UNIVERSITÉ DE FRIBOURG
UNIVERSITÄT FREIBURG

Gestion des postes de travail

Directive DIT-6 Champ d'application : Université

1 Introduction

La gestion du parc informatique nécessite l'utilisation de logiciels spécialisés pour les domaines de l'inventaire informatique, la gestion des tickets, la mise à jour des systèmes et le support technique. Dans ce cadre, la gestion des postes de travail est prévue selon les principes énoncés ci-après.

Cette directive s'applique aux postes de travail disposant d'une étiquette d'inventaire DIT, installés avec l'image standard de l'Université.

2 Gestion de l'inventaire

2.1 Postes de travail Apple

Les clients *Apple Remote Desktop* récupèrent les informations d'inventaire sur chaque poste de travail, et les envoient sur le serveur hébergeant l'application *Apple Remote Desktop*. Depuis ce serveur, un export SQL light est exécuté mensuellement, et les informations d'inventaire sont importées dans Pytheas Asset Management. Le client *Apple Remote Desktop* fait partie de l'image standard Mac fournie par la DIT.

2.2 Postes de travail Windows

Deux fois par mois, au login de l'utilisateur, l'agent Pytheas est installé sur le poste de travail. L'agent écrit les informations d'inventaire dans un fichier texte temporaire, qui est envoyé au serveur Pytheas Asset Management. L'agent est ensuite désinstallé.

2.3 Postes de travail Linux

Aucune gestion de l'inventaire n'est en place pour les postes de travail Linux.

3 Distribution de logiciels

3.1 Postes de travail Apple

Le service *NetBoot* permet l'installation d'images du système d'exploitation et de logiciels sur un poste de travail. Un catalogue d'applications standard est disponible, lesquelles peuvent être installées via *NetBoot*. Le service *NetBoot* fait partie de l'image standard Mac fournie par la DIT.

Version	Date	Remplace	Auteur(s)	Commentaires
1.0	6.10.2008	-	J.F. Descloux B. Helfer	Etablissement de la directive
1.1	1.7.2014	1.0	A. Gachet	Changement SIUF par DIT ; mise aux normes de la nouvelle corporate ; normalisation des numéros de directives DIT
1.2	20.2.2018	1.1	S. Recrosio A. Gachet	Refonte du document, ajout de la section 4 Prise de contrôle à distance

3.2 Postes de travail Windows

L'agent *Baramundi* permet à la DIT de distribuer des logiciels directement par le réseau. Il permet aussi à l'utilisateur d'installer un ensemble de logiciels mis à disposition par la DIT dans le « kiosque » *Baramundi*. L'agent *Baramundi* fait partie de l'image standard Windows fournie par la DIT.

3.3 Postes de travail Linux

Aucune solution centralisée de distribution de logiciels n'est en place pour les postes de travail Linux.

4 Prise de contrôle à distance

Les Correspondant-e-s Informatiques (CIs) ainsi que certains collaborateurs et certaines collaboratrices de la DIT sont habilité-e-s à prendre le contrôle d'une machine dans le cadre de leur activité de support informatique. Les contrôles à distance effectués par les correspondants informatiques sont limités aux ordinateurs Windows des unités organisationnelles pour lesquelles ils fournissent du support.

Une prise de contrôle à distance, sur un ordinateur Windows et sur un Mac, permet au technicien de voir l'écran de l'ordinateur et d'interagir avec le système et les applications.

4.1 Protection des données

Parmi les cas de figure décrits aux chapitres 4.2 et 4.3 ci-après, il peut arriver que le technicien prenant le contrôle à distance d'une machine ait accès aux données de l'utilisateur en son absence (disque local, HOME, COMMON/<UO>). Il n'existe pas de solution technique permettant d'empêcher un tel accès en toutes circonstances. Dans une telle situation, il est formellement interdit au technicien de consulter les données de l'utilisateur, de quelque manière et sous quelque forme que ce soit. Toute infraction à cette règle sera considérée comme une atteinte à l'ordre universitaire (art. 115 des Statuts de l'Université). En outre, les dispositions prévues par la LPers (art. 44 et 75) demeurent réservées.

4.2 Postes de travail Apple

L'outil *Apple Remote Desktop* est utilisé pour la prise de contrôle à distance. Le service doit être actif sur le poste client, et *Apple Remote Desktop server* doit être installé sur le poste initiant la prise de contrôle. Avant une prise de contrôle, l'utilisateur est systématiquement contacté par le technicien effectuant la prise de contrôle. En outre, cette activité doit être documentée dans un ticket Pytheas.

Lorsqu'une session utilisateur est ouverte sur le poste à contrôler et que l'utilisateur est présent devant son poste de travail, il peut observer les manipulations du technicien. Toutes les données de l'utilisateur (disque local, HOME, COMMON/<UO>) sont accessibles.

Lorsqu'une session utilisateur est ouverte mais verrouillée, la prise de contrôle à distance n'est pas possible.

Lorsqu'aucune session utilisateur n'est ouverte et qu'une prise de contrôle est initiée, les données de l'utilisateur (disque local, HOME, COMMON/<UO>) ne sont pas accessibles. Ce cas de figure se présente lors d'une installation d'un logiciel spécifique à distance.

Lorsqu'une session utilisateur est ouverte et non verrouillée, il est possible d'accéder à toutes les données de l'utilisateur (disque local, HOME, COMMON/<UO>), sans quittance de l'utilisateur. Une telle prise de contrôle, sans agrément explicite de l'utilisateur, ne peut être autorisée à titre exceptionnel que par la préposée à la protection des données de l'Université, le responsable de la sécurité informatique (RSI), ou leurs suppléants désignés. Les autorisations sont documentées sous forme écrite. Le chapitre 4.1 de la présente directive s'applique.

4.3 Postes de travail Windows

L'outil *Remotely Anywhere* est utilisé pour la prise de contrôle à distance. Avant une prise de contrôle, l'utilisateur est systématiquement contacté par le technicien effectuant la prise de contrôle. En outre, cette activité doit être documentée dans un ticket Pytheas.

Lorsqu'une session utilisateur est ouverte sur le poste à contrôler, la prise de contrôle est effective uniquement après la quittance de l'utilisateur. L'utilisateur peut donc observer les manipulations du technicien. Toutes les données de l'utilisateur (disque local, HOME, COMMON/<UO>) sont accessibles.

Lorsqu'une session utilisateur est ouverte mais verrouillée, la prise de contrôle à distance n'est pas possible.

Lorsqu'aucune session utilisateur n'est ouverte et qu'une prise de contrôle est initiée, les données de l'utilisateur (HOME et COMMON/<UO>) ne sont pas accessibles. Par contre, les données du disque local (« C : ») sont accessibles. Ce cas de figure se présente lors de l'installation d'une machine à distance. Le chapitre 4.1 de la présente directive s'applique.

Lorsqu'une session utilisateur est ouverte et non verrouillée, il est possible d'accéder à toutes les données de l'utilisateur (disque local, HOME, COMMON/<UO>), sans quittance de l'utilisateur, en modifiant un paramètre de *Remotely Anywhere*. Une telle prise de contrôle, sans agrément explicite de l'utilisateur, ne peut être autorisée à titre exceptionnel que par la préposée à la protection des données de l'Université, le responsable de la sécurité informatique (RSI), ou leurs suppléants désignés. Les autorisations sont documentées sous forme écrite. Le chapitre 4.1 de la présente directive s'applique.

4.4 Postes de travail Linux

La prise de contrôle à distance de postes de travail Linux n'est pas utilisée par la DIT.

5 Règles à respecter

Pour assurer une gestion efficace du parc informatique, il est impératif que les techniciens (DIT et CIs) respectent les règles suivantes pour les systèmes configurés par la DIT :

- n'installer que les images standard fournies par la DIT;
- ne pas modifier/désactiver/supprimer les comptes d'administration des machines ;
- ne pas désactiver le service "Apple Remote Desktop" (qui autorise un accès via le compte d'administration) ;
- ne pas désinstaller/désactiver le service "Baramundi" ;
- installer les patchs de sécurité du système et des applications pour PC et Macintosh ;
- ne pas modifier les paramètres de sécurité (Firewall, antivirus, système) ;
- ne pas modifier les paramètres de configuration insérés par la DIT ;
- respecter toutes les directives de la DIT ;
- les cas particuliers demeurent réservés.

6 Application

Cette directive a été approuvée par la Comité de direction IT (séance du 29.11.2017), par le Comité Stratégique IT lors de la séance du 20.2.2018, et par la préposée à la protection des données de l'Université, et entre en vigueur immédiatement.