

# GUIDE PRATIQUE POUR L'UTILISATION DES RESSOURCES INFORMATIQUES

---

*Ce document complète la "Directive concernant les ressources informatiques de la HE-Arc (Charte informatique)".*

Pour un plus grand confort de lecture, le texte est rédigé au masculin. Il s'adresse



évidemment aussi bien aux femmes qu'aux hommes.

# TABLE DES MATIÈRES

ISO 9001  
1006 051 18

haute école  
neuchâtel berne jura **arc**

|        |  |   |
|--------|--|---|
| 0      | Introduction                             | 3 |
| 0.1    | Public cible                             | 3 |
| 0.2    | Objectifs                                | 3 |
| 1      | Dispositions générales                   | 3 |
| 1.1    | Concernant l'article 2                   | 3 |
| 1.2    | Concernant l'article 3                   | 3 |
| 1.3    | Concernant l'article 4                   | 3 |
| 2      | Utilisation des ressources informatiques | 4 |
| 2.1    | Concernant l'article 5                   | 4 |
| 2.2    | Concernant l'article 6                   | 4 |
| 2.3    | Concernant l'article 7                   | 4 |
| 2.4    | Concernant l'article 8                   | 4 |
| 2.5    | Concernant l'article 10                  | 5 |
| 2.6    | Concernant l'article 11                  | 5 |
| 2.7    | Concernant l'article 12                  | 6 |
| 2.8    | Concernant l'article 13                  | 6 |
| 2.9    | Concernant l'article 15                  | 6 |
| 2.10   | Concernant l'article 16                  | 6 |
| 2.11   | Concernant l'article 17                  | 7 |
| 2.12   | Concernant l'article 18                  | 8 |
| 2.12.1 | Réception du courriel                    | 8 |
| 2.12.2 | Envoi du courriel                        | 9 |
| 2.13   | Concernant l'article 19                  | 9 |
| 3      | Moyens de contrôle                       | 9 |
| 3.1    | Concernant l'article 20                  | 9 |
| 4      | Sanctions                                | 9 |
| 4.1    | Concernant l'article 23                  | 9 |

# 1 Introduction

## 1.1 Public cible

Ce document s'adresse à toutes les personnes qui utilisent les ressources informatiques et/ou téléphoniques de la HE-Arc.

## 1.2 Objectifs

Ce texte constitue un guide pratique d'utilisation des ressources informatiques et téléphoniques de la HE-Arc. Il complète et explicite la « Directive concernant les ressources informatiques de la HE-Arc (Charte informatique) », ci-après la Charte informatique. Il est basé sur la même structure et il est conseillé de lire les deux documents en parallèle.

# 2 Dispositions générales

## 2.1 Concernant l'article 2

Les droits et obligations spécifiques aux membres du service informatique et aux autres personnes ayant des droits élargis sont documentés dans la « Directive concernant les droits d'accès élargis aux ressources informatiques », disponible sur le site web de l'école.

Les activités des laboratoires ou de l'enseignement nécessitent parfois des configurations particulières. Néanmoins les règles de base de la charte informatique doivent toujours être respectées comme avoir un antivirus sur tous les équipements connectés au réseau et effectuer les mises à jour de sécurité.

Les bénéficiaires de prestation sont les personnels des établissements auxquels la HE-Arc fournit des prestations comme le ceff, la HEM, Néode...

## 2.2 Concernant l'article 3

Le catalogue des services disponible sur l'intranet indique quelles sont les prestations du service informatique et de l'infrastructure informatique. Le contenu de ce catalogue est fixé par la direction de l'école.

## 2.3 Concernant l'article 4

La HE-Arc souhaite travailler dans un climat de confiance avec les utilisateurs. Elle attend de ces derniers qu'ils fassent preuve de loyauté envers l'institution, de respect pour les autres usagers et de bon sens. Elle attend aussi que les ressources mises à disposition soient utilisées avec parcimonie et que le matériel soit traité avec soin.

Afin d'assurer le bon fonctionnement des équipements, il est demandé de ne pas boire ou manger dans les bureaux, les salles de cours, les salles de conférences, les salles de groupes et les salles équipées de PC publics. Les règlements propres aux différents bâtiments s'appliquent.

Les équipements remis en prêt par la HE-Arc (PC portables, téléphones portables...) doivent être traités avec soin et préservés du vol. Il n'existe pas de droit à la remise d'un tel appareil. En principe de tels appareils ne sont remis qu'à des personnes ayant un taux d'activité d'au moins 50% à la HE-Arc.

## 3.1 Concernant l'article 5

Actuellement des quotas sont configurés pour la zone de stockage personnelle (disque U:) et pour la boîte aux lettres. Des augmentations de quota du disque U: peuvent être demandées au service informatique. La décision finale concernant une telle augmentation revient au directeur du domaine concerné.

## 3.2 Concernant l'article 6

Les données personnelles des utilisateurs sont traitées par la HE-Arc conformément aux lois sur la protection des données. Certains logiciels de gestion de l'école sont mis à disposition par la HES-SO ou par l'administration neuchâteloise (IS-Academia, SAP...). Des données des utilisateurs y sont enregistrées et sont visibles par certains membres du personnel de ces organisations.

Voici une liste non exhaustive des données gérées dans IS-Academia :

- Nom
- Prénom
- Date de naissance
- Sexe
- Numéro d'immatriculation
- Numéro AVS
- Langue préférée
- École fréquentée
- Filière, orientation et spécialisation fréquentées
- Adresse de courrier électronique à la HE-Arc
- ...

Les annuaires web de la HE-Arc et de la HES-SO publient le nom, le prénom et l'adresse de courriel HE-Arc des étudiants et du personnel, ainsi que le numéro de téléphone professionnel lorsqu'il en existe un.

En outre, dans le cadre des relevés destinés à l'office fédéral de la statistique, différentes données du personnel et des étudiants sont transférées à cet organisme. Veuillez vous référer aux règles de ces institutions concernant leurs engagements à respecter la protection des données.

## 3.3 Concernant l'article 7

Des règles particulières existent concernant l'utilisation des téléphones mobiles mis à disposition par la HE-Arc.

## 3.4 Concernant l'article 8

L'installation de logiciels à des fins de test est tolérée sans en référer au service informatique pour autant que les conditions suivantes soient respectées :

- Installation uniquement sur le PC personnel, ou sur un PC de laboratoire. Pas d'installation sur les PC publics ni ceux des salles de cours. L'installation se fait en principe sur un seul PC.
- Le logiciel n'abaisse pas le niveau de sécurité de l'infrastructure de la HE-Arc (par exemple pas de pont vers internet, pas d'analyse du trafic réseau, pas de logiciel contrevenant à la charte informatique...)

Aucun support n'est fourni pour ces logiciels.

ISO 9001:2015

De lors qu'un logiciel est utilisé pour l'enseignement, pour de la Ra&D ou pour toutes autres activités que des tests, le service informatique doit être consulté.

### 3.5 Concernant l'article 10

L'utilisation des ressources informatiques de la HE-Arc au travers d'équipements privés (PC privés, tablettes, téléphones portables) amenés dans les locaux de l'école (ou au travers du VPN) est autorisée. Néanmoins les utilisateurs de tels équipements sont tenus de s'assurer que ces appareils ne constitueront pas un danger pour le réseau de la HE-Arc. Les aspects suivants devront être contrôlés avant même la connexion au réseau de la HE-Arc:

- Les PC Windows, Linux et Mac sont équipés d'un antivirus fonctionnel et disposant d'une base de détection à jour
- Toutes les mises à jour des logiciels ont été installées
- L'appareil utilise le mode de configuration dynamique de l'adresse IP (client DHCP)
- Il n'offre aucun service pouvant interférer avec ceux de la HE-Arc (en particulier pas de serveur DHCP actif)

Actuellement un antivirus n'est pas exigé pour les équipements fonctionnant sous Android, sous IOS et sous Windows Phone.

### 3.6 Concernant l'article 11

Le personnel utilise systématiquement le compte privé lié à son badge lorsqu'il fait des impressions/copies qui ne sont pas directement liées à son travail à la HE-Arc. Dans la mesure du possible l'impression en noir est préférée à l'impression en couleur afin de limiter les coûts.

Il est nécessaire d'utiliser les appareils multifonctions de Canon ("photocopieur") pour toutes les impressions dépassant une dizaine de pages. Il est vivement recommandé d'anticiper les gros travaux d'impression et de copie afin de ne pas être à la merci d'une panne toujours possible.

Toutes sortes de problèmes peuvent surgir lors de l'utilisation de photocopieurs multifonctions, comme un manque de papier ou de toner, ou encore un bourrage de papier. En cas de difficulté nous vous recommandons la démarche suivante:

- Suivez les instructions du photocopieur (remettre du papier, résoudre un bourrage...). N'exercez jamais de forces importantes, car vous pourriez détériorer l'appareil. Tous les éléments s'ouvrent et se ferment sans effort.
- Si vous ne parvenez pas à résoudre le problème, informez le service informatique sans délai ([helpdesk@he-arc.ch](mailto:helpdesk@he-arc.ch))
- Si vous traitez des documents confidentiels, vous souhaitez vous assurer qu'aucune page ne reste dans le photocopieur ou n'en sortira lors de sa remise en service. Les travaux en cours peuvent être consultés en utilisant la touche représentant un oeil ou la touche de l'écran tactile 'Moniteur syst.' selon le modèle. Là vous verrez les travaux encore en attente et vous pourrez les effacer, y compris la tâche en cours. Ceci vous assure que ces travaux ne seront pas relancés lors de la remise en service. Les travaux d'impression ainsi annulés devront être relancés depuis un PC. Si vous pensez que des feuilles sont peut-être encore dans le photocopieur, par exemple si vous n'avez pas pu résoudre un bourrage, contactez le service informatique.
- Vous pouvez ensuite poursuivre vos travaux sur un autre photocopieur

### **3.7 Concernant l'article 12**

Assurer la sécurité de l'infrastructure informatique d'une école est un défi tout à fait particulier, car celle-ci doit être très ouverte. Il doit être possible de l'utiliser avec des équipements qui ne sont pas sous le contrôle du service informatique de l'école, et la palette des activités qu'on doit pouvoir y exercer est très large. En outre des données sensibles y sont enregistrées.

C'est pourquoi les utilisateurs, par leur comportement, jouent un rôle essentiel dans cette sécurité. Leur prudence et leur circonspection sont indispensables, en particulier

- lors de la réception de mail
- lors de téléchargement depuis internet
- lors de la connexion d'appareils privés au réseau de la HE-Arc
- lors de la lecture de support de données externes
- lors du stockage de données ailleurs que sur les serveurs de la HE-Arc
- dans la gestion de leur mot de passe
- lors de l'accueil de visiteurs

Tous les logiciels utilisés à l'école, y compris les systèmes d'exploitation, doivent être à jour et supportés par le fournisseur. Les mesures nécessaires doivent être prises pour éviter de contaminer l'infrastructure informatique avec des logiciels malveillants.

L'enseignement de l'informatique et les activités de « Ra&D/prestations de service » dans ce domaine peuvent nécessiter des dérogations aux règles de la charte informatique. Ces dérogations sont à demander au service informatique. Lorsqu'il est fait usage de telles dérogations, il sera toujours fait tout ce qui est possible pour en limiter l'usage dans le temps et le périmètre concerné.

### **3.8 Concernant l'article 13**

Le compte informatique est bloqué dès le départ de la personne. C'est pourquoi il faut anticiper la récupération des données privées ainsi que leur nettoyage de l'infrastructure de la HE-Arc.

### **3.9 Concernant l'article 15**

Toute action faite dans le cadre d'une session ouverte avec un certain binôme nom d'utilisateur/mot de passe est réputée avoir été faite par la personne à laquelle appartient le nom d'utilisateur. Le mot de passe doit être protégé contre l'accès par des tiers.

Les utilisateurs verrouillent les PC qu'ils quittent, même temporairement, et s'assurent que personne ne peut faire usage de leur compte

Un changement de mot de passe est exigé par le système deux fois par an au travers d'un mail. Diverses vérifications sont faites concernant le choix d'un nouveau mot de passe (utilisation de majuscule, de minuscule, de chiffre et de caractères spéciaux, longueur minimale, non-réutilisation d'un ancien mot de passe...). Il faut éviter de choisir des mots de passe trop simples à deviner par des tiers. Le mot de passe du compte informatique de la HE-Arc ne doit pas être utilisé pour d'autres comptes utilisés au travers d'internet comme ceux des réseaux sociaux ou des magasins en ligne.

### **3.10 Concernant l'article 16**

Comme des droits d'accès et de l'argent sont liés au badge, il faut éviter de le laisser sans surveillance, par exemple sur un photocopieur durant les impressions/copies.

La perte du badge doit être annoncée immédiatement au secrétariat qui l'a émis.

Le remplacement d'un badge, lorsqu'il est payant, coûte 20.-

### 3.11 Concernant l'article 17

On entend par 'données', toutes les informations disponibles sous format électronique. Il peut s'agir de textes, de listes, d'images, de contenus de bases de données, d'annuaires ou de courriels... Ces informations peuvent concerner l'enseignement, la gestion de l'école, le personnel et les étudiants, les projets...

Il existe une large panoplie d'espaces de stockage possibles pour les fichiers. En voici les principales caractéristiques:

| Espace de stockage  | Pérennité <sup>1</sup> | Confidentialité | Remarque  |
|---|------------------------|-----------------|---|
| Disque réseau sur les serveurs de la HE-Arc (disque I: à U:, sauf T:) | Assurée                | Assurée         | C'est la variante à utiliser par défaut et la seule tolérée pour les données confidentielles et/ou sensibles. Toutes les données appartenant à la HE-Arc doivent être à jour sur ces disques. |
| Disque C: du PC   | Pas assurée            | Pas assurée     | À utiliser uniquement pour des données non confidentielles et dont la pérennité ne doit pas être assurée  |
| Disque crypté du PC   | Pas assurée            | Assurée         | À utiliser uniquement pour des données dont la pérennité ne doit pas être assurée   |
| Bureau du PC  | Pas assurée            | Pas assurée     | Ces données sont sur le disque C:   |
| SwitchDrive   | Pas assurée            | Pas assurée     | À utiliser uniquement pour des données non confidentielles et devant être partagées   |
| Autres services dans le cloud (Dropbox, OneDrive, Google Drive...)    | Pas assurée            | Pas assurée     | L'utilisation pour des données professionnelles ou en rapport avec les études est prohibée  |
| Clé USB ou autre support amovible non crypté <sup>2</sup>             | Pas assurée            | Pas assurée     | À utiliser uniquement pour des données non confidentielles et dont la pérennité ne doit pas être assurée  |
| Clé USB ou autre support amovible crypté                              | Pas assurée            | Assurée         | À utiliser uniquement pour des données dont la pérennité ne doit pas être assurée   |

Pour des raisons techniques le service informatique a accès à toutes les données stockées sur les serveurs et les PC de la HE-Arc. Des dispositions particulières règlent le comportement des membres de ce service lors de l'accès aux données personnelles et privées (voir article 14 de la charte).

<sup>1</sup> La pérennité des données stockées dans des zones non pérennes peut être assurée en ayant une copie actuelle des données en zone pérenne.

<sup>2</sup> Disque dur amovible, carte SD, CD, DVD...





## 3.12 Concernant l'article 18

### 3.12.1 Réception du courriel

Le courriel constitue un canal d'entrée important pour les logiciels malveillants. Il peut aussi être utilisé dans le cadre de l'ingénierie sociale<sup>3</sup> ou pour de l'hameçonnage<sup>4</sup>. Il est donc particulièrement important d'analyser attentivement les courriels reçus, avant même de les ouvrir ou d'en ouvrir les pièces jointes. Voici quelques règles simples afin de ne pas être victime d'un courriel malveillant :

- Vérifier l'adresse de l'expéditeur.
- Vérifier l'objet et le texte du message : si vous estimez que le courriel ne vous concerne pas, effacez-le.
- Vérifier les liens dans le courriel, ceux-ci doivent être cohérent avec l'adresse de l'expéditeur. (exemple, si vous recevez un courriel de Swisscom et que le lien dans le courriel pointe sur [www.voleur.xx](http://www.voleur.xx), cela doit vous mettre la puce à l'oreille !). Il faut passer le pointeur de la souris sur les liens contenus dans le courriel pour voir l'URL où ils pointent réellement. Le texte du lien, l'adresse de l'expéditeur et l'URL doivent être cohérents. Ne cliquez sur les liens que si vous êtes raisonnablement sûr de la sécurité du courriel.
- Vérifier le professionnalisme du courriel : l'orthographe et la grammaire sont souvent maltraitées dans les courriels malveillants.

Soyez tout particulièrement vigilant avant d'ouvrir une éventuelle pièce jointe. Celles-ci contiennent parfois des virus ou autres malwares.

Les arnaques par courriel sont souvent :

- Des messages alarmistes et des menaces de fermeture de compte.
- Des promesses d'argent avec peu ou pas d'effort.
- Des affaires qui semblent trop belles pour être vraies.
- Des demandes de donation à une œuvre caritative après une catastrophe qui a été annoncée dans les médias
- Des factures ou des rappels de factures qui ne vous concernent pas

Soyez prudents, ne donnez jamais vos informations de login, vos informations bancaires, ou toutes autres informations personnelles suite à la réception d'un courriel. Ne cliquez sur aucun lien figurant sur un spam. Ne téléchargez pas de fichiers à partir de liens inconnus.

Le service informatique ne vous demandera jamais votre mot de passe par mail, ni même par téléphone.

Le mail entrant subit différents filtrages. Ils visent à réduire le volume de courriels indésirables que vous recevez. Vous pouvez configurer les expéditeurs dont vous ne voulez jamais recevoir les courriels, ou ceux dont vous voulez toujours les recevoir.

Nous vous recommandons de séparer rigoureusement vos courriels privés de vos courriels professionnels. À cette fin il est utile d'avoir deux adresses distinctes pour ces deux pans de votre vie. Vous vous éviterez beaucoup de courriels indésirables en ne saisissant votre adresse professionnelle que lorsque c'est réellement indispensable.

<sup>3</sup> L'ingénierie sociale (ou social engineering en anglais) est une forme d'acquisition déloyale d'information et d'escroquerie, utilisée en informatique pour obtenir d'autrui, un bien, un service ou des informations clés (Wikipedia)

<sup>4</sup> L'hameçonnage, phishing ou filoutage est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité (Wikipedia)

Il est obligatoire de lire régulièrement les courriels arrivant à votre adresse de l'école. Les directions utilisent le courriel pour faire passer des informations importantes devant être lues par toutes et tous.

Votre boîte aux lettres doit toujours être configurée de manière à ce qu'un courriel qui vous est adressé personnellement, et à vous seul, ne soit lu que par vous. Une fois un tel courriel lu, vous pouvez bien entendu décider de le faire suivre à un tiers. Mais ceci ne peut pas être automatisé afin qu'on puisse s'adresser à vous seul.

Veuillez noter que les échanges de courriels sont cryptés au sein de l'école, mais que ce n'est plus le cas en dehors de celle-ci. Les courriels circulent en clair au travers d'internet et doivent être considérés comme des cartes postales.

### **3.12.2 Envoi du courriel**

Les courriels professionnels, ou en lien avec les études à la HE-Arc, doivent impérativement être envoyés avec l'adresse mail de l'école comme adresse d'expéditeur. L'utilisation d'une adresse mail privée pour des communications ayant un rapport avec l'école est interdite et il est également interdit d'utiliser une telle adresse pour recevoir du courriel en rapport avec l'école.

L'envoi de mail publicitaire ou de propagande aux listes de distribution de l'école est interdit. Il est également défendu d'envoyer des courriels non désirés (spam).

Lorsque l'envoi d'un courriel à un grand nombre de destinataires est indispensable (par exemple pour un sondage), le service informatique sera contacté afin que l'envoi n'amène pas à un blocage des serveurs de mail de la HE-Arc. La gestion de listes d'adresses externes doit permettre aux personnes y figurant de se faire retirer des listes.

## **3.13 Concernant l'article 19**

L'accès à la partie académique d'internet (autres hautes écoles du monde entier) est gratuit. Par contre l'accès aux sites non académiques est lui payant, à des tarifs différents entre le jour et la nuit. C'est pourquoi l'accès à cette partie d'internet doit rester modéré.

L'utilisation de logiciels d'échange de fichier peer-to-peer est interdite, sauf accord explicite du service informatique sur la base d'une demande motivée. Les utilisateurs s'abstiendront d'accéder à des contenus illicites ou contraires aux bonnes mœurs. Les jeux en réseau sont également prohibés, qu'ils fassent usage de la connexion à internet ou non.

Lors de téléchargements une grande prudence est de mise, car chaque logiciel, chaque image, chaque mise à jour peut contenir des logiciels malveillants. Il convient de ne télécharger que des versions officielles des logiciels, et directement depuis la page du fournisseur original.

L'accès à internet ne doit évidemment pas être utilisé pour des activités malveillantes, telles que par exemple des attaques par déni de service.

# **4 Moyens de contrôle**

## **4.1 Concernant l'article 20**

À titre d'exemple, le service informatique surveille la charge de l'accès internet, ou l'évolution de l'occupation des espaces de stockage sur les serveurs.



# 5 Sanctions

## 5.1 Concernant l'article 23

Pour les étudiants, les sanctions prévues dans le règlement des études peuvent être appliquées.