La charte informatique

Table des matières

1. Champ d'application de la charte

Les règles et obligations ci-dessous énoncées s'appliquent à toute personne ; en particulier enseignants, chercheurs, enseignants-chercheurs, étudiants, personnels administratifs ou techniques ; autorisée à utiliser les moyens et systèmes informatiques de l'Université Catholique de l'Ouest, UCO. Ces derniers comprennent notamment les datacenters, les serveurs, stations de travail et micro-ordinateurs des services administratifs, des salles de cours ou d'informatique, des laboratoires et des Centres de Documentation de l'Université, ainsi que les services contractualisés par l'une ou l'autre des associations de gestion de l'UCO tels que les accès à l'Internet, les applications et services hébergés par des partenaires de l'UCO.

2. Conditions d'accès aux services et réseaux informatiques de l'UCO.

La DSI gère les accès aux services et réseaux informatiques.

L'utilisation des moyens informatiques de l'UCO a pour objet exclusif de mener des activités de recherche, d'enseignement ou d'administration.

Chaque utilisateur se voit attribuer des identifiant et mot de passe, ainsi que des habilitations en fonction de ses besoins (accès internet, accès aux applications, accès à des serveurs, applications hébergées, ressources numériques etc.).

Les identifiant et mot de passe attribués sont strictement personnels et incessibles. Chaque utilisateur est responsable de l'utilisation qui en est faite.

Le mot de passe choisi par l'utilisateur doit respecter des règles de longueur et de complexité : ainsi le mot de passe ne peut correspondre ni à un mot, ni à un nom propre d'aucune langue que ce soit. Il doit comporter des minuscules, majuscules, des chiffres et au moins un caractère spécial (&#$* !<>@) et être long de plus de 12 caractères.

En cas d'essais infructueux répétés, le compte utilisateur est automatiquement bloqué d'une durée suffisante pour ralentir les tentatives d'accès frauduleuses. Le compte se débloque automatiquement.

Afin de renforcer la sécurité du compte utilisateur dans un contexte où les tentatives d'usurpation d'identité et de vol de données sont massives et automatiques, un mécanisme d'authentification à double facteur est mis en place : un n° de téléphone, une adresse électronique personnelle ou une application de sécurité sont utilisés afin de communiquer un code personnel à usage unique lors du renouvellement du mot de passe, et lors de l'authentification sur certains systèmes sensibles. La conservation du n° de téléphone et l'adresse mail personnelle dans l'Annuaire du Nuage Microsoft est conforme au RGPD la politique de confidentialité de Microsoft.

En cas d'impossibilité de se connecter, de soupçon d'usurpation de son compte, ou de toute anomalie détectée, l'utilisateur doit prévenir la DSI de l'UCO (accueil_dsi@uco.fr) et le responsable informatique local qui prendront les mesures adaptées en concertation avec l'utilisateur.

Les habilitations des utilisateurs changent en fonction de l'évolution de leur statut (étudiant, salarié, prestataire), rôles (enseignant, chercheur, personnel administratif et technique, etc.) et appartenances (campus, faculté, service, filière et parcours de formation). Tout changement de statut, de rôle ou d'appartenance doit être notifié à la DSI par l'entité responsable de l'utilisateur.

Les accès sont révoqués à l'issue :

- des études ;
- de la collaboration ;
- de la prestation.

3. Respect des règles de déontologie

Chaque utilisateur s'engage à respecter les règles de déontologie suivantes et notamment à ne pas effectuer intentionnellement des opérations qui pourraient avoir pour conséquences :

- de masquer sa véritable identité ;
- de s'approprier et d'utiliser le compte ou le mot de passe d'un autre utilisateur ;
- d'altérer, de modifier ou détruire des données ou d'accéder à des informations appartenant à d'autres utilisateurs du réseau ou à l'UCO, sans leur autorisation ;
- de porter atteinte à la réputation d'un autre utilisateur ou à sa sensibilité, notamment par l'intermédiaire de messages, textes ou images provocants ou insultants ;
- d'interrompre ou de perturber le fonctionnement normal du réseau ou d'un des systèmes connectés au réseau ;
- de modifier ou de détruire des informations sur un des systèmes ;
- de se connecter ou d'essayer de se connecter sur des sites ou systèmes illégaux.

La réalisation d'un programme informatique ayant de tels objectifs est interdite.

4. Respect du Règlement Général sur la Protection des Données personnelles

Tout utilisateur doit respecter le Règlement Général sur la Protection des Données (RGPD).

Si dans l'accomplissement de son travail ou de ses missions, l'utilisateur est amené à mettre en œuvre un traitement des données personnelles (ex. enquêtes, formulaires, etc.), il doit effectuer une déclaration de traitement de données personnelles, informatisé ou non, auprès du Délégué à la Protection des Données (dpo.uco@uco.fr)

La liste des données personnelles collectées doit être minimale et nécessaire pour le déroulement légitime du traitement. En particulier, le traitement de données sensibles est strictement interdit sans une base légale.

Les données sensibles sont définies comme :

- révélant l'origine prétendument raciale ou ethnique ;
- portant sur les opinions politiques, philosophiques ou religieuses ;
- relatives à l'appartenance syndicale ;
- concernant la santé ou l'orientation sexuelle ;
- génétiques ou biométriques.

L'utilisateur doit informer les personnes concernées par le traitement :

1. de la finalité, ayant une base légale ou légitime, du traitement ;
2. des personnes ou organismes pouvant accéder aux données ;
3. de la durée de conservation des données personnelles ;
4. des modalités selon lesquelles les personnes concernées peuvent exercer leurs droits ;

5. des éventuels sous-traitants.

L'utilisateur dispose d'un droit d'accès, de modification, de suppression de ses données personnelles qu'il peut exercer auprès de chaque responsable de traitements pour peu qu'elles n'entravent pas le bon déroulement des activités pédagogiques et administratives, en particulier la candidature, l'inscription, le suivi des cours, le passage des examens écrits et oraux, les soutenances, le recrutement, la paie et la gestion de la carrière des salariés, et les communications institutionnelles.

La politique de confidentialité de l'UCO présente la manière dont sont traitées les données personnelles.

5. Installation de logiciels et souscription de services

La DSI est garante de la conformité des licences et de la bonne gestion de l'accès aux services et applications en ligne.

L'utilisateur ne devra en aucun cas sans accord préalablede la DSI ou du responsable informatique local :

1. souscrire un abonnement, à titre onéreux ou gratuit, à un service ou une application en ligne avec son adresse de messagerie UCO ;
2. installer des logiciels à caractère ludique ;
3. développer des programmes constituant ou s'apparentant à des logiciels malveillants.

En aucun cas l'utilisateur ne peut faire une copie d'un logiciel commercial ou contourner les restrictions d'utilisation d'un logiciel.

L'utilisateur doit demander à la DSI ou au responsable informatique local s'il peut installer un logiciel.

L'utilisateur doit demander à la DSI (accueil_dsi@uco.fr) ou au responsable informatique local la souscription à un service ou une application en ligne.

6. Utilisation des moyens informatiques

Chaque utilisateur s'engage à prendre soin du matériel, des locaux informatiques et logiciels mis à sa disposition. Il informe la DSI (accueil_dsi@uco.fr) ou le responsable informatique local de toute anomalie constatée.

L'UCO est engagée dans une démarche de Responsabilité Société et Environnementale : Transition écologique, Comité de Pilotage DD & RS, , signataire de la Charte Numérique Responsable.

A ce titre, et parce que le numérique est un acteur majeur d'émissions de gaz à effet de serre, d'épuisement des ressources et d'affaissement de la biodiversité, participant activement au changement climatique, les utilisateurs sont invités à optimiser l'usage des moyens informatiques. Par exemple en éteignant les postes informatiques et les écrans à la fin de leur usage.

Stockage

L'utilisateur doit s'efforcer de n'occuper que la quantité d'espace de stockage qui lui est strictement nécessaire, en particulier il est responsable d'effectuer la suppression périodique des fichiers inutiles.

Les espaces de stockage pédagogiques mis à disposition sont vidés de tous les travaux des étudiants entre le 15 juillet et le 30 août de chaque année. Les enseignants sont sollicités pour arbitrer en cas de doute. Les étudiants et enseignants sont invités à récupérer leurs travaux avant le 15 juillet de chaque année.

Dans Chamilo, les travaux des étudiants sont supprimés au bout de 18 mois. Les cours et documents inutilisés doivent être supprimés par les enseignants. L'usage des sessions est à préférer à la duplication des cours. En cas de duplication des cours, les anciens cours doivent être supprimés.

La mise en ligne de vidéo sur Chamilo doit être exceptionnelle : il est recommandé de charger des vidéos sur la plateforme Vimeo et de les intégrer dans des cours de façon transparente.

Les espaces de stockage dans le Nuage, tels que Microsoft 365, dont SharePoint et Teams, ou Adobe Cloud, doivent faire l'objet d'une revue périodique pour archiver et supprimer les fichiers, documents et contenus inutiles. Une bonne pratique est d'organiser un plan de stockage des fichiers et de définir des durées de conservation raisonnables.

Outils de Communication

Les moyens de communication sont multiples et n'ont pas le même impact sur la qualité de la collaboration et sur l'environnement.

La communication directe favorise l'interaction et la contribution collective. Elle est sans impact sur l'environnement.

La communication téléphonique favorise l'immédiateté. Non prévue, elle est interruptive et doit être préférée dans les situations de réelle urgence. Son impact sur l'environnement est très faible.

La communication par Teams, audio ou vidéo réduit les distances et permet le travail sans contrainte de localisation. Comme la communication téléphonique, non prévue, elle est interruptive et doit être utilisée de manière planifiée de préférence. Son impact sur l'environnement est modéré.

La communication par messagerie permet de garder trace des échanges. Elle s'apparente à un échange écrit, rédigé et réfléchi. Elle est inadaptée pour des échanges interactifs.

L'usage qui consiste à joindre des fichiers à des messages et à diffuser de tels messages à plusieurs destinataires est à éviter du fait de son fort impact sur l'environnement. Il convient de lui préférer le partage de lien vers un fichier

disponible dans le Nuage ou mis à disposition sur une plateforme d'échange de fichiers sécurisée, telle que FileSender de Renater.

En règle générale, le respect de la Netiquette est préconisé dans l'usage de la messagerie.

Réseau et sécurité

Afin de permettre l'usage des équipements personnels (téléphone mobile, portable personnel), l'UCO offre sur la plupart de ses campus un accès Wifi Invité qui comprend l'accès à Internet. Cet accès est à préférer au partage de connexion Mobile qui sollicite davantage les infrastructures des opérateurs de téléphonie mobile et consomme les forfaits.

Pour les ordinateurs fournis par un campus de l'UCO, la connexion au réseau est effectuée par le service informatique du campus. Ce dernier s'assure en particulier que les bonnes pratiques d'installation et les règles de sécurité en vigueur sur le campus de l'UCO sont respectées.

Un utilisateur ne doit jamais quitter un poste de travail en libre-service sans se déconnecter.

Sur certains campus, les postes des salles informatiques et des salles équipées sont arrêtés automatiquement la nuit.

Télétravail ou travail en mobilité

Des services sont proposés aux utilisateurs en télétravail ou en mobilité.

En particulier, tous les services dans le Nuage ou exposés à l'Internet sont disponibles depuis n'importe quel appareil. En particulier, Microsoft 365 (Suite Office en ligne, Teams, SharePoint), @cademia, Intranet UCO, Chamilo, Ressources numériques des Bibliothèques Universitaires, entre autres. L'utilisation de ces services, en particulier la synchronisation par OneDrive de SharePoint ou Teams, doit être faite avec précaution sur un ordinateur personnel : cet ordinateur ne doit pas être partagé, doit être récent, maintenu à jour et doté d'un antivirus. Pour les utilisateurs salariés équipés par l'UCO d'un ordinateur portable, la synchronisation depuis un ordinateur personnel est inutile et non recommandée.

Les services « locaux », tels que des outils de gestion, paye, serveurs de fichiers, ne sont accessibles que par le moyen d'un Réseau Privé Virtuel (VPN). Seuls les ordinateurs portables mis à disposition par le service informatique du campus sont habilités à utiliser un client VPN permettant de se connecter au réseau local du campus. Il est interdit d'installer un tel outil sur un ordinateur personnel.

Chaque campus mettant en œuvre sa politique de télétravail, les utilisateurs sont invités à se tourner vers le service RH de leur campus pour connaître les procédures adaptées.

7. Information des utilisateurs sur la gestion des systèmes et réseaux informatiques

Les services, applications, systèmes et matériels informatiques de l'UCO sont opérés par des informaticiens (administrateurs, consultants, chefs de projets, techniciens, DSI) internes ou externes à la DSI de l'UCO.

Sous la responsabilité des directions des campus, des services et des facultés, ils mettent en œuvre les mesures appropriées et proportionnées pour garantir la disponibilité, l'intégrité et la confidentialité des données dans la limite des exigences exprimées et des moyens disponibles.

Ils peuvent entreprendre toute démarche nécessaire pour le maintien en conditions opérationnelles des services.

Ils doivent informer les parties prenantes, utilisateurs, responsables et partenaires concernés, de toute intervention susceptible d'affecter la disponibilité ou de modifier l'usage des services.

En cas de faille de sécurité identifiée, ils doivent en informer le groupe de sécurité informatique (cybersecurite@uco.fr)

8. Accès aux salles de cours Informatiques

Les utilisateurs s'engagent à respecter les règles d'accès aux salles de cours Informatiques. En particulier, les dispositifs de contrôle d'accès par badge , quand ils sont existants : la fermeture des portes ne doit pas être entravée et chaque personne doit badger pour entrer.

Les utilisateurs ne doivent pas débrancher, modifier la configuration des équipements, déplacer le matériel, réaménager les salles informatiques et laisser l'endroit dans l'état fonctionnel dans lequel ils aimeraient le trouver en arrivant.

9. Fichiers de traces

L'ensemble des services utilisés génèrent "des fichiers de traces". Ces fichiers sont essentiels à l'administration des systèmes. Ils servent à remédier aux dysfonctionnements des services ou systèmes informatiques utilisés. Ces fichiers conservent des informations personnelles par exemple concernant la messagerie (expéditeur, destinataire(s), date), mais aussi heures de connexion aux applications, au service de connexion à distance, identification de la machine depuis laquelle les services sont utilisés, etc.

Ce type de traces existent pour l'ensemble des services Internet. Ces fichiers ne sont utilisés que pour un usage technique. Toutefois, dans le cadre d'une procédure judiciaire et après accord du directeur de campus et du DSI ces fichiers peuvent être mis à la disposition de la justice.

10. Conclusion

Ce document est revu périodiquement et mis à disposition des utilisateurs pour mise en application.

L'utilisateur qui contreviendrait aux règles précédemment définies s'expose au retrait de son compte informatique, ainsi qu'aux poursuites disciplinaires et pénales, prévues par les textes législatifs et réglementaires en vigueur.

11. Les adresses utiles

accueil_DSI@uco.fr : Contact général avec la DSI
cybersecurite@uco.fr : Signaler une faille de sécurité
dpo_uco@uco.fr : Question sur le RGPD, déclaration d'un traitement de données personnelles