Université de Rouen Normandie

# CHARTE DE GESTION DU POSTE DE TRAVAIL

Validé par le Comité de Pilotage du Numérique le 9 novembre 2020

## 1 Préambule

Ce document a pour but de préciser les bonnes pratiques concernant la gestion des postes de travail à l'université de Rouen Normandie. Il entre dans la catégorie des chartes spécifiques prévues au paragraphe 7 de la Charte du système d'information de l'université de Rouen-Normandie, elle-même adoptée par le Conseil d'Administration.

Il tient compte des recommandations de la politique de sécurité des systèmes d'information de l'État (PSSI-E).

Il a pour but de permettre une utilisation rationnelle et organisée des moyens informatiques.

## 2 Propriété du poste de travail

Les postes de travail (fixes ou portables) sont fournis par l'établissement ou par les partenaires institutionnels (CNRS, INSERM, etc.) pour les unités mixtes.

Les personnels, quel que soit leur statut, ne sont donc pas propriétaires des postes mis à leur disposition.

Les personnels doivent restituer les postes mis à leur disposition sur simple demande et en tous les cas lors de leur départ de l'établissement, quelle qu'en soit la raison.

Les postes portables sont gravés au nom de l'établissement.

## 3 Connexion au réseau d'établissement

Les postes personnels (non fournis par l'institution) ne doivent en aucun cas être connectés au réseau filaire de l'établissement.

La connexion d'équipements non fournis par l'institution ou par les partenaires institutionnels est néanmoins possible via le réseau sans-fil (Wi-Fi) eduroam ou via les réseaux « invités ».

## 4 Choix du poste de travail

### 4.1 Ordinateur fixe ou portable

En accord avec sa hiérarchie, chaque agent peut opter pour un poste fixe ou pour un ordinateur portable (associé à une station d'accueil et ses périphériques) selon ses besoins. La puissance actuelle des ordinateurs portables ne justifie pas la mise à disposition d'un poste fixe et d'un ordinateur portable.

Compte tenu du développement des usages en situations de mobilité (enseignement et recherche, déplacements, réunions, télétravail...), le choix d'un ordinateur portable est préconisé en priorité au niveau de l'établissement.

Lors de la remise de l'équipement, l'utilisateur doit signer un « bordereau de remise d'un ordinateur » et s'engager à en respecter les conditions.

### 4.2 Configuration type

En cas d'équipement portable, l'utilisateur pourra être équipé d'une station d'accueil avec des périphériques externes (écran, clavier, souris, etc.). En revanche, sauf dérogation spécifique, un seul écran externe sera attribué par poste.

En fonction des missions de l'agent, un filtre de confidentialité peut constituer une option.

Le matériel de marque Apple n'est pas recommandé au niveau de l'établissement. A performances égales, il représente un surcoût d'environ 40% selon les modèles. Les périphériques sont également beaucoup plus coûteux. Surtout, il est plus difficile pour les services informatiques d'administrer ce type d'équipement et de l'intégrer au domaine unique.

### 4.3 Travail à distance

En cas de travail à distance, l'équipement sera obligatoirement de type portable. Conformément, au protocole de télétravail, il ne sera pas fourni de station d'accueil ou de périphériques externes pour équiper le domicile des agents.

### 4.4 Choix technique

Les utilisateurs peuvent exprimer leurs besoins fonctionnels auprès des personnels informatiques de l'établissement. Ces besoins fonctionnels sont pris en compte pour le choix du matériel dans la mesure des moyens de l'établissement. Les personnels informatiques sont compétents pour le choix technique du matériel.

#### 4.4.1 Adaptation du poste de travail

L'adaptation du poste de travail à un éventuel handicap ou pour répondre à une exigence médicale est possible sur demande.

## 5 Administration des postes de travail

La gestion des postes est assurée par les personnels informaticiens de l'établissement. En conformité avec la politique de sécurité des systèmes d'information de l'État (17 juillet 2014), par défaut, les utilisateurs ne disposent pas des droits d'administration de leur poste de travail.

### 5.1 Accès au poste de travail

L'accès à tous les postes de travail doit être protégé par des identifiants (login et mot de passe).

### 5.2 Intégration au domaine

Afin de permettre une homogénéité de gestion du parc informatique de l'établissement, les postes doivent, chaque fois que c'est possible, être intégrés au domaine unique de l'établissement

### 5.3 Configuration logicielle

Dans la majorité des cas, l'établissement utilise des mécanismes de déploiement de logiciels basés sur des paquetages. Cela permet une standardisation des postes de travail, accélérant les déploiements et facilitant les maintenances et mises à jour ultérieures.

Il est souhaitable, dans la mesure du possible, d'utiliser exclusivement les logiciels référencés par l'établissement. Des dérogations sont possibles pour répondre à des besoins fonctionnels particuliers. Ces installations spécifiques ne pourront se faire qu'après expression explicite de ces besoins par les utilisateurs et après validation par la DSI.

Dans tous les cas :

- Les licences logicielles seront strictement respectées
- Les logiciels préconisés par l'établissement ne seront ni désactivés, ni désinstallés

### 5.4 Droits d'administration

De manière exceptionnelle, certains utilisateurs peuvent souhaiter disposer des droits d'administration de leur poste. Cette possibilité est soumise à l'appréciation du responsable informatique local ou de la DSI.

Dans ce cas, un compte local supplémentaire disposant des droits d'administration doit être créé. Les utilisateurs ne doivent pas se connecter avec ce compte disposant des privilèges « administrateur », mais utiliser temporairement le mécanisme d'élévation de privilèges.

Les utilisateurs choisissant de disposer de droits administrateurs sur leur poste s'engagent :

- À respecter l'ensemble des lois, règlements, chartes et politiques en vigueur dans l'établissement
- À assurer eux-mêmes la gestion de leur poste en autonomie

## 6 Stockage des données

### 6.1 Type de données

Les données stockées localement sur le poste de l'utilisateur ne sont pas sauvegardées. Il appartient à l'utilisateur de stocker les données qu'il souhaite sauvegarder sur les espaces partagés mis à sa disposition par la DSI et ceci selon le type de données (Cf. ci-dessous).

### 6.2 Données professionnelles

Les données professionnelles qui nécessitent d'être partagées avec d'autres utilisateurs doivent trouver leur place sur l'espace « GroupDir » (dénommés X: ou Y: en environnement Windows).

Les données professionnelles propres à l'utilisateur doivent être stockées sur l'espace « HomeDir » (Z: ).

### 6.3 Données professionnelles « de recherche »

Pour les données de recherche (volumétrie importante), il convient de prendre contact avec la DSI pour envisager une solution adaptée (disponibilité, intégrité, confidentialité, etc.)

### 6.4 Données personnelles

En application du droit à la vie privée résiduelle, les utilisateurs peuvent stocker leurs données personnelles dans un dossier local dénommé « privé ».

Ces données doivent être légales (pas de téléchargement illicite, logiciels piratés, etc.) et respecter le caractère résiduel de la vie privée sur le lieu de travail (volumétrie raisonnable, sans impact financier pour l'établissement).

### 6.5 Confidentialité/Sécurité

Les utilisateurs sont informés qu'afin d'assurer le respect de la présente charte, la DSI peut être amenée à mettre en place des traitements automatiques (via robots logiciels) parcourant les espaces et les données qu'ils contiennent.

## 7 Procédure d'urgence

### 7.1 En cas de compromission du poste de travail

En cas de compromission du poste de travail (virus, ransomware, etc.), le poste peut être repris par les personnels informatiques de l'établissement afin d'être réinstallé sans récupération des données locales.

Il appartient à l'utilisateur de s'assurer que :

- Ses données professionnelles sont stockées à un endroit où la sauvegarde est assurée
- Ses données personnelles sont sauvegardées par ses propres moyens

### 7.2 En cas de perte ou vol du poste de travail

Tout vol ou perte d'un poste de travail doit systématiquement être signalé dans les meilleurs délais au RSSI (rssi@univ-rouen.fr) et au responsable sûreté (surete@univ-rouen.fr).

## 8 Chiffrement du poste de travail

Afin d'assurer la protection des données stockées localement sur le poste en cas de vol, il est nécessaire de chiffrer l'intégralité du disque dur.

Cette mesure technique concerne particulièrement les ordinateurs portables. Elle correspond à la mesure "PDT-NOMAD-STOCK" de la PSSI de l'État (17 juillet 2014). En outre, elle est obligatoire dans les unités CNRS depuis le 6 janvier 2011.

L'intégralité du disque dur sera donc chiffrée en utilisant la solution associée au système d'exploitation natif :

- BitLocker pour Windows
- FileVault pour MacOS
- LUKS/DM-Crypt pour Linux

Afin de respecter les règles de l'art, les mesures complémentaires suivantes seront systématiquement appliquées :

- Mise en place d'une clé de recouvrement
  - Cette clé permet l'accès aux données en cas d'oubli, d'indisponibilité de l'utilisateur ou de réquisition judiciaire
- Séquestre de cette clé dans une infrastructure de stockage à accès hiérarchisé
  - Conservation dans les coffres-forts numériques mis à disposition par l'établissement ou éventuellement au sein du domaine unique.
- Stockage des données conformément au paragraphe 5-Stockage des Données (ci-dessus)

- Cette mesure permet de garantir la récupération des données en cas de vol du poste ou d'incident technique