UNIVERSITÉ DE FRIBOURG
UNIVERSITÄT FREIBURG

Mandat attribué à une entreprise externe

Directive DIT-17 Champ d'application : Université

1 Buts

Le but de cette directive est de rendre les entreprises externes attentives à la législation à laquelle l'Université de Fribourg est soumise et aux règles qui doivent être respectées en matière d'infrastructure informatique. Le but principal est de sensibiliser aux éventuels problèmes et non de gêner le travail des deux parties.

Cette directive constitue une convention entre l'Université de Fribourg et une entreprise externe dans le cadre de travaux impliquant l'infrastructure informatique. Celle-ci doit figurer en annexe à toutes commandes de travaux à des firmes externes.

2 Abréviation

DIT Direction des services IT de l'Université de Fribourg

3 Bases légales

Vu:

- l'article 3 de la loi du 19 novembre 1997 (état au 10 septembre 2015) sur l'Université,
- l'article 18 al. 2 de la loi cantonale du 25 novembre 1994 sur la protection des données (LPrD),
- le règlement du 29 juin 1999 sur la sécurité des données personnelles (RSD),

l'université de Fribourg (ci-après, « l'Université »), par l'intermédiaire de l'unité organisationnelle (UO) concernée, doit établir une convention (présente directive) avec toute entreprise extérieure à l'Université (ci-après, « l'entreprise ») effectuant des travaux permettant un accès direct ou indirect à des ressources informatiques de l'Université, et entre autres à ses machines (serveurs, machines de bureau, machines réseau, etc.) ou à ses données (fichiers, bases de données, etc.).

Version	Date	Remplace	Auteur(s)	Commentaires
1.0	24.6.2003	-	B. Vuillemin/ J.-F. Descloux	
2.0	26.2.2014	1.0	B. Vuillemin/ A. Gachet	Actualisation et validation par comité de direction IT ; intégration commentaires GSI ; validation GSI
2.1	5.3.2015	2.0	B. Vuillemin/ A. Gachet	Ajout de la version allemande de la directive
2.2	11.11.2016	2.1	B. Vuillemin/ A. Gachet	Ajout de la signature DIT à l'annexe 1.
2.3	21.8.2019	2.2	A. Gachet	Ajout du nom de l'entreprise à l'annexe 1 ; corrections mineures d'ordre formel

4 Règles de conduite

Selon l'activité de l'entreprise, certaines règles de la présente directive ne sont pas applicables. Dans ce cas, elles seront biffées d'un commun accord. Néanmoins, les éléments figurant aux points 4.1, 4.2, 4.3 et 4.9 s'appliquent dans tous les cas et ne sauraient faire l'objet d'amendements.

4.1 Généralités

Les collaborateurs de l'entreprise s'engagent à respecter les règles d'utilisation de l'informatique applicables à tous les utilisateurs de l'Université.

Les collaborateurs de l'entreprise seront annoncés nominativement à la DIT[1]. L'Université se réserve le droit de supprimer les droits d'accès de tout collaborateur de l'entreprise, à tout moment.

L'Université doit permettre aux collaborateurs de l'entreprise de travailler dans des conditions adéquates pour réaliser leurs tâches, durant l'intégralité de la période d'autorisation.

Si le collaborateur de l'entreprise fait une fausse manipulation quelle qu'elle soit (débrancher un câble électrique, détruire un fichier, etc.), il doit la signaler à un collaborateur de la DIT sans délai.

Si le collaborateur de l'entreprise remarque quelque chose qu'il juge anormal, il doit prévenir un collaborateur de la DIT sans délai.

4.2 Sécurité informatique

Le travail de l'entreprise doit respecter en tout temps la sécurité informatique mise en place par l'Université.

Il est du ressort de l'entreprise de s'en assurer, notamment en se renseignant auprès de la DIT.

4.3 Protection des données

Dans le cadre de son travail, le collaborateur de l'entreprise pourra être amené à accéder à des données de types *personnelles* ou *sensibles* de *degré de confidentialité* 1 (accessible au public), 2 (à usage interne) ou 3 (confidentiel ou secret) au sens de la réglementation fribourgeoise sur la protection des données.

Au-delà des dispositions cantonales en matière de protection des données, le Rectorat a émis ses propres règles de fonctionnement en limitant l'extraction de listes de personnes à un résultat de 10 noms au maximum.

De plus, le simple fait de rechercher un nom d'étudiant est soumis à une autorisation écrite. En ce sens, le fichier des étudiants n'est pas accessible, sauf autorisation écrite du Rectorat sur la base d'une demande motivée.

Il est de la responsabilité de l'entreprise de sensibiliser ses collaborateurs. La DIT peut fournir de la documentation à ce sujet.

[1] Dans les cas où l'entreprise peut justifier que la livraison à la DIT d'une liste nominative *ex ante* relève d'une procédure inutilement lourde et complexe, elle doit au minimum s'engager à pouvoir livrer, si la DIT en fait la requête, une liste *ex post*. *In fine*, la DIT est seule habilitée à décider si une livraison *ex ante* est requise ou non.

4.4 Accès physique aux machines et aux locaux de la DIT

Le collaborateur de l'entreprise doit être accompagné par un collaborateur de la DIT ou de l'unité organisationnelle mandant la prestation pour accéder aux locaux de la DIT (dont les salles machines, répartiteurs, etc.).

Demeure réservée la possibilité pour la DIT d'autoriser une dérogation à ce principe, dans des cas exceptionnels. Le chef du service de la DIT ou de l'unité organisationnelle mandant la prestation[2] peut donner à un collaborateur de l'entreprise une autorisation écrite, limitée dans le temps, nominative[3], précisant les lieux autorisés. Le collaborateur de l'entreprise montrera cette autorisation à tout collaborateur de l'Université qui lui en fera la requête. Une pièce d'identité officielle avec photo (carte d'identité, permis de conduire) pourra être exigée.

Dans tous les cas, il est obligatoire de respecter les règles d'accès éventuellement affichées sur certaines portes de locaux informatiques, ou à leur proximité immédiate et évidente.

Le directeur de la DIT (ou toute autorité supérieure), les chefs des services de la DIT ou le responsable de la sécurité informatique, peuvent exiger de tout collaborateur de l'entreprise de quitter les lieux sans délai. L'entreprise ne pourra exiger que son collaborateur soit à nouveau autorisé à poursuivre sa mission pour l'Université.

4.5 Accès logique aux machines

Les collaborateurs de l'entreprise, qu'ils soient dans les locaux de l'Université ou à distance, ne pourront se connecter que sous leurs propres noms d'utilisateur. Ces noms d'utilisateur seront attribués par la DIT, pour un temps limité.

L'Université aura accès aux différents logs et notamment ceux relevant les connexions (*login/logout*) des utilisateurs. Les machines devront être configurées pour enregistrer ces logs. Cela est de la responsabilité de l'administrateur de la machine.

Toute communication à un tiers d'un nom d'utilisateur ou d'un mot de passe est interdite et engage la responsabilité du possesseur du compte. Pour les cas exceptionnels, une autorisation de la DIT est indispensable.

Sur toutes les machines de type serveur, un accès administratif anonyme est interdit.

4.6 Transferts de données, réparations externes

L'entreprise n'est pas autorisée à exporter des données de l'Université vers sa propre infrastructure.

Demeure réservée, sur la base d'une convention additionnelle et en fonction de certains besoins spécifiques, la possibilité d'obtenir une autorisation du responsable de la sécurité informatique[4] pour une telle exportation, pour une durée limitée et prédéfinie. Dans ce cas, seront indiquées, selon le mode de transfert utilisé (réseau ou support physique) les dispositions de cryptage imposées. Le transfert sans cryptage est interdit (protocoles réseau, disques, CD/DVD, clés USB, etc.). A la fin de la période autorisée, l'entreprise fournira la déclaration de destruction des données selon les modalités de

[2] Un chef d'un service de la DIT ou d'une unité organisationnelle peut déléguer cette compétence à un de ses collaborateurs directs. Dans tous les cas, le signataire d'une autorisation porte la responsabilité de son contenu.
[3] Dans les cas où l'établissement d'autorisations nominatives relève d'une procédure jugée par la DIT inutilement lourde et complexe, le chef du service de la DIT ou de l'unité organisationnelle mandant la prestation peut délivrer une autorisation globale strictement limitée au périmètre du mandat attribué à l'entreprise.
[4] En cas d'absence de ce dernier, les règles de suppléance en vigueur s'appliquent.

l'annexe 2. Cela s'applique aux transferts entre l'Université et l'entreprise, mais aussi entre l'entreprise et ses éventuels sous-traitants (voir aussi chapitre 4.8).

De plus, il est de la responsabilité de l'entreprise de s'assurer que les moyens de transfert de données (réseau, disques, CD/DVD, clés USB, etc.) ne seront pas utilisés par un de ses collaborateurs pour exporter des données en contradiction avec la protection des données telle qu'édictée par l'Université.

En outre, il est de la responsabilité de l'entreprise de s'assurer qu'elle n'introduira pas de virus, de chevaux de Troie ou n'importe quel logiciel abaissant le niveau de sécurité de l'informatique de l'Université. Un anti-virus même à jour n'est pas un élément de sécurité jugé suffisant. Une information sur les moyens de protection des machines (faisant des transferts de données avec l'Université par réseau, disques, CD/DVD, clés USB, etc.) de l'entreprise extérieure doit pouvoir être fournie.

4.7 Pose de câbles informatiques dans ou au profit de l'Université

Dans le cas de mandants impliquant la pose de câbles informatiques dans ou au profit de l'Université, il faut de plus se conformer aux consignes du service télécommunication de la DIT (DIT-TE), ainsi qu'à celles des organes (instituts, services, etc.) où se déroulent les travaux.

4.8 Sous-traitance

Si l'entreprise sous-traite ou collabore avec une organisation tierce (entreprise, organisme public, etc.) qui sera amenée à traiter des données de l'Université, l'entreprise organisant la sous-traitance transmettra la présente directive aux organisations liées, collectera leurs déclarations et les adjoindra à la sienne.

4.9 Non-respect des règles, interruption du contrat

Le non-respect d'une ou plusieurs de ces règles sera étudié avec attention par l'Université et toutes les suites appropriées seront envisagées, y compris des prétentions en dommages et intérêts. Le contrat pourra être interrompu par l'Université, notamment en cas de faute grave. Dans tous les cas, l'entreprise devra fournir toute la documentation sur le travail déjà effectué. Cette documentation devra être à jour et de qualité jugée acceptable par la DIT.

5 Application

La version 2 de cette directive a été approuvée par le Groupe de Sécurité Informatique lors de la séance du 5 mars 2015 (remplace version 1 du 24 juin 2003) et entre en vigueur immédiatement.

Annexe 1. Formulaire d'acceptation de la directive DIT-17 de l'université de Fribourg

Principe

L'entreprise soussignée[5] déclare avoir lu la directive DIT-17 de l'université de Fribourg et s'engage à en respecter le contenu. Elle devra, sur demande de l'université de Fribourg, fournir les informations suivantes :

- date, heure, durée des accès physiques ou logiques (depuis la date de signature du contrat ou, pour les contrats de longue durée, au maximum durant les 6 mois précédents la demande) ;
- motifs des accès ;
- noms des collaborateurs et collaboratrices concerné-e-s ;
- machines et locaux accédés ;
- données personnelles accédées (fichiers, bases de données).

Validité

Ce document, signé par le représentant légal de l'entreprise externe, est à retourner au responsable du mandat au sein de l'université de Fribourg, qui le contresignera puis en transmettra l'original au secrétariat de la DIT, à l'adresse suivante : Université de Fribourg, Direction des services IT, Bd de Pérolles 90, 1700 Fribourg.

Pour l'université de Fribourg	Pour l'entreprise externe
	Nom de l'entreprise :_____
Responsable du mandat	Représentant légal
Nom :_____	Nom :_____
Fonction :_____	Fonction :_____
Date :_____	Date :_____
Signature :_____	Signature :_____

Le formulaire d'acceptation de la directive DIT-17 ne sera considéré comme valide que s'il comporte la signature du directeur des services IT ou la personne désignée par lui :

Direction des services IT	
Nom :_____	Date :_____
Fonction :_____	Signature :_____

Muni des trois signatures ci-dessus, ce document est valable pour la durée du mandat, à partir de la date de signature par le responsable des services IT.

La DIT se charge d'établir trois exemplaires de la présente convention, un pour la firme mandatée, un pour le responsable du mandat, et un pour la DIT (Direction des services IT de l'Université de Fribourg).

[5] Dans les cas exceptionnels où une autorisation doit être délivrée rapidement et où le présent formulaire ne peut pas être signé dans l'immédiat par un représentant légal de l'entreprise, le formulaire peut être rempli par le signataire à titre personnel. La durée de validité d'une autorisation personnelle est d'un mois. L'établissement d'une autorisation temporaire à titre personnel ne décharge pas l'entreprise de remplir le formulaire au nom de la société.

Annexe 2. Annonce de destruction des données

L'entreprise enverra une lettre (voir modèle ci-dessous) au responsable du mandat au sein de l'université de Fribourg, qui en fera une copie pour ses dossiers (et la fournira au maître des données sur demande) et transmettra l'original au secrétariat de la DIT.

Modèle de base de l'annonce de destruction des données. La lettre doit être signée par un représentant légal.

Concerne : Annonce de destruction de données appartenant à l'université de Fribourg

Madame, Monsieur,

Dans le cadre du mandat …… nous vous informons par la présente que nous avons détruit les données appartenant à l'université de Fribourg, utilisées du …… au …… .

Ces données ont été effacées de tous nos serveurs, ainsi que de toutes nos installations de tests.

Les sauvegardes de ces données ont également été détruites.

Les supports de transfert, tels que bandes, CD, DVD, ont été détruits.

[selon cas] Nous n'avons pas transmis ces données à des entreprises tierces (collaboration ou sous-traitance).

[selon cas] L'entreprise ……, à qui nous avons sous-traité du travail, a elle aussi détruit toutes les données de l'université de Fribourg, comme l'atteste sa déclaration en annexe [l'entreprise sous-traitante utilisera le même modèle de lettre].

<Signature par un représentant légal de l'entreprise>