Charte de la Sécurité des Systèmes d'Information de l'OCA

Cette charte, annexée au règlement intérieur des Entités, a pour objet d'informer les Utilisateurs de leurs droits et de leurs responsabilités à l'occasion de l'usage des ressources informatiques et des services numériques de l'OCA, en application de la politique de sécurité de l'information de l'OCA et de la législation.

La politique de sécurité de l'information en vigueur dans les unités mixtes dépend de l'établissement qui a en charge la politique de sécurité de l'Entité, elle est décidée par accord conventionnel entre les établissements.

Dans une politique d'harmonisation et de simplification, sachant que les unités de l'OCA sont des unités mixtes à tutelles CNRS, la charte proposée par l'OCA est celle du CNRS adaptée à l'établissement.
La présente charte s'applique à l'ensemble des personnels des unités de l'Observatoire de la Côte d'Azur (OCA) quel que soit leur statut, et plus généralement à l'ensemble des personnes, permanentes ou temporaires qui utilisent, à quelque titre que ce soit, les ressources informatiques et services internet de l'OCA, ainsi que ceux auxquels il est possible d'accéder à distance directement ou en cascade à partir du réseau de l'établissement.
La charte est portée à la connaissance des personnes susvisées par tous moyens et notamment : par la signature de l'acceptation de la charte avant ouverture d'un compte, par l'envoi sur la messagerie de l'URL de téléchargement de la charte lorsqu'un compte est ouvert pour un utilisateur, celui-ci acceptant de fait la présente charte en poursuivant l'accès aux ressources informatiques, par voie d'affichage sur le site web de l'établissement ou par voie d'annexe au règlement intérieur de l'OCA et de ses unités.

Elle répond à la préoccupation de l'OCA de protéger les informations qui constituent son patrimoine immatériel contre toute altération, volontaire ou accidentelle, de leur confidentialité, intégrité ou disponibilité. Tout manquement aux règles qui régissent la sécurité des systèmes d'information est en effet susceptible d'avoir des impacts importants (humains, financiers, juridiques, environnementaux, atteinte au fonctionnement de l'organisme ou au potentiel scientifique et technique).

L'Utilisateur contribue à son niveau à la sécurité des systèmes d'Information. À ce titre, il applique les règles de sécurité en vigueur dans l'Entité et signale tout dysfonctionnement ou événement lui apparaissant anormal.

L'Entité met à la disposition de l'Utilisateur les moyens nécessaires à l'application de la politique de sécurité des systèmes d'information.

A son niveau, le personnel d'encadrement favorise l'instauration d'une « culture sécurité » par son exemplarité dans le respect de cette charte et par un soutien actif des équipes en charge de la mise en œuvre de ces règles.

Définitions

On désignera sous le terme « Utilisateur » : la personne ayant accès ou utilisant les ressources informatiques et services Internet quel que soit son statut.

On désignera sous le terme « Entité » : les unités de recherche ou de service propres ou mixtes ainsi que les services et directions administratives.

I. Principes de sécurité

Les règles ci-après s'appliquent à tous les Utilisateurs, et peuvent être complétées par des mesures spécifiques à leur Entité résultant de la PSSI (Politique de Sécurité des Systèmes d'Information) opérationnelle.

Protection des informations et des documents électroniques

Tout Utilisateur est responsable de l'usage des ressources informatiques auxquelles il a accès.
L'Utilisateur protège les informations qu'il est amené à manipuler dans le cadre de ses fonctions, selon leur sensibilité. Lorsqu'il crée un document, l'Utilisateur détermine son niveau de sensibilité et applique les règles permettant de garantir sa protection durant tout son cycle de vie (marquage, stockage, transmission, impression, suppression, etc.).

Lorsque ses données ne font pas l'objet de sauvegardes automatiques mises en place par l'Entité dont il relève, l'Utilisateur met en œuvre le système de sauvegarde manuel préconisé par son Entité.

Afin de se prémunir contre les risques de vol de documents sensibles, l'Utilisateur, lorsqu'il s'absente de son bureau, s'assure que ses documents papier, lorsqu'ils existent, sont rangés sous clé et que son poste de travail est verrouillé.

Protection des moyens et droits d'accès aux informations

L'Utilisateur est responsable de l'utilisation des systèmes d'information réalisée avec ses droits d'accès.

A ce titre, il assure la protection des moyens d'authentification qui lui ont été affectés ou qu'il a généré (badges, mots de passe, clés privées, clés privées liées aux certificats, etc.) :

- Il ne les communique jamais, y compris à son responsable hiérarchique et à l'équipe chargée des SI de son Entité ;
- il applique les règles de « génération/complexité » et de renouvellement en vigueur selon le moyen d'authentification utilisé ;
- Il met en place tous les moyens mis à sa disposition pour éviter la divulgation de ses moyens d'authentification ;
- Il modifie ou demande le renouvellement de ses moyens d'authentification dès lors qu'il en suspecte la divulgation.
- Il garantit l'accès à ses données professionnelles, notamment dans le cadre de la politique de recouvrement[1] de données mise en œuvre au sein de l'Entité.

L'Utilisateur ne fait pas usage des moyens d'authentification ou des droits d'accès d'une tierce personne. De la même façon, il n'essaie pas de masquer sa propre identité.

1 Le recouvrement est le dispositif de secours permettant à une personne habilitée d'accéder à des données lorsque le mécanisme principal n'est plus utilisable (perte de mot de passe par exemple).

L’Utilisateur ne fait usage de ses droits d'accès que pour accéder à des informations ou des services nécessaires à l’exercice des missions qui lui ont été confiées et pour lesquels il est autorisé :

- il s'interdit d'accéder ou de tenter d'accéder à des ressources du système d'information pour lesquelles il n’a pas reçu d’habilitation explicite ;
- il ne connecte pas aux réseaux locaux de l’Entité – quelle que soit la nature de ces réseaux (filaires ou non filaires) - des matériels autres que ceux confiés ou autorisés par la direction ou l’Entité ;
- il n’introduit pas des supports de données (clé USB, CDROM, DVD, etc.) sans respecter les règles de l’Entité et prend les précautions nécessaires pour s’assurer de leur innocuité ;
- il n’installe pas, ne télécharge pas ou n’utilise pas, sur le matériel de l'Entité ou sur du matériel personnel utilisé à des fin professionnelles, des logiciels ou progiciels dont les droits de licence n’ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, ou interdits par l’Entité ;
- il s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations anormales du matériel ou du logiciel.

L’Utilisateur informe les administrateurs de toute évolution de ses fonctions nécessitant une modification de ses droits d’accès.

Protection des équipements informatiques

L’Utilisateur protège les équipements mis à sa disposition :

- il applique les consignes de l’équipe informatique issues de la PSSI opérationnelle de l’Entité afin de s’assurer notamment que la configuration de son équipement suit les bonnes pratiques de sécurité (application des correctifs de sécurité, chiffrement, etc.) ;
- il utilise les moyens de protection disponibles (câble antivol, rangement dans un tiroir ou une armoire fermant à clé, etc.) pour garantir la protection des équipements mobiles et des informations qu’ils renferment (ordinateur portable, clé USB, smartphones, tablettes, etc.) contre le vol ;
- en cas d’absence, même momentanée, il verrouille ou ferme toutes les sessions en cours sur son poste de travail ;
- il signale le plus rapidement possible au chargé de la sécurité des SI (chargé de la SSI au sein de l’Entité ou le cas échéant responsable SSI de l’OCA) toute perte, tout vol ou toute compromission suspectée ou avérée d’un équipement mis à sa disposition.

L’Utilisateur protège les équipements personnels qu’il utilise pour accéder, à distance ou à partir du réseau local d’une Entité, aux SI de l’OCA ou stocker des données professionnelles en respectant les règles édictées par l’OCA et l’Entité.

L’Entité l’informe et l’accompagne dans la mise en œuvre de ses mesures de protection.

Protection vis-à-vis des échanges sur les réseaux

Adresse électronique

L’OCA s'engage à mettre à la disposition de l'Utilisateur une boîte à lettres professionnelle nominative lui permettant d’émettre et de recevoir des messages électroniques. L’utilisation de cette adresse nominative se fait sous la responsabilité de l’Utilisateur.

L’aspect nominatif de l'adresse électronique constitue le simple prolongement de l'adresse administrative : il ne retire en rien le caractère professionnel de la messagerie.

Contenu des échanges sur les réseaux

Les échanges électroniques (courriers, forums de discussion, messagerie instantanée, réseaux sociaux, partages de documents, voix, images, vidéos, etc.) respectent la correction normalement attendue dans tout type d'échange tant écrit qu'oral.

La transmission de données classifiées de défense est interdite sauf dispositif spécifique agréé et la transmission de données sensibles doit être réalisée suivant les règles de protection en vigueur.

Vigilance

L’Utilisateur fait preuve de vigilance vis-à-vis des informations reçues (désinformation, virus informatique, tentative d’escroquerie, chaînes, hameçonnage, ...).

Statut et valeur juridique des informations échangées

Les informations échangées par voie électronique avec des tiers peuvent, au plan juridique, former un contrat sous certaines conditions ou encore être utilisés à des fins probatoires.

L'Utilisateur doit, en conséquence, être prudent sur la nature des informations qu’il échange par voie électronique au même titre que pour les courriers traditionnels.

Stockage et archivage des informations échangées

L’Utilisateur est informé que le courriel est un document administratif reconnu en tant que preuve en cas de contentieux.

Protection vis-à-vis de l’accès aux services en ligne sur Internet

Si une utilisation résiduelle privée peut être tolérée, il est rappelé que les connexions établies grâce à l’outil informatique mis à disposition par l’OCA sont présumées avoir un caractère professionnel.

L’Utilisateur utilise ses coordonnées professionnelles, en particulier son adresse électronique ou autre identifiant, avec précaution. En les utilisant sur des sites sans rapport avec son activité professionnelle il facilite les atteintes à sa réputation, à la réputation de l’Entité ou à celle de l’OCA.

Certains sites malveillants profitent des failles des navigateurs pour récupérer les données présentes sur le poste de travail. D’autres sites mettent à disposition des logiciels qui, sous une apparence anodine, peuvent prendre le contrôle de l’ordinateur et transmettre son contenu au pirate à l’insu de l’Utilisateur. Enfin, certains sites ne fournissent aucune garantie sur l’utilisation ultérieure qui pourra être faite des données transmises. Par conséquent, l’Utilisateur :

- évite de se connecter à des sites suspects ;
- évite de télécharger des logiciels dont l’innocuité n’est pas garantie (nature de l’éditeur, mode de téléchargement, etc.) ;
- n’opère les sauvegardes de données, les partages d’information, les échanges collaboratifs, que sur des sites de confiance, mis à disposition par l’établissement et dont la sécurité a été vérifiée par l’établissement (via par exemple un audit de sécurité) ;
- chiffre les données non publiques qui seraient stockées sur des sites tiers ou transmises via des messageries non sécurisées.

Publication d’informations sur Internet

Toute publication d’information sur les sites internet ou intranet de l’Entité est réalisée sous la responsabilité d’un responsable de site ou responsable de publication nommément désigné.

Aucune publication d’information à caractère privé (pages privées au sens non professionnelles) sur les ressources du système d’information de l’Entité n’est autorisée, sauf disposition particulière décidée au sein de l’Entité.

Le chargé de la SSI de l’Entité ou le responsable SSI de la délégation dont il relève apporte son soutien à l’Utilisateur pour la mise en œuvre de l’ensemble de ces mesures.

II. Vie privée et ressources informatiques personnelles

Vie privée résiduelle

Les ressources informatiques (poste de travail, serveurs, applications, messagerie, Internet, téléphone, etc.) fournies à l’Utilisateur, par l’OCA ou ses partenaires, EPST, université, etc. - sont réservées à l'exercice de son activité professionnelle.

Un usage personnel de ces ressources est toutefois toléré à condition :

- qu’il reste de courte durée pendant les heures de travail au bureau ;
- qu’il n’affecte pas l’usage professionnel ;
- qu'il ne mette pas en danger leur bon fonctionnement et leur sécurité ;
- qu’il n’enfreigne pas la loi, les règlements et les dispositions internes.

Toute donnée est réputée professionnelle à l’exception des données explicitement désignées par l'Utilisateur comme ayant un caractère privé (par exemple en indiquant la mention « privé » dans le champ « objet » des messages).

L’Utilisateur procède au stockage de ses données à caractère privé dans un espace de données prévu explicitement à cet effet ou en mentionnant le caractère privé sur la ressource utilisée. Cet espace ne doit pas contenir de données à caractère professionnel et il ne doit pas occuper une part excessive des ressources. La protection et la sauvegarde régulière des données à caractère privé incombent à l'Utilisateur.

Ressources informatiques personnelles

Les ressources informatiques personnelles (ordinateurs, smartphones, tablettes, etc. achetés sur des crédits personnels), lorsqu’elles sont utilisées pour accéder aux SI de l’OCA, ne doivent pas remettre en cause ou affaiblir, les politiques de sécurité en vigueur dans les Entités par une protection insuffisante ou une utilisation inappropriée.

Lorsque ces ressources informatiques personnelles sont utilisées pour accéder, à distance ou à partir du réseau local d’une Entité, aux SI de l’OCA ou stocker des données professionnelles, ces ressources sont autorisées et sécurisées suivant les directives issues de la PGSI (Politique Générale des Systèmes d’Information) et déclarées au service informatique qui gère le parc matériel de l’Entité. Les personnels qui souhaiteraient faire l’acquisition de tels matériels prennent préalablement conseil auprès de leur service informatique.

Gestion des départs

L'Utilisateur est responsable de son espace de données à caractère privé et il lui appartient de le détruire au moment de son départ. En cas de circonstances exceptionnelles (départ impromptu ou décès) l'OCA ne conserve les espaces de données à caractère privé présents sur les ressources informatiques fournies par l'OCA que pour une période de 3 mois maximum (délai permettant à l'Utilisateur ou ses ayants droits de récupérer les informations qui s'y trouvent).

Les données professionnelles restent à la disposition de l'employeur. Les mesures de conservation des données professionnelles sont définies au sein de l'Entité.

III. Respect du Règlement Général à la Protection des Données (RGPD)

Si, dans l'accomplissement de ses missions, l'Utilisateur constitue des fichiers contenant des données à caractère personnel soumis aux dispositions du RGPD, il en informe le directeur d'unité afin que les déclarations nécessaires puissent être réalisées auprès du Délégué à la Protection des Données (DPD ou DPO) de l'OCA.

IV. Respect de la propriété intellectuelle

L'Utilisateur ne reproduit pas, ne télécharge pas, ne copie pas, ne diffuse pas, ne modifie pas ni n'utilise 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.

V. Impact des droits et devoirs spécifiques aux administrateurs des SI sur les données des utilisateurs

La loi et les règlements[2] imposent à l'OCA de garder un historique des accès réalisés par les agents. L'OCA a donc mis en place une journalisation des accès, conformément aux règles énoncées dans la PGSI et à la déclaration réalisée auprès de la CNIL en application de la loi n°78-17 du 6 janvier 1978 modifiée.

L'administrateur a accès aux traces laissées par l'Utilisateur lors de ses accès sur l'ensemble des ressources informatiques mises à sa disposition par l'Entité ainsi que sur les réseaux locaux et distants.

Ces traces (appelées également « fichiers de journalisation » ou « journaux ») sont sauvegardées 12 mois au maximum.

2 En particulier l'article 6-II de la Loi pour la Confiance Numérique (LCEN) du 21 juin 2004 qui impose aux fournisseurs d'hébergement et aux fournisseurs d'accès internet de conserver les données d'identification pour les connexions à leurs services et l'article L. 34-1 du Code des postes et communications électroniques (CPCE) qui impose une obligation de conservation de ces données.

Les administrateurs peuvent, en cas de dysfonctionnement technique, d'intrusion ou de tentative d'attaque sur les systèmes informatiques utiliser ces traces pour tenter de retrouver l'origine du problème.

Ces personnels sont soumis à une obligation de confidentialité. Ils ne peuvent donc divulguer les informations qu'ils sont amenés à connaître dans le cadre de leur fonction, en particulier lorsqu'elles sont couvertes par le secret des correspondances ou relèvent de la vie privée de l'utilisateur, dès lors que ces informations ne remettent pas en cause ni le bon fonctionnement technique des applications, ni leur sécurité.

Ils peuvent prendre connaissance ou tenter de prendre connaissance du contenu des répertoires, fichiers ou message manifestement et explicitement désignés comme personnels qu'en présence de l'agent et avec son autorisation expresse, en cas d'urgence justifiée ou de nécessité vis-à-vis de la législation et de la sécurité.

VI. Respect de la loi

L'Utilisateur est tenu de respecter l'ensemble du cadre légal lié à l'utilisation des systèmes d'information, ainsi que toute autre réglementation susceptible de s'appliquer.

En particulier, il respecte :
► la loi du 29 juillet 1881 modifiée sur la liberté de la presse. L'Utilisateur ne diffuse pas des informations constituant des atteintes à la personnalité (injure, discrimination, racisme, xénophobie, révisionnisme, diffamation, obscénité, harcèlement ou menace) ou pouvant constituer une incitation à la haine ou la violence, ou une atteinte à l'image d'une autre personne, à ses convictions ou à sa sensibilité ;
►la réglementation relative au traitement des données à caractère personnel (notamment la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés) ;
► la législation relative aux atteintes aux systèmes de traitement automatisé de données (art. L 323-1 et suivants du code pénal) ;
►la loi n° 94-665 du 4 aout 1994 modifiée relative à l'emploi de la langue française ;
►la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ;
►les dispositions du code de la propriété intellectuelle relatives à la propriété littéraire et artistique. L'Utilisateur ne fait pas de copies illicites d'éléments (logiciels, images, textes, musiques, sons, etc.) protégés par les lois sur la propriété intellectuelle ;
►les dispositions relatives au respect de la vie privée, de l'ordre public, du secret professionnel.
►les dispositions relatives à la Protection du Potentiel Scientifique et Technique de la Nation.

Certaines de ces dispositions sont assorties de sanctions pénales.