UNIVERSITÉ DE FRIBOURG
UNIVERSITÄT FREIBURG

Procédure en cas de vol ou de perte de matériel IT

Directive DIT-13 Champ d'application : Université

1 Introduction

Le développement constant d'appareils informatiques mobiles et performants (*ultrabooks*, tablettes, *smartphones*) amène les utilisateurs à se déplacer de plus en plus fréquemment avec ces machines, lesquelles contiennent souvent une grande quantité de données propres à l'utilisateur, que ce soit dans le cadre professionnel ou privé.

Corollaire de cette mobilité accrue, le risque d'égarer ou de se faire voler ces appareils augmente, avec toutes les conséquences que cela implique en termes financiers et de protection des données.

La constatation d'un vol ou d'une perte est un événement perturbant, face auquel il n'est pas toujours aisé de réagir de manière optimale. Dans ce contexte, la présente directive vise deux objectifs : *(a)* garantir la meilleure protection possible des données et des infrastructures IT de l'Université en cas de vol de matériel IT, et *(b)* apporter aux utilisateurs confrontés à un vol ou à une perte un soutien dans la manière de gérer cet événement.

2 Prévenir un vol ou une perte de matériel et/ou de données

Différentes bonnes pratiques générales, la plupart découlant du bon sens, permettent de réduire les risques de vol ou de perte de matériel lors de déplacements (ne jamais laisser ses affaires sans surveillance, ne pas quitter sa place dans un train sans prendre ses affaires avec soi si l'on voyage seul, même pour se rendre aux WC, etc.).

Cette directive ne revient pas sur ces bonnes pratiques, mais se concentre sur les mesures propres à l'IT permettant, même en cas de vol ou de perte de matériel, d'éviter le vol des données qui s'y trouvent :

1. *Choisir un mécanisme fort de verrouillage de l'appareil IT.* Quasiment tous les appareils IT mobiles récents permettent de verrouiller l'accès au système lorsqu'il n'est pas utilisé. Le degré de protection du mode de verrouillage va d'une protection faible (déverrouillage par simple *swipe* sur l'écran) à une protection forte (login avec validation en deux étapes) en passant par diverses protections moyennes (*pattern*, PIN, mot de passe). La DIT recommande de choisir

Version	Date	Remplace	Auteur(s)	Commentaires
1.0	23.9.2013	-	A. Gachet/ B. Vuillemin	Etablissement de la directive et validation par comité de direction IT
1.1	3.10.2013	-		Validation par Comité stratégique IT
1.2	15.7.2014	1.1	A. Gachet	Mise aux normes de la nouvelle corporate identity ; nouvelle numérotation de la directive

un mode de verrouillage aussi fort que possible, tout en restant adapté au type d'appareil utilisé[1].

2. *Chiffrer l'intégralité du contenu de l'appareil IT.* La plupart des appareils IT récents permettent de chiffrer de manière complète les comptes, configurations, applications téléchargées, données, fichiers multimédia et autres fichiers de l'appareil, sans impact remarquable sur les performances. Dans le meilleur des cas, le chiffrement se fait de manière transparente sur l'ensemble du système de fichiers, sans que l'utilisateur n'ait à sélectionner manuellement les fichiers à chiffrer. Le chiffrement du contenu de l'appareil réduit sensiblement le risque que les données de l'appareil soient exploitées à mauvais escient en cas de vol ou de perte de l'appareil lui-même. La DIT recommande de toujours chiffrer le contenu de l'appareil.
3. *Utiliser un logiciel de suivi et de contrôle à distance.* Il existe pour la plupart des systèmes d'exploitation des logiciels permettant de suivre un appareil mobile à distance (géolocalisation), de réaliser à distance des opérations de protection des données, voire de supprimer le contenu de l'appareil (*wipe*). En particulier, les périphériques mobiles synchronisés avec la boîte aux lettres Exchange de l'Université sont en principe visibles depuis l'application Outlook Web App (https://mail.unifr.ch)[2] et, le cas échéant, peuvent faire l'objet d'un *wipe* à distance. Par contre, Outlook Web App n'offre pas de fonction de géolocalisation. L'utilisation de tels logiciels permet dans le meilleur des cas de donner des informations utiles à la police pour retrouver l'appareil perdu et dans le pire des cas d'éviter que les données ne soient exploitées à mauvais escient. Cependant, l'exploitation d'un tel logiciel dans le cadre professionnel soulève des questions liées à la protection de la sphère privée et, pour un parc IT de la taille de celui de l'Université, demande des ressources que la DIT n'a pas. Dès lors, la DIT n'offre aucun support pour ce type de logiciel (à part Outlook Web App) et ne peut que suggérer son installation et son utilisation à titre privé.

Dans le cas des *smartphones* et autres téléphones cellulaires, il faut toujours conserver le numéro d'identification IMEI dans un endroit sûr afin de faciliter la procédure de blocage de l'appareil auprès de l'opérateur téléphonique concerné.

3 Procédure à suivre en cas de vol ou de perte de matériel IT

Dans le cas malheureux où un appareil IT utilisé dans le cadre de l'Université devait être perdu ou volé malgré les recommandations décrites précédemment (chapitre 2), la Figure 1 (page 5) et l'annexe A (page 8) résument la procédure générale à suivre.

L'utilisateur doit commencer par établir l'inventaire de tout ce qui lui a été volé ou perdu. Non seulement son matériel IT privé ou de l'Université (ordinateur, tablette, smartphone), mais également ses objets personnels, tels que cartes bancaires et de crédit, cartes d'identité, abonnements, objets de valeur, etc., puis déclarer sans délai le vol dans sa globalité à la police.

Le vol ou la perte de matériel IT utilisé dans le cadre professionnel doit être annoncé sans délai au service Administration et Finances de la DIT (DIT-AF ; +41 26 300 72 02 ou dit@unifr.ch). Le service DIT-AF commence par demander à l'utilisateur si d'autres utilisateurs de l'Université se sont connectés avec leur nom d'utilisateur ou ont utilisé la machine volée par le passé. Toute connexion laisse une trace numérique sur la machine (mots de passe en cache, cookies, etc.), qui peut être exploitée à mauvais escient. Dès lors, il est important de prendre les mesures appropriées, non seulement envers

[1] Un verrouillage par mot de passe complexe, recommandé pour des appareils IT avec claviers, n'est pas forcément réaliste sur un *smartphone*.
[2] Après connexion dans Outlook Web Apps, choisir **Paramètres > Options > Téléphones**.

l'utilisateur principal de la machine volée, mais aussi envers les autres utilisateurs ayant utilisé cette machine.

Une fois cette liste obtenue, le DIT-AF transmet le cas au responsable de la sécurité informatique (RSI[3]), lequel vérifie auprès de l'utilisateur si des données personnelles au sens de la loi se trouvaient sur la machine au moment du vol. Si tel est le cas, l'information est transmise à la préposée à la protection des données de l'Université. Le RSI en informe la DIT.

Le service DIT-AF va ensuite vérifier si le matériel IT volé fait partie de l'inventaire de la DIT. Si oui, il démarre la procédure de traitement de vol de matériel de l'Université (voir chapitre 3.1). Si non, il démarre la procédure de traitement de vol de matériel privé (voir chapitre 3.2).

En cas de vol d'effets personnels, l'utilisateur ne doit pas oublier d'informer les organes compétents (par exemple, institutions financières pour bloquer les cartes bancaires et de crédit, autorités en cas de vol de cartes d'identité, etc.). L'utilisateur doit également informer toutes les personnes, de l'Université ou non, qui auraient pu utiliser la machine volée avec des données privées (par exemple, achat sur Internet avec paiement par carte de crédit). Enfin, le service DIT-AF informe également l'utilisateur de l'importance de changer tous les mots de passe de ses comptes privés (par exemple, Google, LinkedIn, Facebook, etc.).

3.1 Traitement d'un vol de matériel IT de l'Université

La Figure 2 (page 6) présente la procédure à suivre en cas de vol de matériel IT faisant partie du parc IT de l'Université.

Sitôt après réception de la liste des utilisateurs concernés, le service Administration et Finances de la DIT (DIT-AF) démarre la procédure de traitement du vol, laquelle implique quatre services de la DIT :

- ☐ le DIT-AF annonce le vol à la compagnie d'assurance avec laquelle travaille l'Université et suit le traitement du cas, puis établit l'inventaire des licences logicielles de l'Université qui étaient activées sur la machine volée. A la fin du processus, le DIT-AF met à jour l'inventaire de la DIT (mutation de la machine volée et saisie de la machine de remplacement) ;
- ☐ sur la base des informations reçues du DIT-AF, le service des Moyens informatiques de la DIT (DIT-MI) prépare une machine de remplacement pour l'utilisateur, selon la procédure d'installation standard ;
- ☐ sur la base des informations reçues du DIT-AF, le service Serveurs et Stockage de la DIT (DIT-SR) bloque temporairement le compte non seulement de l'utilisateur principal de la machine, mais aussi de chaque utilisateur s'étant servi de cette machine, afin que ces comptes ne puissent pas être utilisés à mauvais escient par la personne ayant volé la machine. Le-s compte-s sont réactivé-s dès que le-s utilisateur-s ont changé leur mot de passe. Le Support Center de la DIT (DIT-SC) et micromus se tiennent à disposition des employés, respectivement des étudiants, pour les aider dans cette procédure. Le cas échéant, la machine volée est également sortie du domaine UNIFR ;
- ☐ sur la base des informations reçues du DIT-AF, le service Télécom de la DIT (DIT-TE) active une alarme sur la *MAC address* WiFi de la machine volée. Si d'aventure la machine est détectée et/ou localisée par ce biais, la sous-procédure d'annonce appropriée est activée (voir chapitre 3.3) ;
- ☐ sur la base de la modification d'état de la machine dans l'inventaire, le DIT-TE sort la machine du réseau câblé de l'Université ;

[3] http://www.unifr.ch/dit/fr/about/security

- ☐ si l'utilisateur avait sur la machine volée un générateur logiciel à codes secrets (de type RSA) délivré par la DIT (en principe le DIT-TE), le DIT-TE annule les autorisations d'accès.

Ce n'est qu'une fois toutes ces tâches réalisées que le DIT-MI peut livrer la machine de remplacement à l'utilisateur, puis fermer le cas.

3.2 Traitement d'un vol de matériel IT privé

La Figure 3 (page 7) présente la procédure à suivre en cas de vol de matériel IT privé, mais utilisé dans le cadre de l'Université.

L'utilisateur ne doit pas oublier d'annoncer le vol à sa compagnie d'assurance privée. Ensuite, le service Administration et Finances de la DIT (DIT-AF) démarre la procédure de traitement du vol, laquelle implique deux services de la DIT :

- ☐ le DIT-AF commence par établir l'inventaire des licences logicielles de l'Université qui étaient activées sur la machine volée ;
- ☐ sur la base des informations reçues du DIT-AF, le service Serveurs et Stockage de la DIT (DIT-SR) bloque temporairement le compte non seulement de l'utilisateur principal de la machine, mais aussi de chaque utilisateur s'étant servi de cette machine, afin que ces comptes ne puissent pas être utilisés à mauvais escient par la personne ayant volé la machine. Le-s compte-s sont réactivés-s dès que le-s utilisateur-s ont changé leur mot de passe. Le Support Center de la DIT (DIT-SC) et micromus se tiennent à disposition des employés, respectivement des étudiants, pour les aider dans cette procédure ;
- ☐ si l'utilisateur est en mesure de communiquer la *Mac address* WiFi de la machine volée, le service Télécom de la DIT (DIT-TE) active une alarme sur cette *MAC address*. Si d'aventure la machine est détectée et/ou localisée par ce biais, la sous-procédure d'annonce appropriée est activée (voir chapitre 3.3) ;
- ☐ si l'utilisateur avait sur la machine volée un générateur logiciel à codes secrets (de type RSA) délivré par la DIT (en principe le DIT-TE), le DIT-TE annule les autorisations d'accès.

Ce n'est qu'une fois ces tâches réalisées que le DIT-AF ferme le cas.

3.3 Procédure en cas de localisation d'une machine volée

Si une machine volée faisant partie de l'inventaire se reconnecte sur le réseau WiFi de l'Université après que le DIT-TE ait activé un filtre sur la *MAC address* WiFi (voir chapitre 3.1), une alarme sera automatiquement générée auprès du service DIT-TE. Dans ce cas de figure, le DIT-TE contacte la préposée à la protection des données de l'Université pour l'informer que la machine a été détectée/localisée et lui transmet les informations à sa disposition.

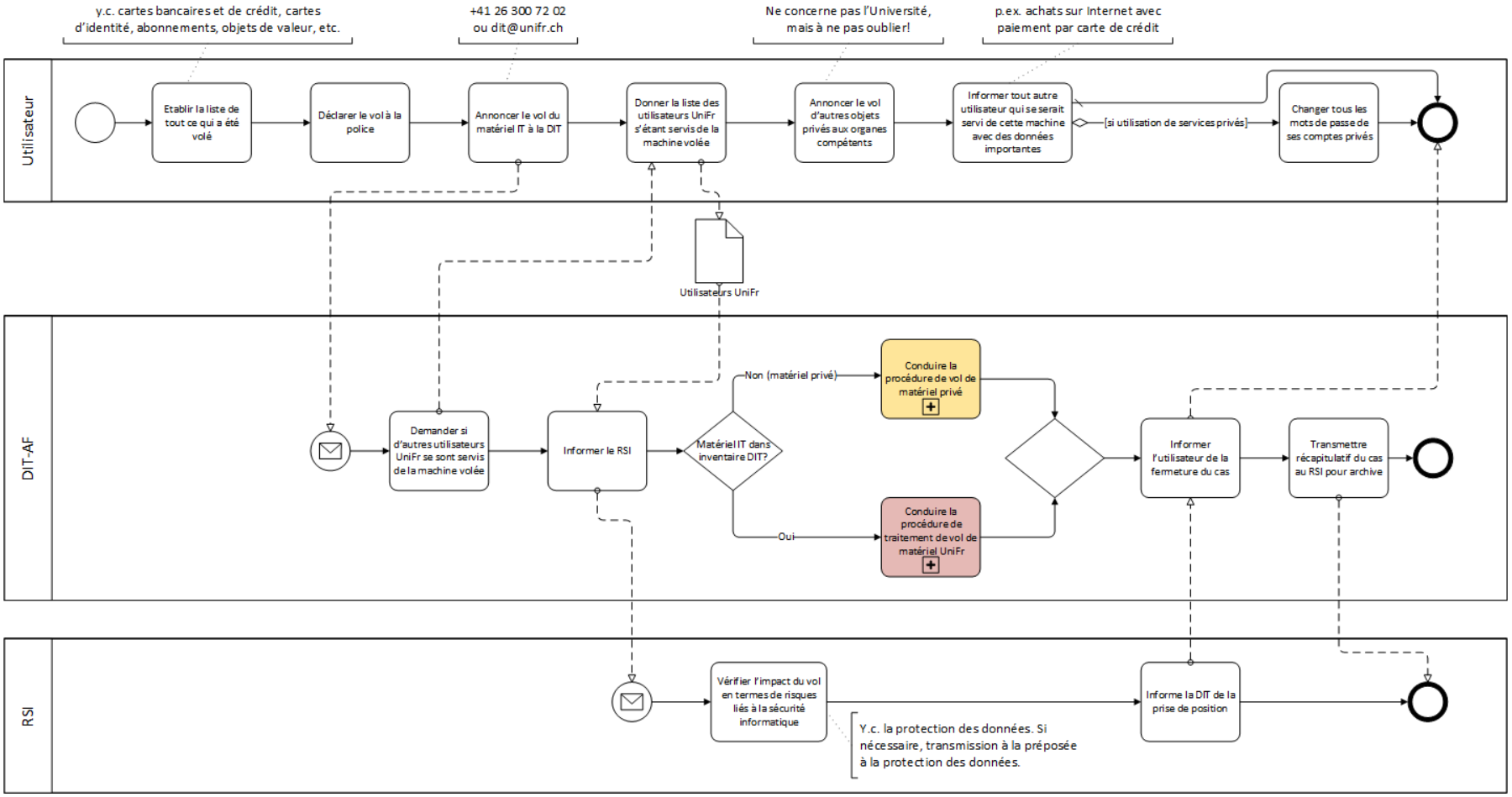

Figure 1. Procédure générale à suivre en cas de vol ou de perte de matériel IT

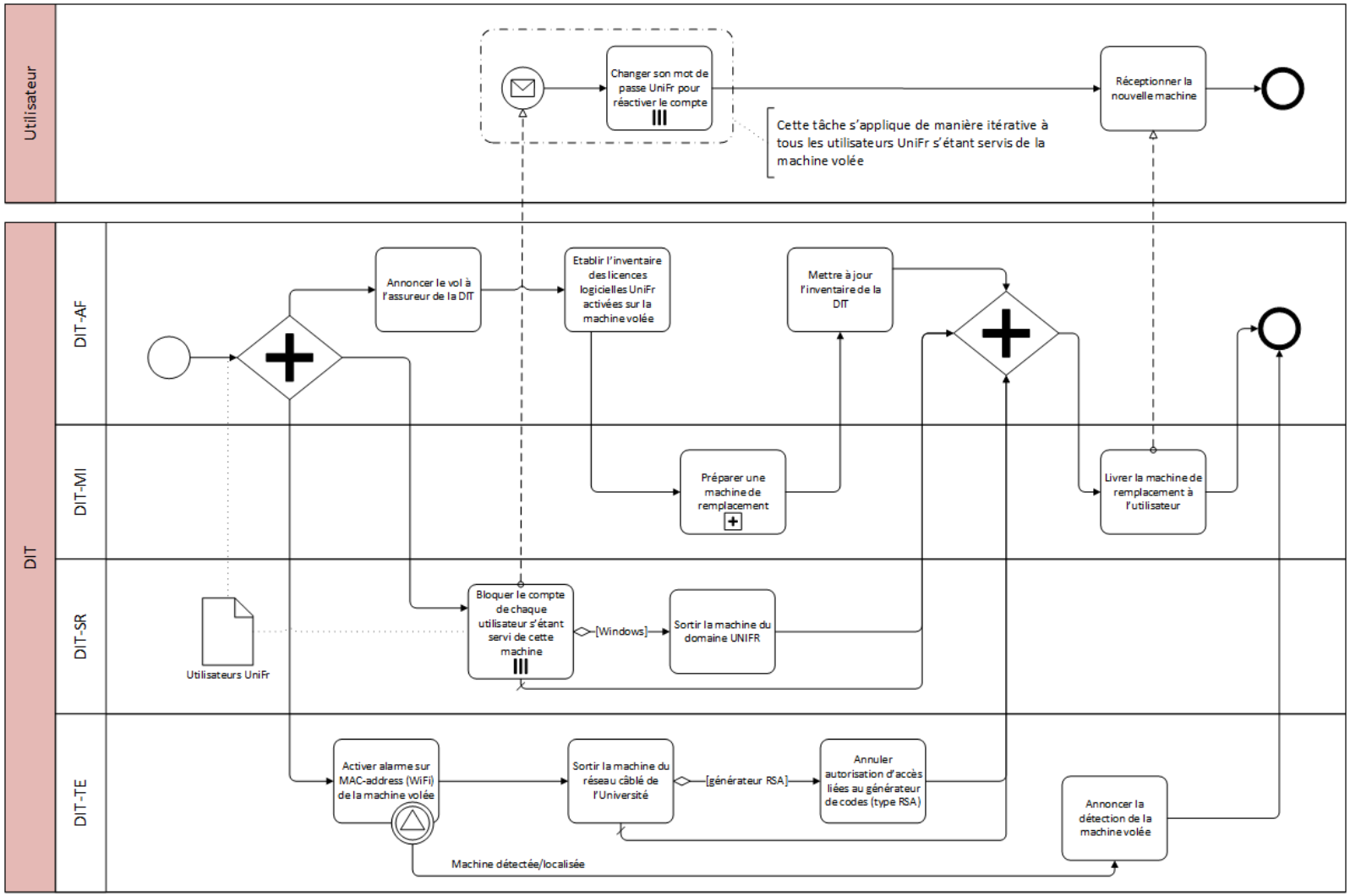

Figure 2. Procédure de traitement d'un vol de matériel IT faisant partie du parc de l'Université

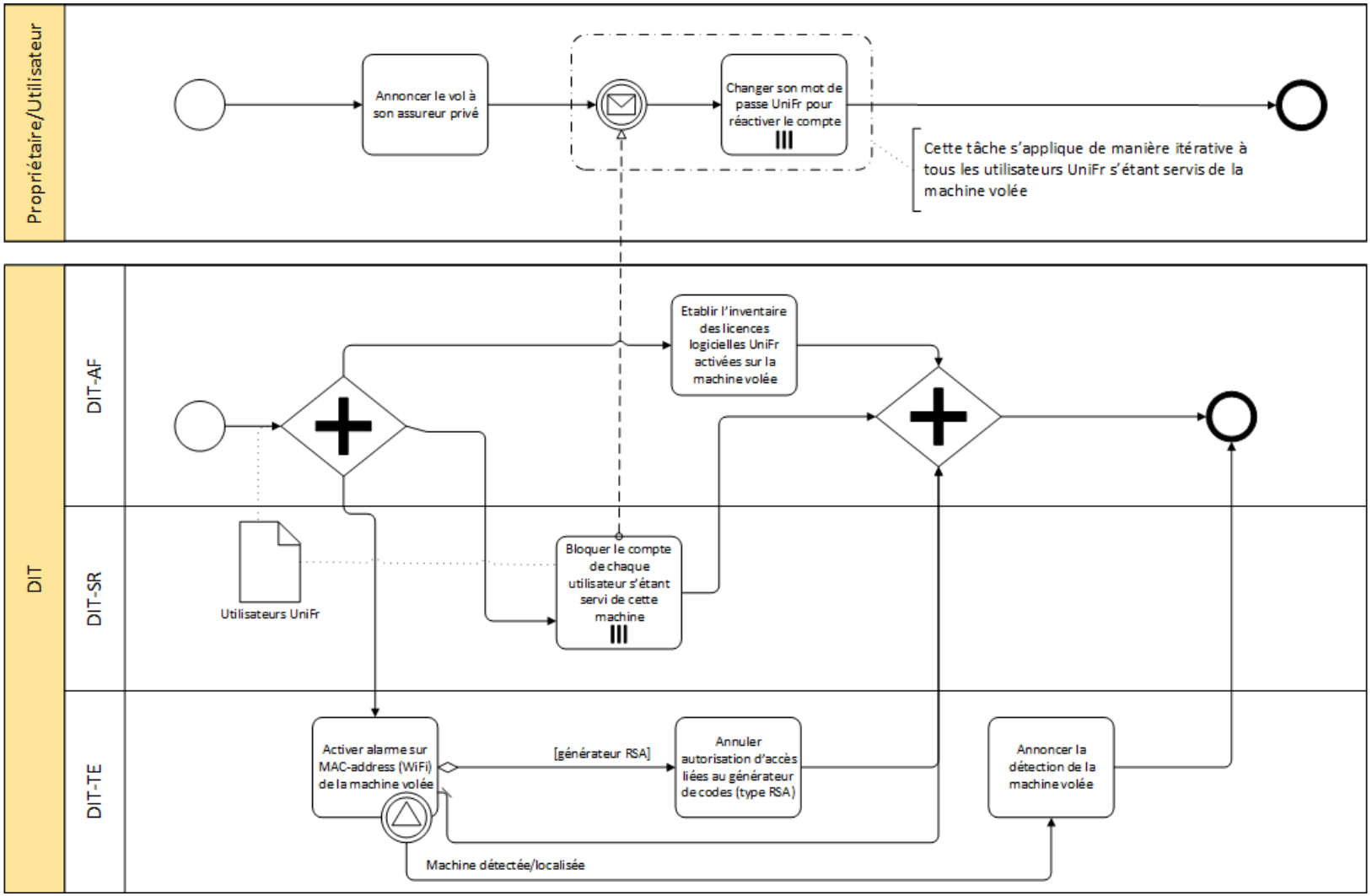

Figure 3. Procédure de traitement d'un vol de matériel IT privé, mais utilisé dans le cadre de l'Université

Annexe A. Checklist récapitulative pour l'utilisateur

La liste suivante résume de manière sommaire les actions qu'un utilisateur dont la machine a été volée ou perdue doit entreprendre.

- ☐ Etablir l'inventaire de tout ce qui a été volé ou perdu (matériel IT privé ou de l'Université, objets personnels, cartes bancaires et de crédit, cartes d'identité, abonnements, objets de valeur, etc.).
- ☐ Déclarer le vol dans sa globalité à la police.
- ☐ Annoncer le vol du matériel IT (privé ou de l'Université) à la DIT (DIT-AF ; +41 26 300 72 02 ou dit@unifr.ch), y.c. liste des utilisateurs de l'Université s'étant servis de la machine volée.
- ☐ En cas de vol de matériel personnel, annoncer le vol aux organes compétents (assurances privées, etc.).
- ☐ Sur demande de la DIT, changer son mot de passe de l'Université afin de réactiver le compte personnel qui aura préventivement été bloqué.
- ☐ Informer tout autre utilisateur qui se serait servi du matériel volé en y utilisant des données importantes (p.ex. achats sur Internet avec paiement par carte de crédit).
- ☐ Changer tous les mots de passe de ses comptes privés.