS	11
7	ENTREE EN VIGUEUR	11

1 OBJET

Ce document est un ensemble de règles à respecter dans le cadre du règlement intérieur. Il a pour objet de préciser les droits et devoirs des utilisateurs et des administrateurs des moyens informatiques de l'ONERA, en accord avec la législation, afin d'en promouvoir un usage loyal et responsable. Il présente par ailleurs les dispositifs de journalisation et de filtrage permettant la supervision de ces moyens.

En fonction des questions des utilisateurs, de l'actualité et de l'évolution des technologies, il s'accompagne d'un support dynamique type « FAQ » disponible sur le site DSID¹.

2 DOMAINE D'APPLICATION

Le document s'applique à l'ensemble du personnel de l'ONERA, tous statuts confondus, permanents ou temporaires, utilisant les moyens informatiques de l'ONERA ainsi que ceux auxquels il est possible d'accéder à distance par l'intermédiaire des réseaux administrés par l'ONERA, quelles que soient les technologies de connexion utilisées.

Il sera également appliqué et annexé, aux contrats conclus avec les sociétés extérieures dont les employés auront accès aux systèmes d'information de l'ONERA. Dans le cas de ces sociétés, l'usage des moyens informatiques, par leurs propres salariés, est absolument limité aux impératifs liés à l'exécution du contrat.

3 DEFINITIONS

La définition des termes « moyen ou équipement informatique », « périphérique informatique », « support informatique », « système d'information », « réseau informatique », « services Internet », « journalisation » et « filtrage », susceptible d'évoluer et d'être complétée, est disponible sur le site de DSID².

Un moyen, équipement, périphérique, réseau ou système d'information dit « tiers » est externe et non géré par l'ONERA. Il s'agit de moyens personnels ou provenant d'une entité partenaire.

On désigne sous le terme « utilisateur » toute personne qui est autorisée à accéder à un ou plusieurs moyens informatiques de l'ONERA.

On désigne sous le terme « entité » ou « DDS » les entités administratives créées par l'ONERA pour l'accomplissement de ses missions, telles que les départements de recherche ainsi que les services et directions administratives.

On désigne sous le terme « administrateur » d'un équipement, une personne ayant les droits et assumant la fonction de mise à jour des logiciels, du système d'exploitation et des autorisations d'accès des utilisateurs de cet équipement. Chaque équipement a donc au moins un administrateur. Il en est de même des réseaux informatiques de l'ONERA.

On désigne sous le terme « sécurité des systèmes d'information » les procédures organisationnelles et dispositifs techniques permettant d'assurer la disponibilité, l'intégrité et la confidentialité des systèmes d'information.

Une donnée dite « classifiée » est couverte par la protection du secret de défense et fait l'objet d'une mention « confidentiel défense », « secret défense » ou équivalence étrangère. Elle est régie par des règles particulières venant compléter la présente charte.

Une donnée dite « sensible » n'est pas classifiée mais reste associée à une mention de protection du type « Diffusion Restreinte », « Confidentiel ONERA » ou « Confidentiel personnel ».

¹ <http://iris.onera/SSI/> rubrique « Charte informatique/FAQ »

² <http://iris.onera/SSI/> rubrique « Charte informatique/Définition »

Une donnée « privée » ou « personnelle » est explicitement identifiée comme telle (exemple : message dont le titre est précédé de la mention « privé » ou « personnelle », répertoire ou fichier contenant le mot « privé » ou « personnelle ») ou si elle concerne de manière évidente un sujet d'ordre privé (exemple : dossier médical, entretien individuel, RIB, ...).

Une donnée « à caractère personnel », au sens de la loi, est une notion différente. Elle identifie une personne physique par un ou plusieurs éléments qui lui sont propres (exemple : n° de sécurité sociale, photo, nom et prénom...) et doit être traitée conformément à la loi Informatique et Libertés du 6 janvier 1978 modifiée le 6 août 2004 et au règlement européen sur la protection des données (RGPD) en vigueur depuis le 25 mai 2018.

4 RESPONSABILITES GENERALES

4.1 MISE EN ŒUVRE DES SYSTEMES D'INFORMATION

La Direction des Systèmes d'Information (DSI)³ est responsable de la mise en œuvre des systèmes d'information de l'ONERA ou devra y être associée étroitement en cas de délégation locale d'administration (voir paragraphe 5.4.5). Elle est à la disposition des utilisateurs pour leur fournir toute information concernant l'utilisation des systèmes d'information. Elle les informe régulièrement sur l'évolution des limites techniques des systèmes d'information et sur les menaces susceptibles de peser sur leur sécurité.

Pour lui permettre d'accomplir ces tâches, tout moyen informatique doit être enregistré dans la base de parc informatique de l'ONERA gérée par la DSI.

Les moyens informatiques le permettant doivent être équipés d'un compte d'administration réservé à la DSI. A cet effet, la DSI réalise l'installation initiale de tout poste de travail ou serveur dans l'ensemble des centres ONERA.

Les directeurs de DDS nomment les responsables informatiques locaux (RID), chargés de diffuser l'information de la DSI vers les utilisateurs, de synthétiser les besoins et de piloter les investissements spécifiques de leur entité.

4.2 LA SECURITE DES SYSTEMES D'INFORMATION

La sécurité des systèmes d'information de l'ONERA est une des missions de la Direction Sécurité, Industrielle et de Défense (DSID).

En son sein, l'officier central de la sécurité des systèmes d'information (OCSSI) est chargé de définir la politique de sécurité des systèmes d'information de l'ONERA (PSSI-O), de vérifier sa mise en œuvre au niveau de l'ONERA, de piloter la diffusion des bonnes pratiques et de s'assurer leur respect.

Sur chaque centre, un officier SSI (OSSI) est chargé de contrôler l'exécution des mesures de sécurité des systèmes d'information prises dans son établissement.

Le correspondant local SSI (CSSI) est chargé du contrôle de l'exécution des mesures de sécurité des systèmes d'information prises dans son DDS et de la diffusion des bonnes pratiques de cette charte.

³ <http://iris.onera/DSI/accueilDSI> rubrique « Organisation »

5 REGLES D'UTILISATION

Dans le cadre de leur activité professionnelle, l'ONERA met à la disposition des utilisateurs un poste de travail et un compte individuel. Sous certaines conditions, les utilisateurs peuvent disposer de comptes sur des serveurs centraux ainsi que de supports de stockage amovibles.

5.1 CONDITIONS GENERALES D'UTILISATION

5.1.1 Finalité d'utilisation des moyens informatiques de l'ONERA

L'utilisation des moyens informatiques est destinée à un usage strictement professionnel au bénéfice de l'ONERA, à savoir :

- les activités de recherches, d'enseignements⁴, de développements techniques, de réalisation et d'exploitation d'essais en soufflerie, de transferts de technologies, de diffusion d'informations scientifiques et techniques, d'expérimentations de nouveaux services présentant un caractère d'innovation technique,
- toute activité administrative et de gestion découlant ou accompagnant ces activités.

Un usage non professionnel est toléré dans les conditions suivantes :

- Il concerne des actes administratifs ponctuels ou besoins urgents de la vie courante,
- il n'impacte pas l'activité professionnelle,
- il ne porte pas préjudice à la sécurité des moyens informatiques,
- il ne tombe pas sous le coup de la loi ni ne porte atteinte à l'image de l'ONERA.

L'utilisateur ne doit se connecter ou essayer de se connecter aux moyens informatiques autrement que par les dispositions prévues. Est en particulier interdite toute manœuvre qui viserait à accéder aux moyens sous une fausse identité ou en masquant l'identité véritable de l'utilisateur. En fonction de son expertise, chaque utilisateur doit signaler toute anomalie constatée et susceptible de mettre en péril la sécurité des moyens informatiques à sa disposition⁵.

5.1.2 Respect de l'intégrité des moyens

Pour son travail quotidien l'utilisateur se voit confier des moyens informatiques. Ceci implique des responsabilités en termes de respect de l'intégrité physique et de suivi (par exemple en cas de prêt à un collègue). Il doit en particulier en prendre soin, signaler toute détérioration, perte, vol, voire disparition momentanée et les restituer en cas de départ de l'ONERA ou sur demande.

L'utilisateur ne doit pas connecter lui-même un périphérique tiers sur un équipement de l'ONERA. Si elle est prévue, une procédure de vérification dérogatoire doit être exécutée par l'administrateur de l'équipement qui prend alors la responsabilité de cette connexion⁶. À défaut, toute connexion est interdite.

Inversement, un utilisateur amené à utiliser un périphérique ONERA sur un équipement tiers, doit vérifier que la politique de sécurité de cet équipement l'autorise et s'assurer, avec l'aide d'un administrateur ou du CSSI, de l'intégrité du périphérique après l'opération.

Par ailleurs, l'utilisateur doit solliciter la validation du RID de son DDS et de la DSI en cas de projet de modification d'attribution ou de déménagement de moyen informatique. Cette opération a pour but le maintien à jour de la gestion de parc et la réalisation des actions techniques de conformité nécessaires.

⁴ Les activités d'enseignement faites au titre d'une dispense horaire sont considérées comme faisant partie d'un usage « professionnel »

⁵ Les points de contacts sont : assistance@onera.fr, RID ou CSSI.

⁶ Procédure de vérification mise à disposition par l'OCSSI et dont l'OSSI ou le CSSI est dépositaire. Exemple : Scan de clé USB.

L'utilisateur ne doit pas apporter de perturbations au bon fonctionnement des moyens par une action volontaire ou par imprudence caractérisée. Cette règle concerne la manipulation anormale des moyens informatiques ou l'introduction de logiciels non autorisés. En cas de doute, il peut se rapprocher de la DSI, de l'OSSI ou du CSSI.

Dans la même logique, toute tentative de contournement des dispositifs de journalisation et de filtrage décrits au paragraphe 6.1 est interdite.

5.1.3 Conditions d'accès aux réseaux de l'ONERA

Par défaut, les réseaux informatiques de l'ONERA sont administrés par la DSI. La connexion d'un équipement ONERA aux réseaux est conditionnée par son enregistrement dans la base de parc informatique de l'ONERA.

La réutilisation, sans en référer à la DSI, d'une adresse de connexion pour un équipement autre que celui initialement déclaré est interdite.

La connexion d'un équipement tiers aux réseaux de l'ONERA, ou d'un moyen permettant cette connexion via un équipement de l'ONERA, est interdite. Une dérogation exceptionnelle peut être accordée par l'OCSSI⁷.

Inversement, la connexion d'un équipement ONERA pour accéder à un réseau tiers est également soumise à l'autorisation de l'OCSSI. Toutefois, cette connexion est autorisée dans le cadre de l'utilisation du VPN afin d'accéder à distance au réseau de l'ONERA.

Ces autorisations de connexion sont strictement individuelles et ne peuvent en aucun cas être cédées, même temporairement. Ces autorisations peuvent être retirées à tout moment. Toute autorisation prend fin lors de la cessation même provisoire de l'activité professionnelle qui l'a justifiée.

La constitution d'un sous-réseau local sans fil relié au réseau de l'ONERA est interdite.

5.2 REGLES DE CONFIDENTIALITE

5.2.1 Comptes d'accès individuels et dispositifs associés

Les utilisateurs doivent :

- veiller à la confidentialité des codes, mots de passe, cartes magnétiques, clés ou tout autre dispositif de contrôle d'accès qui leur sont confiés à titre strictement individuel,
- changer régulièrement codes d'accès et mots de passe⁸,
- fermer leur session après la fin de leur période de travail (il est recommandé d'éteindre le poste de travail dès que cela est compatible avec l'activité de l'utilisateur),
- verrouiller leur session de travail lorsqu'ils s'absentent momentanément,
- informer immédiatement l'administrateur de toute tentative d'accès frauduleux ou de tout dysfonctionnement suspect,
- s'assurer que les fichiers confidentiels ne soient pas accessibles, par exemple en les déposant sur des répertoires protégés par des droits d'accès individuels,

5.2.2 Données professionnelles

Les utilisateurs sont responsables de la confidentialité des données dont ils ont la charge à titre professionnel.

Les utilisateurs ne doivent pas stocker de données professionnelles ONERA sur tout moyen informatique ou périphérique où leur sécurité n'est pas assurée par l'ONERA.

⁷ C'est notamment le cas du Wifi « invité » de l'ONERA, précisément dédié à ce type de connexion.

⁸ Des consignes de complexité de mots de passe sont proposées sur le site de DSI.

S'ils souhaitent partager des informations confidentielles avec d'autres utilisateurs, ils ne doivent pas le faire sur leur poste de travail mais sur des serveurs où les droits d'accès spécifiques sont gérés par le système d'exploitation du serveur. Ils doivent au préalable s'assurer du droit d'en connaître des utilisateurs concernés à accéder aux informations déposées. Il leur appartient également de préserver la disponibilité et l'intégrité des données en utilisant les différents moyens de sauvegarde individuels existants ou mis à leur disposition sur des serveurs.

L'utilisateur ne doit pas tenter de lire, copier, modifier, ou détruire les données d'autres utilisateurs, sauf si ces données sont explicitement mises à disposition dans des espaces partagés prévus à cet effet.

Lorsqu'un utilisateur quitte l'ONERA, ou fait l'objet d'une mutation, ses données individuelles professionnelles peuvent être transmises, sur demande du directeur de département ou du chef de service, à un autre utilisateur. Ce transfert ne nécessite pas l'accord préalable de l'utilisateur concerné. Ceci s'applique notamment aux courriers électroniques reçus et envoyés.

Lorsqu'un utilisateur est absent pour une durée prolongée et en cas de nécessité liée à la poursuite de l'activité, le directeur de DDS peut obtenir, après validation de la DRH, et sous sa propre responsabilité, l'accès aux données individuelles professionnelles de l'utilisateur. Cette demande doit être formalisée afin que le salarié en soit informé.

5.2.3 Données privées

Dans la mesure où une donnée est identifiée par l'utilisateur comme « privée »⁹, seule la DRH peut y avoir accès, après accord de l'OCSSI, dans l'un des cas suivants :

- Utilisation des moyens informatiques contraire à la charte : Le constat a lieu en présence, de l'utilisateur, voire en son absence, mais s'il a été dûment sollicité par écrit,
- ou en cas de danger avéré sur des personnes ou les systèmes d'information.

L'utilisateur ne peut s'opposer à un tel accès si l'une de ces conditions est respectée.

Toutes les données, notamment celles échangées par messagerie électronique, qui ne sont pas identifiées comme privées sont réputées professionnelles.

5.2.4 Données syndicales

Si l'utilisateur exerce une activité syndicale ou de représentation du personnel au sein de l'ONERA, il peut utiliser les moyens informatiques de l'ONERA à cet effet, conformément à l'accord sur le droit syndical¹⁰, notamment la messagerie électronique.

Si une donnée est identifiée comme concernant une activité prévue par l'accord sur le droit syndical, la DRH peut y avoir accès, sur demande motivée, en cas d'infraction à la charte ou de danger avéré sur des personnes ou les systèmes d'information. L'utilisateur ou un délégué syndical doit impérativement être présent.

5.3 CONDITIONS PARTICULIERES D'UTILISATION

5.3.1 Messagerie et services Internet (réseaux sociaux, blog, forum, ...)

Dans et hors du cadre professionnel, tout personnel ONERA ou de société liée par contrat de prestation de service, doit faire usage des services Internet dans le respect des règles suivantes :

- ne pas utiliser ces services pour proposer ou rendre accessibles aux tiers des données et informations confidentielles de l'ONERA,
- ne pas émettre d'opinions personnelles susceptibles de porter préjudice à l'image de l'ONERA,

Dans le cadre professionnel il doit :

⁹ Voir définition.

¹⁰ <http://iris.onera/DRH/accord-de-droit-syndical>

- faire preuve de vigilance vis-à-vis de la réception de pièces attachées à des courriers ou des liens Internet. En cas de doute, en particulier sur l'émetteur, il ne doit ni ouvrir les pièces jointes, ni suivre les liens internet proposés dans les messages, ni transférer de tels messages.
- faire preuve de la plus grande correction à l'égard de ses interlocuteurs,
- fermer le ou les navigateurs internet s'il n'en a plus l'usage.

La transmission de données classifiées par la messagerie et sur les services Internet est interdite et celle de données DR doit être effectuée par un moyen de chiffrement agréé.

5.3.2 Imprimantes multifonctions

Les imprimantes et copieurs numériques multifonctions permettent de numériser des documents papier et de les envoyer par messagerie.

La numérisation des documents classifiés est strictement interdite. La numérisation des documents sensibles est autorisée si elle n'est pas transmise par messagerie.

L'utilisateur doit limiter autant que faire se peut, l'impression des documents sensibles et privilégier les modes « programmés », « différés », voire « privés » protégés par mot de passe, des imprimantes qui le permettent.

5.3.3 Supports de stockage amovibles

Des supports de stockages individuels peuvent être mis à disposition de l'utilisateur pour les cas où le stockage sur serveur n'est pas possible (systèmes isolés ou nomades).

Les supports de stockage contenant des informations classifiées ou sensibles, doivent faire l'objet d'une mention de protection explicite et correspondant au niveau de protection des informations.

5.3.4 Postes de travail nomades

Seuls sont concernés par ce paragraphe les ordinateurs dit « portables » attribués par l'ONERA à ses collaborateurs dans le cadre de leurs missions à l'extérieur de l'ONERA.

L'usage des postes nomades en dehors de la protection physique d'un établissement ONERA les rend particulièrement vulnérables et les précautions suivantes sont à prendre :

- Effectuer des mises à jour des logiciels impactant la sécurité des systèmes d'information, en se connectant à fréquence raisonnable au réseau de l'ONERA,
- Effectuer des sauvegardes fréquentes en se connectant au réseau de l'ONERA ou sur un support de stockage externe chiffré,
- Respecter les consignes en vigueur de chiffrement des disques ou des fichiers disponibles sur le site de DSID,
- Ne pas inscrire en clair de mots de passe sur le poste lui-même ou à proximité¹¹,
- Ne pas consulter de document sensible dans un lieu public.

5.3.5 Respect de la propriété intellectuelle et usage licite de logiciels

L'utilisateur ne doit pas reproduire, télécharger, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits et de l'ONERA.

5.4 RESPONSABILITES DE L'ADMINISTRATEUR

L'administrateur est un utilisateur à part entière, tenu de respecter le contenu de la présente charte. Il possède des droits étendus lui conférant des devoirs et des responsabilités particulières.

¹¹ Des méthodes et des outils de mémorisation sont proposés sur le site de DSID.

Il est explicitement désigné pour ce rôle et agit sous la responsabilité de la DSI. Son rôle principal est d'assurer au quotidien la continuité de service et la sécurité des systèmes d'information de l'ONERA. Pour ce faire, il possède un compte à privilège destiné aux tâches d'administration uniquement et un compte sans privilège pour toutes autres activités, notamment pour accéder à des services Internet.

5.4.1 Devoir d'assistance technique

L'administrateur assure des tâches d'assistance technique et de maintenance en appliquant les consignes suivantes :

- mettre à jour régulièrement les logiciels impactant la sécurité du système d'information,
- se tenir informé des failles pouvant affecter les moyens informatiques dont il a la responsabilité,
- inciter les utilisateurs au respect des consignes figurant dans la présente charte,

5.4.2 Devoir d'intervention

Il appartient à l'administrateur de signaler à sa hiérarchie toute anomalie constatée et susceptible de mettre en péril la sécurité des moyens d'information ou d'enfreindre la présente charte.

En cas d'incident de sécurité avéré ou de non-respect manifeste de la charte, l'administrateur est chargé d'exécuter les mesures d'urgence ou préventives décrites en 6.2.

5.4.3 Devoir de gestion des moyens de supervision

L'administrateur en charge des moyens de supervision, assure la gestion opérationnelle de la supervision prévue au paragraphe 6.1 :

- La configuration des équipements et des logiciels de sécurité afin que la journalisation d'événements soit activée,
- l'analyse des journaux d'événements,
- la sauvegarde et la conservation des journaux,
- la restitution sur demande par la DSI des journaux d'événements concernant un équipement ou un utilisateur particulier.

5.4.4 Devoir de confidentialité

L'administrateur doit assurer la confidentialité de toute information à laquelle il pourrait avoir accès, ce qui implique notamment :

- de veiller à ce que les tiers non autorisés n'aient pas connaissance de données sensibles,
- de ne pas divulguer de mot de passe administrateur,
- de ne pas divulguer de mots de passe utilisateur dont il aurait pu avoir connaissance lors d'une intervention d'assistance,
- de ne pas diffuser ni de données à caractère personnel¹², ni de données privées.

Toute prise en main à distance sur un poste est soumise à des règles de confidentialité strictes consultables sur le site de la DSI. L'ensemble des prestataires de la DSI, travaillant dans le cadre et les conditions de marchés sensibles, applique les mêmes règles sous le contrôle de DSI.

5.4.5 L'administrateur local

La responsabilité d'administration peut être déléguée à de rares exceptions à certains utilisateurs et sous les conditions suivantes :

- l'administrateur est sensibilisé et formé, pour exercer ses fonctions,
- l'administrateur local s'engage à respecter les devoirs spécifiques des administrateurs,

¹² En dehors du cadre défini par la nature du traitement déclaré dans le registre du CIL.

- **il existe un besoin opérationnel spécifique et justifié ne pouvant être assuré par un administrateur DSI,**
- l'administrateur local a obtenu la validation de sa hiérarchie et de l'OCSSI, puis l'accord technique de la DSI¹³,
- dans le cas d'un poste nomade, il est interdit de l'utiliser avec des droits d'administration en dehors de l'ONERA. Le compte utilisateur sans privilège doit être utilisé à cet effet.

Outre un accès aux moyens d'administration, la DSI dispose d'un moyen de surveillance du maintien en condition de sécurité du système concerné.

6 MESURES ET SANCTIONS APPLICABLES

6.1 SUPERVISION DES MOYENS INFORMATIQUES

DSI et DSID collaborent à la supervision des moyens informatiques et des services internet. La finalité est d'assurer la continuité de service et la sécurité des systèmes d'information de l'ONERA, tout en permettant de veiller à l'application de la présente charte.

Dans ce cadre, des dispositifs automatisés de journalisation des accès à Internet et des événements de sécurité (détection de virus, saturation des espaces disques ou des réseaux, tentatives répétées d'accès à des moyens protégés ou à sites Internet interdits,...) sont mis en œuvre en conformité avec la loi « informatique et libertés ». Les journaux peuvent être conservés pour une durée de 1 an maximum.

A tout moment, les systèmes d'information, en particulier certains espaces privatifs comme les répertoires de fichiers « utilisateurs » sur les services de fichiers ou les comptes de messagerie peuvent également faire l'objet de vérifications automatiques consistant en la vérification de conformité des configurations et la détection d'information sensible ne devant pas transiter¹⁴. En cas d'atteinte à la sécurité des systèmes d'information de l'ONERA ou de non-respect des dispositions de la charte, ces contrôles automatiques peuvent amener à l'analyse individuelle de l'activité (volume de données échangées, sites internet consultés, logiciels installés, contenu des messages électroniques, ...) après en avoir averti l'utilisateur concerné. Un accès physique ou à distance sur un poste utilisateur pourra également être effectué.

6.2 AUDIT ET SENSIBILISATION

Dans le cadre de la diffusion des bonnes pratiques, DSID organise des actions de sensibilisation SSI du personnel. La présence des utilisateurs aux séances d'information est fortement encouragée, obligatoire pour les personnels habilités. Dans certains cas, il peut être fait appel à des intervenants externes avec lesquels une partie des coordonnées professionnelles est partagée dans le respect des lois en vigueur.

Pour ce qui concerne le suivi de la mise en œuvre de la PSSI-O, DSID pilote des audits de conformité¹⁵ sur l'ensemble des SI de l'ONERA. Les modalités d'intervention sont définies en coordination avec les utilisateurs concernés et en minimisant les impacts sur la production.

6.3 MESURES PRISES EN CAS D'INCIDENT DE SECURITE OU DE NON-RESPECT DE LA CHARTE

Suite à la détection d'une anomalie, des mesures d'urgence ou préventives peuvent être prises pouvant impacter les utilisateurs. La DSI et DSID se coordonnent pour décider des mesures à mettre en œuvre en impliquant, selon les cas, la hiérarchie des utilisateurs et la DRH.

En cas de non-respect manifeste de la charte par un utilisateur, celui-ci sera préalablement informé et sensibilisé. Si son comportement persiste et sans préjuger d'éventuelles sanctions, les mesures préventives suivantes seront susceptibles d'être prises à son encontre :

¹³ Formulaire d'accord disponible sur le site de DSID.

¹⁴ Le site DSID référence les mentions de protection interdites et les mots-clefs susceptibles d'être recherchés par les outils de vérification de la conformité de l'usage de la messagerie électronique (voir lien <http://iris.onera/SSI/?q=rglmtintssi>).

- limitation provisoire des accès,
- retrait provisoire des codes d'accès et suspension des comptes,

En cas d'incident avéré mettant en péril la sécurité des moyens informatiques, les procédures d'urgence suivantes sont susceptibles d'être prises, avec ou sans préavis, selon la gravité de la situation et dans la mesure où cela n'entraîne pas de dégâts matériels importants :

- déconnexion d'équipements informatiques ou partie de réseau,
- isolement provisoire ou neutralisation de données ou fichiers pouvant présenter un danger.

6.4 SANCTIONS

Indépendamment des poursuites civiles ou pénales qui pourraient être engagées par l'ONERA ou des tiers suite à un non-respect de la législation en vigueur, tout manquement intentionnel ou par négligence répétée aux règles de la présente charte sera susceptible d'entraîner une des sanctions prévues dans le règlement intérieur de l'ONERA.

7 ENTREE EN VIGUEUR

La présente charte est applicable à compter du 1^{er} avril 2019.

Elle est adoptée après consultation des représentants du personnel et information des salariés de l'ONERA.