GUIDE TECHNIQUE DE L'UTILISATEUR DU SYSTEME D'INFORMATION

Mars 2022

université angers

TABLE DES MATIERES

INTRODUCTION

L'article 34 de la loi du 6 janvier 1978 modifiée (dite « loi Informatique et Libertés ») oblige l'université d'Angers à mettre en place toutes les précautions utiles pour préserver la sécurité des données.

L'article 32 du règlement européen 2016/679 du 27 avril 2016 (dit « règlement général sur la protection des données » ou RGPD) précise que la protection des données personnelles nécessite de prendre des « mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ».

C'est dans ce contexte que l'université d'Angers propose ce guide technique de l'«utilisateur» du système d'information pour aider à la mise en conformité et permettre d'appliquer les précautions élémentaires qui doivent être mises en œuvre.

Ce présent guide technique a pour objet de définir une série de procédures techniques devant être appliquées par toute personne utilisant les moyens informatiques et de télécommunications de l'université d'Angers.

Il complète la charte d'usage du système d'information présente dans le règlement intérieur de l'université d'Angers.

Les utilisateurs·trices sont informés·es que la violation des procédures régissant l'accès et l'utilisation du système d'information mis à leur disposition est susceptible d'entraîner des sanctions.

PROCÉDURES DE SÉCURITÉ

Gestion des codes d'accès

L'université d'Angers fournit à chaque utilisateur·trice de son système d'information un ou plusieurs codes d'accès (identifiants et mots de passe) qui lui sont propres.

L'identifiant principal est celui qui sert à s'authentifier sur la plupart des services numériques de l'université, notamment la messagerie électronique. Les autorisations d'accès aux données délivrées pas nos services numériques sont spécifiques à chaque personne authentifiée.

L'université d'Angers met en œuvre les moyens techniques afin d'assurer la confidentialité des codes d'accès mais ne peut être poursuivie si ceux-ci sont divulgués par suite d'une action frauduleuse.

Les mots de passe doivent respecter les règles générales présentes ci-après ; le mot de passe de l'identifiant principal requiert des exigences plus précises.

Règles de définition et de gestion des mots de passe

Chaque utilisateur·trice doit veiller au respect de la sécurité liée aux mots de passe permettant l'accès à ses environnements.

À cet égard, chaque utilisateur·trices est personnellement responsable des mots de passe qu'il a choisis. Il/Elle s'engage à :

- choisir un mot de passe sûr, n'ayant aucun lien avec son environnement familier ou social ;
- ne pas employer des mots de passe similaires à ceux qu'il/elle utiliserait dans un contexte autre que l'université d'Angers (réseaux sociaux, comptes bancaires, etc.) ;
- changer de mot de passe régulièrement selon une périodicité d'un an maximum si les applications le permettent ;
- changer son mot de passe dès le moindre soupçon de piratage de son compte ;
- ne pas écrire son mot de passe sur un support facilement accessible ;
- garder confidentiels ses mots de passe.

Actuellement le mot de passe associé à l'identifiant principal doit comporter au moins huit caractères, avec la présence d'au moins quatre types de caractères : alphabétiques majuscules (A-ZË), alphabétiques minuscules (a-zë), chiffres (0-9) et caractères spéciaux (@,#,;,!,*,…). Il ne doit pas contenir le nom, prénom et date de naissance.

L'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information) conseille d'employer des mots de passe de 16 caractères afin de minimiser les risques de découverte.

L'université d'Angers publie régulièrement sur son site web des conseils pour aider à construire un mot de passe sûr.

Paramétrage des postes de travail

Le poste de travail de l' utilisateur·trice fournit par l'université d'Angers constitue un outil qui doit être protégé des intrusions.

À cet égard, il convient :

- de ne jamais utiliser de session avec une identité ayant les droits administrateur autre que pour une opération le nécessitant ;
- de paramétrer la mise en veille automatique du poste de travail avec au

minimum demande du mot de passe pour la réactivation après 15 minutes d'inactivité ;
- de ne pas se connecter au réseau ou ouvrir des sessions applicatives inutilement ;
- de maintenir à jour le système d'exploitation ;
- de maintenir à jour les logiciels installés ;
- de ne pas désinstaller de logiciels qui participent à la sécurisation du poste de travail ;
- de ne pas installer de logiciels sans droit ou licence valide, et pour ceux à installer de s'assurer de leur origine (éditeur,…) ; pour toute installation il est recommandé d'en informer le Service d'Assistance et Moyens Informatique (SAMI) de la Direction du Développement du Numérique (DDN) ;
- de quitter les applications actives et effectuer systématiquement une déconnexion de l'ensemble des sessions ouvertes avant de quitter ou éteindre son poste de travail.

Recommandations liées au stockage des documents

En fonction de la sensibilité attribuée à un document des espaces de stockage différents sont proposés.

Pour tout utilisateur·trice uabox.univ-angers.fr est l'application conseillée si vous avez besoin de partager vos fichiers facilement via Internet.

Pour les personnels de l'université, les documents qui relèvent d'activités de recherche ou administratives ou qui contiennent des informations à caractère personnel doivent être conservés dans les espaces de stockage des personnels sur le réseau de l'UA. Ces espaces sont attribués généralement de manière automatique en fonction des services ou entités d'affectation.

Si des besoins spécifiques de sécurité renforcés apparaissent, exprimer les auprès du SAMI via l'application de demande d'assistance numérique (HelpDesk).

Pour des documents sans sensibilité produits au sein de groupes construits sur des durées limitées et pour lesquels des accès via Internet sont attendus nous recommandons d'utiliser la suite Office 365.

Dans tous les cas, évitez de stocker vos documents ou fichiers en local sur votre poste de travail car ils ne seraient pas sauvegardés par les procédures automatiques mises en œuvre par la DDN et ne pourraient donc pas être restaurés.

Utilisation d’un poste de travail personnel

L’université d’Angers fournissant en cas de besoin des postes de travail portables configurés selon ses prérogatives, l’utilisateur·trice ne doit pas installer sur ses propres postes de travail de composants logiciels liés au système d’information de l’université d’Angers sans validation explicite du SAMI.

MESSAGERIE ÉLECTRONIQUE

Limitations de la messagerie électronique

Les messages envoyés ou reçus font l’objet d’une limitation de taille particulière.

En cas de dépassement de la taille limite, le message est rejeté et l'émetteur reçoit un message de non-distribution.

Stockage et archivage des messages électroniques

Chaque utilisateur·trice est responsable du classement des messages qu'il a relevés.

Les messages électroniques gérés par le système de messagerie de l'université d'Angers et conservés sur les espaces de stockage associés sont sauvegardés quotidiennement.

L’ utilisateur·trice doit mettre en œuvre les moyens nécessaires à la conservation des messages qui pourraient être indispensables notamment en tant qu’élément de preuve.

Sécurité anti-virale

Il est déconseillé d’ouvrir des fichiers, de quelque nature que ce soit, en provenance d’un expéditeur inconnu, et en particulier, les fichiers compressés ~~(extension en .zip par exemple)~~ ou exécutables qui peuvent générer l’activation de virus informatiques, code malicieux etc., susceptibles d’entraîner des conséquences d’une extrême gravité pour l'université d'Angers.

L’université d’Angers émet régulièrement des recommandations sur les conduites à tenir vis-à-vis de messages électroniques frauduleux ou susceptibles de l’être soit par l’intranet soit par messages électroniques.

Les utilisateurs·trices sont informés·ées que l'université se réserve le droit de retenir, d'isoler et / ou de supprimer tout message électronique à l'aide de moyens automatisés de détection de virus et ce, sans que ces messages n'aient été nécessairement ouverts.

Tout message bloquant ou présentant une difficulté technique d'acheminement à son destinataire peut être détruit.

Utilisation abusive du compte de messagerie

Par analyse des flux de messages électroniques, l'université peut déceler qu'un compte de messagerie est utilisé de manière abusive, soit par le/la propriétaire du compte, soit par une utilisation frauduleuse de son compte. Dans ce cas une procédure de blocage du compte est activée. Le compte est désactivé.

La procédure envoie un message d'alerte aux informaticiens de proximité (SAMI) afin de les informer précisément des caractéristiques du compte bloqué. Comme son compte est bloqué, l'intéressé·e devrait prendre contact avec un membre du SAMI qui lui communiquera la procédure à suivre pour le déverrouiller ainsi que les recommandations de sécurité à suivre pour éviter une utilisation frauduleuse de celui-ci.

MATÉRIEL NOMADE

Les principes de précaution

Toute personne de l'université d'Angers, à qui a été confié exclusivement dans le cadre de ses activités professionnelles un équipement de type appareil photo numérique, caméscope, téléphone portable, ordinateur portable etc., doit veiller à le protéger.

L'utilisateur ne doit pas tenter de modifier le matériel ou sa configuration.

En cas de non utilisation, le matériel doit être rangé dans un endroit sécurisé.

Par ailleurs, l'«utilisateur» doit veiller particulièrement à ne pas exposer l'équipement confié à la chaleur, à l'humidité, ni le laisser sans surveillance.

Vol

En cas de vol de l'équipement fourni, une déclaration doit être effectuée sans délai au commissariat de police le plus proche avec copie adressée à ddn-finances@listes.univ-angers.fr.

Toute déclaration volontairement fausse est passible de sanctions disciplinaires et / ou de poursuites pénales.

Perte

En cas de perte de l'équipement confié, une déclaration détaillée doit être adressée à ddn-finances@listes.univ-angers.fr.

Détérioration

En cas de détérioration du matériel portable, celui-ci doit être retourné au responsable du prêt accompagné du détail des circonstances dues à sa détérioration.

Retour sur demande

A tout moment et sur simple demande du service SAMI de la DDN un ordinateur portable professionnel doit être retourné le plus tôt possible afin éventuellement d'être analysé inspecté et réinstallé par les informaticiens de proximité. Il s'agit ici par exemple de pouvoir réagir au plus tôt à une suspicion possible de la compromission de l'ordinateur, via un phishing ou toute autre action frauduleuse.

De cette réactivité dépend la sécurité commune du Système d'Information de l'UA.

ASSISTANCE NUMÉRIQUE

L'université propose à chaque utilisateur·trice de son système d'information de pouvoir formuler toute demande d'assistance numérique via un outil de suivi nommé HelpDesk (http://helpdesk.univ-angers.fr).

L' utilisateur·trice doit utiliser cet outil en cas de constat de panne ou pour effectuer une demande d'évolution ou de demande de service.

ÉVOLUTION DU PRÉSENT GUIDE

Le présent Guide Technique de l'«utilisateur» est régulièrement mis à jour et il appartient aux utilisateurs·trices de prendre connaissance des nouvelles versions qui seront portées à sa connaissance par l'université d'Angers par le biais de la messagerie électronique ou par Intranet.

Les utilisateurs·trices devront veiller à se conformer aux dernières dispositions en vigueur.