Table des matières

1. Introduction

1.1. But

La Haute Ecole Arc met à disposition de ses étudiant-e-s différents services basés sur son infrastructure informatique comme par exemple: le courrier électronique, l'impression, le stockage de données ou encore l'accès à Internet. Tous ces services sont à considérer comme des outils de travail mis à disposition par l'école.
Ce document définit les règles que les utilisateurs et utilisatrices des ressources informatiques de la Haute Ecole Arc doivent appliquer afin de permettre une exploitation efficace et sûre des services offerts par l'informatique. Elle décrit les comportements souhaitables et ceux qu'il faut éviter afin d'assurer la sécurité des données et la disponibilité des services.

1.2. Objet

Ce document existe en deux versions: la première est destinée au personnel de la Haute Ecole Arc et la seconde est destinée aux étudiant-e-s de cette école.
La présente version est celle qui s'adresse à l'ensemble des étudiant-e-s de la Haute Ecole Arc.

2. Comportements inadéquats et sanctions

Tous les comportements considérés comme inadéquats sont décrits en détail dans les chapitres suivants et font l'objet d'un résumé final. Les personnes qui ne respecteraient pas les directives indiquées s'exposent à des sanctions précisées ci-après. Des contrôles périodiques sont réalisés et les résultats positifs ou négatifs sont communiqués aux personnes responsables ainsi qu'aux domaines concernés.

Types de comportements inadéquats et sanctions

Type	Sanctions
N (Négligence)	Ce type de comportement constitue une négligence de l'étudiant-e. En cas de récidive, de comportement répétitif et/ou délibéré, les sanctions prévues pour les cas de malveillance sont applicables.
U (Utilisation abusive)	Utilisation abusive des ressources de la Haute Ecole Arc. En principe, ce type de comportement donne lieu à une sanction administrative, sous réserve d'éventuelles poursuites pénales et du remboursement des montants dus. En cas de récidive, de comportement répétitif et/ou délibéré, les sanctions prévues pour les cas de malveillance sont applicables.
M (Malveillance)	Les cas graves peuvent mener à des sanctions sévères pouvant aller jusqu'au l'exmatriculation. Sont réservés l'engagement de poursuites pénales, la facturation des frais de procédure ainsi que l'engagement d'une action récursoire au sens de l'article 22 de la convention concernant la Haute Ecole Arc.

3. Directives

3.1. Charte globale de sécurité

Cette directive a pour but d'informer tous les utilisateurs et utilisatrices de l'informatique de la Haute Ecole Arc sur les problèmes de sécurité existants et sur les attitudes personnelles et collectives à avoir pour améliorer la sécurité informatique globale.

3.1.1. Sécurité du réseau

La Haute Ecole Arc a créé et exploite son propre réseau informatique qui relie tous ses lieux d'activité. Le réseau est conçu de manière à ce que les utilisatrices et les utilisateurs puissent l'utiliser indépendamment du lieu d'activité où ils se trouvent. Ce réseau est relié à Internet au travers de filtres (pare-feu, serveur mandataire) afin de contrôler autant les accès entrants que ceux sortants.
La sécurité du réseau est de la responsabilité du service informatique et consiste d'une part à assurer la confidentialité des données et d'autre part à garantir l'exploitation des services offerts.

Pour protéger efficacement le réseau de la Haute Ecole Arc, vous avez l'interdiction de :

- mettre en œuvre des services d'accès externes (modems ou autres moyens de télécommunication directs) sur votre serveur, votre PC ou le réseau local
- créer des serveurs locaux, des serveurs Internet ou de messagerie sur le réseau local
- permettre l'accès au réseau interne de l'école à des tiers au travers d'un PC connecté par VPN
- capturer le trafic du réseau de la Haute Ecole Arc
- rediriger ce trafic
- attaquer le réseau ou l'infrastructure informatique (par exemple : attaque par déni de service ou par force brute)

Ceci dit, la possibilité de créer et d'activer d'autres serveurs existe pour autant que l'installation soit faite en collaboration avec le service informatique.

3.1.2. Sécurité des serveurs

L'exploitation de la plupart des services offerts par l'informatique nécessite l'utilisation de serveurs. Ceux-ci sont en général accessibles par toutes les utilisatrices et tous les utilisateurs, ce qui les rend particulièrement délicats à sécuriser. Certains serveurs sont même accessibles de l'extérieur du réseau de la Haute Ecole Arc.

3.1.2.1. Serveur Intranet

Le serveur Intranet est un serveur de communication interne à la Haute Ecole Arc. Toutes les personnes disposants d'un compte informatique de la Haut Ecole Arc ont la possibilité d'accéder au serveur Intranet. Par contre aucune personne externe à notre réseau ne peut y accéder.

3.1.2.2. Serveur Internet

Le serveur Internet (www.he-arc.ch) est le serveur officiel de la Haute Ecole Arc. Il a pour but de concentrer l'ensemble des informations publiques concernant la Haute Ecole Arc sur le Web. C'est un serveur accessible par des personnes du monde entier.

3.1.2.3. Serveur de messagerie

Le risque principal lié au service de messagerie est la réception et la propagation de virus par l'ouverture malencontreuse d'un message douteux. Les destinataires et destinatrices des messages ont donc un rôle fondamental à jouer dans cette gestion. Ils ou elles doivent s'assurer avant de l'ouvrir, que le message reçu provient d'un-e correspondant-e connu-e et que l'objet du message n'est pas douteux.

3.1.3. Accès à Internet

Les utilisateurs et utilisatrices s'engagent à n'utiliser Internet que dans le cadre exclusif de leur fonction au sein de la Haute Ecole Arc et déclarent notamment s'abstenir d'accéder à des serveurs et/ou à des fournisseurs d'informations dont le contenu serait illicite ou contraire aux bonnes mœurs.
Toutes les connexions à Internet faites depuis le réseau de la Haute Ecole Arc doivent obligatoirement passer par un serveur mandataire (proxy) qui contrôle les accès ainsi réalisés. Le serveur mandataire permet ainsi, sur demande d'un-e responsable, de générer la liste des accès effectués durant les derniers mois depuis le réseau interne de la Haute Ecole Arc.

3.2. Les 8 règles d'or

Un comportement correct des utilisatrices et utilisateurs est indispensable pour assurer la sécurité et la stabilité des services et des données. L'expérience a démontré que c'est malheureusement souvent à ce niveau que l'on rencontre le plus de problèmes. Les utilisateurs et utilisatrices peuvent engendrer, par le non-respect des consignes de sécurité, des dégâts dont les conséquences éthiques, juridiques et financières peuvent être importantes.

Les 8 règles d'or à respecter par tous:

1. changer régulièrement tous ses mots de passe (recommandation : 3 fois par an) ;
2. ne jamais communiquer un mot de passe à qui que ce soit ;
3. ne jamais inscrire son mot de passe sur des papiers accessibles par autrui, ni utiliser des mots de passe trop courts (moins de 8 positions) ou évidents (nom de famille, numéro de téléphone, etc.) ; il faut au minimum prévoir une minuscule, une majuscule et un chiffre;
4. ne pas laisser son poste de travail enclenché sans surveillance ; lors d'une absence même brève (pause), sortir au minimum de toutes les applications sensibles ou verrouiller le poste ; et lors d'une absence prolongée, par exemple pause de midi, séance de travail ou le soir, sortir des applications et éteindre ou verrouiller le poste de travail ;
5. ne jamais utiliser une clé USB sans la passer au préalable à l'antivirus ;
6. ne jamais communiquer des informations à autrui sur son environnement de travail ;
7. ne jamais tenter de s'introduire dans un système ou dans un environnement informatique sans avoir, au préalable, reçu une autorisation d'accès ;
8. prévenir le service informatique et, si nécessaire, la direction de tout incident, même bénin, et en particulier de ceux liés à la sécurité et à la confidentialité des données.

Comme on le voit, la sécurité liée au comportement est l'affaire de toutes et de tous. C'est certainement l'un des seuls risques importants qu'il n'est pas possible de gérer par des moyens techniques.

3.3. Règles déontologiques d'utilisation des ressources informatiques

3.3.1. Utilisation des postes de travail de la Haute Ecole Arc

La Haute Ecole Arc met des postes de travail fixes ou mobiles à disposition de son personnel et de ses étudiant-e-s. Seules les modifications de la configuration des PC faites dans un but professionnel sont autorisées. Les utilisateurs-trices de ces postes sont priés de les traiter de manière à ne pas les détériorer (éviter de les faire tomber, de renverser des boissons dessus…).

Comportements inadéquats

- Modifier la configuration du PC dans un but non professionnel (économiseurs d'écran, nouveaux périphériques, nouveaux composants, nouveaux logiciels, etc.).
- Installer des logiciels sans détenir les licences nécessaires.
- Modifier le câblage ou les branchements des PC
- Charger, installer ou utiliser des jeux, des logiciels illégaux, des logiciels ou des images qui ne sont pas en rapport avec l'activité professionnelle.
- Lire, modifier ou détruire des documents d'autres personnes sans leur accord, même si vous y avez accès avec votre propre compte informatique.
- Introduire par manque de précaution des virus ou d'autres logiciels dangereux dans le réseau informatique.
- Introduire délibérément des virus ou d'autres logiciels dangereux dans le réseau informatique.
- Copier des logiciels protégés par des droits d'auteur.
- Charger, consulter, stocker, ou diffuser des documents qui portent atteinte à la dignité de la personne, présentant un caractère pornographique, incitant à la haine raciale, constituant une apologie du crime ou de la violence (respect des règles juridiques, et code pénal art. 173, 197 et 261).

3.3.2. Utilisation des postes de travail privés

On désigne par poste de travail tout équipement informatique fixe ou mobile pouvant se connecter au réseau de la Haute Ecole Arc.
Le service informatique met en place des points de connexion qui permettent de raccorder temporairement des postes de travail privés au réseau informatique de la Haute Ecole Arc.

Toute personne qui désire utiliser ces points de connexion se doit :

- de contacter le service informatique pour obtenir les modalités de configuration et avertir les responsables informatiques qu'il va utiliser ces points de connexion,
- de s'assurer qu'un logiciel antivirus est installé sur son poste de travail et qu'il est à jour,
- d'accepter les mécanismes de sécurité et de mise à jour demandés par la Haute Ecole Arc
- de respecter les règles présentées dans ce document.

Comportements inadéquats

- Installer des logiciels sans détenir les licences nécessaires.
- Lire, modifier ou détruire des documents d'autres personnes sans leur accord, même si vous y avez accès avec votre propre compte informatique.
- Introduire par manque de précaution des virus ou d'autres logiciels dangereux dans le réseau informatique.
- Introduire délibérément des virus ou d'autres logiciels dangereux dans le réseau informatique.
- Copier des logiciels protégés par des droits d'auteur.
- Charger, consulter, stocker, ou diffuser des documents qui portent atteinte à la dignité de la personne, présentant un caractère pornographique, incitant à la haine raciale, constituant une apologie du crime ou de la violence (respect des règles juridiques, et code pénal art. 173, 197 et 261).

3.3.3. Utilisation des mots de passe

Les mots de passe sont nécessaires pour sécuriser l'ensemble des systèmes informatiques (accès aux réseaux, aux applications et aux données). Ils protègent l'utilisateur et l'utilisatrice en lui donnant des droits, en termes de gestion et d'accès aux applications et aux données.
Le mot de passe est une information personnelle et confidentielle qui ne doit être communiquée à personne. Les mots de passe doivent être modifiés régulièrement, par leur détenteur ou leur détentrice, de manière à s'assurer que personne ne puisse les utiliser à son insu.

Le mot de passe identifie également l'utilisateur ou l'utilisatrice lors de toutes les actions faites par ce dernier ou cette dernière dans les différents systèmes informatiques et le ou la rend donc responsable de ses actes.

Comportements inadéquats

- Communiquer un mot de passe à d'autres personnes, même à des proches.
- Afficher ou stocker son ou ses mots de passe à proximité du poste de travail.
- Créer des mots de passe facile à trouver (nom de famille, nom des enfants, etc.). Un bon mot de passe comporte au minimum 8 caractères numériques et alphanumériques (ex. to23bIsA) ainsi que d'un mélange de minuscules et de majuscules.
- Tenter de découvrir le mot de passe d'une autre personne.
- Utiliser un mot de passe ou un compte qui ne vous appartient pas.

3.3.4. Utilisation de la messagerie

La messagerie permet la transmission de documents ou d'informations entre deux ou plusieurs correspondant-e-s.

Elle est particulièrement sensible en terme de sécurité car elle constitue le principal canal d'entrée de données externes (donc potentiellement dangereuses) dans le réseau de la Haute Ecole Arc. En outre elle permet aussi de faire sortir du réseau des données qui ne le devraient peut-être pas. L'envoi et la réception de messages privés sont admis pour autant que leur fréquence soit faible et que leur contenu soit correct.

Le serveur de messagerie de la Haute Ecole Arc permet de centraliser les messages en un seul endroit, ce qui rend la consultation possible depuis plusieurs postes différents. Cette pratique a pour désavantage de consommer beaucoup d'espace disque sur le serveur et de rendre les sauvegardes plus complexes.

Il est donc nécessaire de trier et d'effacer régulièrement les messages trop anciens. Les messages importants pourront être archivés sur d'autres serveurs afin de ne pas surcharger le serveur de messagerie.
Les serveurs de messageries conservent une trace de toutes les opérations effectuées. Ces données pourront être consultées par le service informatique et la direction en cas d'abus.

L'adresse de l'expéditeur-trice est un des éléments permettant aux destinataires de valider leurs courriels entrants. Il est donc nécessaire d'utiliser l'adresse fournie par la Haute Ecole Arc comme adresse d'expéditeur-trice pour les courriels envoyés à titre professionnel ou dans le cadre des études. En outre, l'envoi de courriels au nom de la Haute Ecole Arc, mais portant une adresse d'expéditeur-trice n'appartenant pas à l'école, nuit à l'image de notre établissement.

Comportements inadéquats

- Envoi de courriels professionnels ou en rapport avec les études ayant une adresse d'expéditeur-trice autre que celle fournie par la Haute Ecole Arc.
- Envoi de documents ou de messages sans lien direct avec l'activité professionnelle notamment propagande politique, syndicale ou publicitaire.
- Ouverture de messages douteux (auteur inconnu, nom incongru de l'objet) pouvant contenir des virus (ne surtout pas ouvrir de pièce jointe dans ces cas-là !).
- Envoyer et faire suivre des documents n'ayant rien à faire avec l'activité de la personne (toute information sur les virus doit être envoyée uniquement au service informatique, même si on vous dit qu'il faut la transmettre à tous-toutes vos correspondant-e-s).
- Stocker un grand nombre de messages sur le serveur et encombrer inutilement de l'espace disque.

3.3.5. Utilisation d'Internet

L'Internet permet d'accéder à la plus grande banque d'information mondiale. Il vous permet d'obtenir, dans le cadre exclusif de votre fonction, des informations générales ou particulières sur un grand nombre de domaines.
Une utilisation modérée d'Internet à des fins non professionnelles est tolérée pour autant que les règles déontologiques de ce document soient respectées.

Recommandation

Le coût de la connexion Internet est proportionnel à la quantité de données téléchargées par l'ensemble des postes de la Haute Ecole Arc sur des sites non académiques. Les sites académiques du monde entier (universités, instituts de recherche...) sont gratuits. Il existe un tarif de jour et un tarif de nuit. Le tarif de nuit étant nettement meilleur marché, il est fortement conseillé d'effectuer les gros transferts durant cette période.

Comportements inadéquats

- Utiliser abusivement (en temps moyen passé et/ou en volume de données transmises) l'accès à Internet à des fins privées.
- Télécharger de grandes quantités de données depuis Internet, sans chercher à réduire les coûts (utilisation prioritaire des sites académiques).
- Accéder à des sites qui ne sont pas en rapport avec l'activité professionnelle.
- Discuter sur des « CHATs » ou des forums n'ayant aucun lien avec votre fonction.
- Téléchargement de jeux, de logiciels illicites ou tout autre fichier n'ayant aucun rapport avec votre fonction ou qui pourrait constituer une atteinte aux bonnes mœurs.

Remarque importante :

Pour accéder à Internet, vous devez passer par un serveur mandataire (proxy). Ce dernier permet d'optimiser les accès, de diminuer les temps de réponse et d'obtenir des statistiques, mais également de savoir précisément sur quels sites vous naviguez. Vous devez être conscient-e que ces informations peuvent servir à déceler des comportements inadéquats.

3.3.6. Utilisation de l'accès par VPN

Les réseaux privés virtuels (VPN : Virtual Private Network) vous permettent de créer un canal sécurisé entre une source et une destination. Grâce à cette technologie tous les utilisateurs et toutes les utilisatrices du système informatique (direction, secrétariat, corps enseignant, personnel et corps estudiantin) ont accès aux ressources du réseau de la Haute Ecole Arc depuis n'importe où.
Il suffit de vous connecter chez votre fournisseur Internet habituel puis d'établir la connexion VPN pour accéder aux ressources du réseau de la Haute Ecole Arc.

Toute personne qui désire utiliser l'accès par VPN se doit :

- de s'assurer qu'un logiciel antivirus est installé sur son poste de travail et qu'il est à jour,
- de respecter les règles présentées dans ce document.

Comportement inadéquat

- Avoir le routage actif sur une machine connectée par VPN à l'école.

3.3.7. Utilisation de l'espace disque

La Haute Ecole Arc met à disposition de ses employé-e-s et des étudiant-e-s un certain nombre de disques en réseau. Certains disques sont ouverts à tous et toutes. D'autres sont destinés à un groupe restreint. Les données contenues dans la plupart de ces disques sont sauvegardées régulièrement. Chaque personne se voit attribuer un quota initial d'utilisation pour son espace personnel.

Ce quota initial est fixé avec le responsable de l'utilisateur ou de l'utilisatrice. Toute modification devra être approuvée par le service informatique.

Comportements inadéquats

- Dépasser le quota autorisé.
- Déposer sur un disque public des données confidentielles sans en protéger l'accès.
- Déposer ou installer sur les disques locaux ou en réseau
  - o des documents qui pourraient être une atteinte aux bonnes moeurs selon les articles 173, 197 et 261 du code pénal,
  - o des jeux ou des virus,
  - o des logiciels protégés par des droits d'auteur,
  - o des logiciels mettant en danger la sécurité du réseau informatique.

Remarque importante :

Pour des raisons techniques (par exemple à cause des sauvegardes), le service informatique a accès à tous les fichiers stockés sur les serveurs de la Haute Ecole Arc. Il lui est donc possible de vérifier que les règles ci-dessus sont bien respectées et de détecter des abus.

3.3.8. Utilisation des imprimantes et photocopieuses en réseau

La Haute Ecole Arc met à disposition un certain nombre d'imprimantes et de photocopieuses en réseau.
Pour y accéder, vous devez passer par un serveur d'impression. Ce dernier permet de gérer les droits d'accès, de compter les pages imprimées, d'identifier la nature des documents imprimés et d'obtenir des statistiques. Vous devez être conscient-e que ces informations peuvent servir à déceler des comportements inadéquats.
L'impression sur les imprimantes coûte plus cher que la copie ou que l'impression sur les photocopieurs.
L'utilisation des photocopieurs est recommandée pour tous les tirages de plus de quelques feuilles (en mode copie ou en mode impression).

Comportements inadéquats

- Imprimer des documents qui pourraient être une atteinte aux bonnes mœurs selon les articles 173, 197 et 261 du code pénal.
- Utiliser les imprimantes / photocopieuses pour un usage privé sur les comptes d'exploitation de la Haute Ecole Arc.
- Imprimer des documents et ne pas venir les chercher.
- Imprimer un gros document pendant la journée, ce qui bloque l'accès des autres personnes pendant une trop longue période.
- Imprimer de gros volumes sur les imprimantes de bureau (veuillez imprimer sur les photocopieurs ou faire des photocopies).
- Accéder aux imprimantes réseau sans passer par le serveur d'impression.

3.3.9. Mise à disposition de logiciels et de matériel par la Haute Ecole Arc

La mise à disposition des étudiant-e-s de matériel ou de logiciels fait l'objet d'une réglementation particulière qui dépend des objets mis à disposition. Toute mise à disposition d'objet informatique est coordonnée par le service informatique.
Sauf réglementation contraire lorsque l'étudiant-e quitte l'école tout le matériel est à rendre et tous les logiciels fournis par l'école doivent être désinstallés.

3.3.10. Protection des données de la Haute Ecole Arc

Grâce à leur compte informatique, les utilisateur-trice-s obtiennent un accès à toutes sortes de données propres à la Haute Ecole Arc. Ces données sont par exemple stockées dans des répertoires ou disponibles dans l'Intranet. Il peut s'agir de supports de cours, de listes d'adresses, de règlements, de documents des projets, de processus, etc. La règle de base est de considérer toutes ces données comme étant la propriété de la Haute Ecole Arc et donc de ne pas les transférer à l'extérieur de l'école, ni de les publier sous quelque forme que ce soit sans l'accord de leur propriétaire.
Le stockage de ces données doit se faire de préférence sur les serveurs de l'école afin que leur sauvegarde et leur confidentialité soient assurées. En cas d'utilisation d'autres types de stockage (disque local d'un PC, clé USB, 'cloud'...) les utilisateurs-trices sont responsables de la confidentialité et de la pérennité des données.
Certains projets font l'objet d'une convention de confidentialité entre un mandant et l'école L'ensemble du personnel et des étudiant-e-s est tenu par de telles conventions.

Comportements inadéquats

- Mettre à disposition de tiers par mail, FTP, site Web ou tout autre moyen des données de l'école sans l'accord du propriétaire des données
- Créer des compilations ou des résumés des données de l'école à des fins de publication sans l'accord des propriétaires des données
- Divulguer des listes d'adresses du personnel ou des étudiant-e-s

4. Droits de la Haute Ecole Arc

L'infrastructure informatique de la Haute Ecole Arc est un outil de travail mis à disposition des étudiant-e-s. Il n'existe aucun droit à l'accès à cette infrastructure. La direction de la Haute Ecole Arc décide de la mise à disposition ou non de cet outil. Elle décide également des services qui sont offerts sur la base de cette infrastructure.
La Haute Ecole Arc se réserve le droit de surveiller, dans les limites fixées par la loi, l'utilisation qui est faite par les étudiant-e-s de l'outil informatique.

5. Protection des données des étudiant-e-s

La gestion par l'école des données des étudiant-e-s est conforme à la loi sur la protection des données. Cette gestion est en grande partie centralisée dans l'application IS Academia pour les étudiant-e-s de la HES-SO. Afin d'assurer l'intégration des étudiant-e-s dans les applications de la HES-SO mais aussi dans les réseaux universitaires, il est nécessaire que certaines informations les concernant soient publiées dans des annuaires et donc accessibles à un public plus vaste, mais se limitant toujours au personnel d'autres écoles ou institutions.

Les informations suivantes sont susceptibles d'être publiées :

- Nom
- Prénom
- Date de naissance
- Sexe
- Numéro d'immatriculation
- Langue préférée
- Ecole fréquentée
- Filière, orientation et spécialisation fréquentées
- Adresse de courrier électronique
- Adresse postale

Les annuaires web de la HE-Arc et de la HES-SO publient les noms et prénoms des étudiant-e-s.
Par sa signature au bas du document 'Engagement des étudiant-e-s à suivre les directives pour l'utilisation des ressources informatiques' l'étudiant-e affirme accepter les conditions d'accès à ses données décrites dans de ce chapitre.

6. Résumé des comportements inadéquats et du type de sanctions qui en découlent

Thème	Comportement inadéquat	Type	Pages
Généralités Serveur, Réseaux locaux, PC	• Mettre en oeuvre des services d'accès externes sur un serveur, un PC ou le réseau local.	**M**	3
	• Créer des serveurs locaux, des serveurs Internet ou de messagerie sur le réseau local.	**M**	3
	• Permettre l'accès au réseau interne de l'école à des tiers au travers d'un PC connecté par VPN.	N	3, 7
	• Capturer le trafic du réseau de la Haute Ecole Arc	**M**	3
	• Rediriger le trafic du réseau	**M**	3
	• Attaquer le réseau ou l'infrastructure informatique	**M**	3
	• Modifier la configuration du PC dans un but non professionnel.	**M**	4
	• Charger, installer ou utiliser des jeux, des logiciels illégaux, des logiciels ou des images qui ne sont pas en rapport avec l'activité professionnelle.	U	4, 7
	• Détériorer ou risquer de détériorer le matériel	N	4
	• Installer des logiciels sans détenir les licences nécessaires.	**M**	4, 5
	• Modifier le câblage ou les branchements des PC fixes de la Haute Ecole Arc	**M**	4
	• Lire, copier, modifier ou détruire des documents d'autres personnes sans leur accord, même si vous y avez accès avec votre propre compte informatique.	**M**	4, 5
	• Introduire par manque de précaution des virus ou d'autres logiciels dangereux dans le réseau informatique.	N	4, 5
	• Introduire délibérément des virus ou d'autres logiciels dangereux dans le réseau informatique.	**M**	4, 5
	• Copier des logiciels ou des données protégés par des droits d'auteur.	**M**	4, 5
	• Charger, consulter, stocker, imprimer ou diffuser des documents qui portent atteinte à la dignité de la personne, présentant un caractère pornographique, incitant à la haine raciale, constituant une apologie du crime ou de la violence (respect des règles juridiques, et code pénal art. 173, 197 et 261).	**M**	4, 5, 7, 8

Thème	Comportement inadéquat	Type	Pages
Mots de passe	• Communiquer un mot de passe à d'autres personnes.	N	5
	• Afficher ou stocker son ou ses mots de passe à proximité du poste de travail.	N	5
	• Créer des mots de passe facile à trouver (nom de famille, nom des enfants…).	N	5
	• Tenter de découvrir le mot de passe d'une autre personne.	**M**	5
	• Utiliser un mot de passe, un compte ou les données d'une autre personne.	**M**	5
Utilisation de la messagerie électronique	• Envoyer des courriels professionnels ou en rapport avec les études ayant une adresse d'expéditeur-trice autre que celle fournie par la Haute Ecole Arc.	**M**	6
	• Envoyer des documents ou des messages sans lien direct avec l'activité professionnelle notamment de la propagande politique ou syndicale.	**M**	6
	• Ouvrir des messages douteux (auteur inconnu, nom incongru de l'objet) pouvant contenir des virus (ne surtout pas ouvrir la pièce jointe !).	N	6
	• Envoyer et faire suivre des documents n'ayant rien à faire avec l'activité professionnelle.	U	6
Internet	• Utiliser abusivement (en temps moyen passé et/ou en volume de données transmises) l'accès à Internet à des fins privées.	U	7
	• Télécharger de grandes quantités de données depuis Internet, sans chercher à réduire les coûts (utilisation prioritaire des sites académiques).	U	7
	• Accéder à des sites qui ne sont pas en rapport avec l'activité professionnelle.	U	7
	• Discuter sur des « CHATs » ou des forums n'ayant aucun lien avec votre fonction.	U	7
Stockage sur disques réseaux	• Stocker un grand nombre de messages et de fichiers sur le serveur et encombrer inutilement de l'espace disque.	N	6
	• Dépasser le quota autorisé sur les disques en réseau.	N	8
	• Déposer sur un disque public des données confidentielles sans en protéger l'accès.	**M**	8

Thème	Comportement inadéquat	Type	Pages
Impression de documents et imprimantes	• Utiliser les imprimantes et photocopieuses à des fins privées sur les comptes d'exploitation de la Haute Ecole Arc.	U	8
	• Imprimer des documents sans aller les chercher.	N	8
	• Imprimer de gros documents pendant la journée.	N	8
	• Imprimer de gros volumes sur les imprimantes de bureau.	U	8
	• Accéder aux imprimantes réseau sans passer par le serveur d'impression.	U	8
Protection des données de la Haute Ecole Arc	• Mettre à disposition de tiers par mail, FTP, site Webv ou tout autre moyen des données de l'école sans l'accord du propriétaire des données.	**M**	9
	• Créer des compilations ou des résumés des données de l'éocole à des fins de publication sans l'accord des propriétaires des données.	**M**	9
	• Divulguer des listes d'adresses du personnel ou des étudiant-e-s.	**M**	9
	• Stocker des données de l'école sur des PC ou des serveurs externes et ne garantissant pas leur pérennité et leur confidentialité.	N	9