

Mandate – Externe Firmen betreffend

Richtlinie DIT-17

Geltungsbereich : Universität

1 Ziele

Das Ziel dieser Richtlinie ist es, externe Firmen darauf hinzuweisen, welche Gesetze die Universität betreffend zu berücksichtigen sind sowie welche Regeln hinsichtlich der IT-Infrastruktur zu befolgen sind. Hiermit soll die Sensibilisierung bezüglich gewisser Probleme erreicht werden, um eine reibungslose Projektarbeit sicher zu stellen.

Diese Richtlinie ist Grundlage für Vereinbarungen zwischen der Universität Freiburg und einer externen Firma für Arbeiten welche die IT-Infrastruktur betreffen. Diese Richtlinie muss allen Bestellungen an externe Firmen angehängt werden.

2 Abkürzungen

DIT Direktion der IT-Dienste

3 Gesetzliche Grundlagen

Gestützt auf:

- Artikel 3 des Gesetzes vom 19. November 1997 über die Universität,
- Artikel 18 Absatz 2 des Gesetzes vom 25. November 1994 über den Datenschutz (DSchG),
- das Reglement vom 29. Juni 1999 über die Sicherheit der Personendaten (DSR),

schliesst die Universität Freiburg (nachfolgend „die Universität“), respektive die betroffene Organisationseinheit (UO) der Universität, eine Vereinbarung (vorliegende Richtlinie) mit jeder externen Firma (nachfolgend „Firma“) welche Arbeiten ausführt, die einen direkten oder indirekten Zugang zu den IT-Ressourcen erlaubt, unter anderem zu IT-Geräten (Servern, PC Bürosysteme, Netzwerkgeräten, etc.) oder an Daten (Dateien, Datenbanken, 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	Aktualisierung und Validierung durch die DIT-GL; Integration Kommentare GSI; Validierung GSI
2.1	5.3.2015	2.0	B. Vuillemin/ A. Gachet	Deutsche Version hinzugefügt
2.2	11.11.2016	2.1	B. Vuillemin/ A. Gachet	Unterschrift der DIT im Anhang 1 hinzugefügt.
2.3	21.8.2019	2.2	A. Gachet	Name der Firma im Anhang 1 hinzugefügt.

4 Verhaltensregeln

Je nach Aufgaben, die eine Firma zu erfüllen hat, sind gewisse Regeln dieser Richtlinie nicht anwendbar. In diesem Falle werden diese in gemeinsamer Absprache gestrichen. Unabhängig davon finden die unter den Punkten 4.1, 4.2, 4.3 und 4.9 angeführten Inhalte in jedem Falle Anwendung und können nicht Teil von Änderungsanträgen sein.

4.1 Allgemein

Die Mitarbeitenden der Firma verpflichten sich, die Richtlinien zur Benutzung der Informatik, wie sie für alle IT-Nutzer der Universität gelten, zu befolgen.

Die Mitarbeitenden der Firma werden der DIT namentlich genannt¹. Die Universität behält sich das Recht vor, die Zugangsrechte der Mitarbeitenden von Firmen jederzeit aufzuheben.

Die Universität gewährleistet den Mitarbeitenden von Firmen die notwendigen Voraussetzungen, um die Arbeiten bestmöglich durchführen zu können. Die Gewährleistung gilt während der gesamten bewilligten Periode.

Im Falle von Fehlmanipulationen (wie Ausstecken eines elektrischen Kabels, Löschen einer Datei, etc.) durch Mitarbeitende der Firma, müssen diese dies unverzüglich der DIT melden.

Wenn Mitarbeitende der Firma etwas bemerken, was sie als aussergewöhnlich beurteilen, müssen sie dies unverzüglich einem DIT-Mitarbeitenden mitteilen.

4.2 Informatiksicherheit

Die Arbeiten der Firma müssen jederzeit die Richtlinien der Universität zur Informatiksicherheit erfüllen, wie sie für alle IT-Nutzer der Universität gelten.

Es obliegt der Firma, die hierzu nötigen Informationen bei der DIT einzuholen.

4.3 Datenschutz

Im Rahmen der Arbeiten kann es vorkommen, dass Mitarbeitende der Firma auf Daten zugreifen müssen, welche als persönlich oder besonders schützenswerte Personendaten der Vertraulichkeitsstufe 1 (öffentlich zugänglich), 2 (für internen Gebrauch) oder 3 (vertraulich oder geheim) im Sinne der Freiburger Gesetzgebung (Gesetz und Erlasse) über den Datenschutz gelten.

Zusätzlich zu der Kantonalen Datenschutzverordnung hat das Rektorat eine eigene, den internen Ablauf betreffende Verordnung erlassen. Sie beschränkt die Auszüge von Personenlisten auf ein Maximum von 10.

Im Weiteren unterliegt die Suche nach einem Studierendenname einer schriftlichen Erlaubnis. In diesem Sinne ist die Datenbank der Studierenden nicht zugänglich, es sei denn mit einer schriftlichen Erlaubnis durch das Rektorat aufgrund einer begründeten Anfrage.

Es liegt in der Verantwortung der Firma deren Mitarbeitende zu sensibilisieren. Die DIT stellt die diesbezügliche Dokumentation bereit.

¹ Für den Fall wo die Firma belegen kann, dass die Lieferung einer nominativen Liste *ex ante* an die DIT, zu aufwändig und komplex ist, muss sie sich jedoch für die Lieferung einer Liste *ex post* verpflichten, falls dies die DIT verlangt. *In fine*, ist die DIT einzig und allein befugt zu entscheiden, ob eine Liste *ex ante* notwendig ist oder nicht.

4.4 Physischer Zugang zu den Maschinen und den Räumen der DIT

Der Mitarbeitende der Firma muss durch einen Mitarbeitenden der DIT oder durch die mandatierende Organisationseinheit begleitet werden, um Zugang in die Lokalitäten der DIT zu erhalten (IT-Datencenter, Verteilerräumen, etc.).

In Ausnahmefällen bleibt der DIT vorbehalten, von diesem Prinzip abweichende Regelungen zu erlauben. Der Chef eines Dienstes der DIT oder der Organisationseinheit welche das Mandat für die Leistung² vergibt, kann einem Mitarbeitenden der Firma eine schriftliche, zeitlich limitierte, namentliche³, Genehmigung mit der Auflistung der zugänglichen Lokale erteilen. Der Mitarbeitende der Firma zeigt diese Bewilligung jedem Mitarbeitenden der DIT, welcher dies verlangt. Ein offizieller Ausweis mit Foto (Identitätskarte, Fahrausweis) kann ebenfalls verlangt werden.

Es ist in jedem Falle obligatorisch, allfällige, auf den Türen oder in deren Bereich ersichtliche, angebrachte Beschriftungen mit Zugangsberechtigungen zu respektieren.

Der Direktor der DIT (oder jede höher gestellte Instanz), die Chefs der Dienste der DIT oder der Verantwortliche für IT-Sicherheit können von allen Mitarbeitenden der Firma das sofortige Verlassen der Lokale verlangen. Die Firma kann für den betroffenen Mitarbeitenden keine erneute Bewilligung zum Fortsetzen der Arbeiten für die Universität erwirken.

4.5 Nicht physischer Zugang zu den Maschinen

Die Mitarbeitenden der Firma, ob diese in den Räumen der Universität sind, oder aber per Fernzugriff auf das Netzwerk zugreifen, können sich ausschliesslich mit ihrem von der DIT zugewiesenem Benutzernamen verbinden. Diese Benutzernamen werden von der DIT für einen beschränkten Zeitraum vergeben.

Die Universität hat Zugriff auf die verschiedenen Logs und im Speziellen auf diese welche die Verbindungen (*login/logout*) der Benutzer aufzeigen. Die Geräte müssen so konfiguriert sein, dass diese Logs gespeichert werden. Dies ist im Verantwortungsbereich vom Administrator der Maschine.

Jegliche Weitergabe des Benutzernamens und Passworts an Dritte ist untersagt. Der Kontoinhaber ist für allfällige Schäden verantwortlich. In Ausnahmefällen ist die Bewilligung der DIT unerlässlich.

Auf allen Geräten vom Typ Server ist ein anonymer Serverzugriff verboten.

4.6 Datentransfer und externe Reparaturen

Es ist der Firma untersagt, Daten auf ihre eigene Infrastruktur zu übertragen.

Jedoch besteht die Möglichkeit, aufgrund einer speziellen Vereinbarung und für spezielle Bedürfnisse, eine zeitliche und vordefinierte Bewilligung des Sicherheitsverantwortlichen⁴ für einen solchen Datentransfer zu erhalten. In diesem Falle wird, gemäss der Transferart (Netzwerk oder physischer Datenträger), die geforderte Verschlüsselung festgeschrieben. Der Transfer ohne Verschlüsselung ist verboten (Netzwerkprotokolle, Disks, CD/DVD, USB-Sticks, etc.). Am Ende der genehmigten Zeitspanne übergibt die Firma die Deklaration der Datenvernichtung gemäss den Modalitäten aus

² Ein Chef eines Dienstes der DIT oder einer Organisationseinheit kann diese Kompetenz an einen seiner direkten Mitarbeitenden delegieren. Der Unterzeichnende einer Bewilligung trägt in jedem Falle die Verantwortung über den Inhalt.

³ Falls die Erstellung nominativer Listen durch die DIT als zu aufwändig und komplex erachtet wird, können der Dienstchef der DIT oder der auftraggebenden Organisationseinheit eine generelle, strikt auf den Mandatsrahmen der Firma limitierte Erlaubnis erteilen.

⁴ Im Falle des Fehlens des Letzteren, treten Vertretungsregeln in Kraft.

Anhang 2. Dies gilt für die Transfers zwischen der Universität und der Firma an, aber auch zwischen der Firma und allfälligen Unterlieferanten (vgl. auch Kapitel 4.8).

Im Weiteren obliegt es der Verantwortung der Firma sich zu vergewissern, dass die Mittel für den Datentransfer (Netzwerk, Disks, CD/DVD, USB-Datenträger, etc.) nicht durch einen Mitarbeitenden verwendet werden, um entgegen den Universitätsrichtlinien zum Datenschutz Daten zu exportieren,

Zudem ist die Firma dafür verantwortlich die nötigen Massnahmen zu ergreifen, damit keine Viren, Trojaner und andere Schadsoftware welche die IT-Sicherheit der Universität vermindern würden, ins Universitätsnetz gelangen. Ein up to date gehaltenes Anti-virus Programm wird nicht als ein genügendes Sicherheitselement betrachtet. Die Firma muss eine Information bereitstellen können, über die Mittel zum Schutz der Maschinen (welche Datentransfer machen, mit der Universität über das Netzwerk, Disks, CD/DVD, USB-Datenträger, etc.).

4.7 Verlegung von IT-Netzwerken für die Universität

Im Falle von Mandaten welche die Verlegung von Datenkabel für die Universität zur Folge haben, müssen die Empfehlungen der Abteilung Telekom der DIT (DIT-TE) und weiterer Organe (Institute, Dienste, etc.), bei welchen die Arbeiten ausgeführt werden, befolgt werden.

4.8 Vergabe von Unteraufträgen

Falls die Firma die Arbeiten an Nachunternehmen weitergibt oder mit einer Drittfirma (Firma, öffentliche Körperschaft, etc.) zusammenarbeitet und Daten der Universität bearbeitet werden, muss die betreffende Firma die vorliegende Richtlinie an die ausführende Firma weitergeben, die nötigen Deklarationen zusammentragen und mit der eigenen einreichen.

4.9 Nichteinhalten der Regeln, Vertragsauflösung

Der Nichteinhalt einer oder mehrerer der obigen Regeln wird durch die Universität sorgfältig analysiert und es werden die nötigen Massnahmen getroffen. Hierzu zählen auch Schadensersatzforderungen. Der Vertrag kann durch die Universität aufgelöst werden, insbesondere bei einem schwerwiegenden Fehlverhalten. Die Firma muss auf jeden Fall die gesamte Dokumentation über bereits ausgeführte Arbeiten zur Verfügung stellen. Diese Dokumentation muss lückenlos, auf dem neusten Stand sowie in, durch die DIT beurteilten, ausreichender Qualität sein.

5 Anwendung

Die Version 2 dieser Richtlinie wurde durch die Gruppe für Informatiksicherheit in der Sitzung vom 5. März 2015 gutgeheissen (ersetzt die Version 1 vom 24 Juni 2003) und tritt per sofort in Kraft.

Anhang 1. Formular zur Annahme der Richtlinie DIT-17 der Universität Fribourg

Prinzip

Die unterzeichnende Firma⁵ erklärt hiermit die Richtlinie DIT-17 gelesen zu haben und verpflichtet sich den Inhalt zu respektieren. Auf Verlangen der Universität muss sie folgende Informationen zur Verfügung stellen:

- Datum, Zeit, Zeitdauer der physischen oder logischen Zugänge (seit der Vertragsunterzeichnung oder, für langfristige Verträge, maximal 6 Monate vor der Anfrage);
- Zugangsmotive;
- Namen der betroffenen Mitarbeiter und Mitarbeiterinnen;
- Maschinen und Lokalitäten der Zugänge;
- Zugang zu persönlichen Daten (Dateien, Datenbanken).

Gültigkeit

Dieses Dokument, vom Rechtsvertreter der externen Firma unterzeichnet, ist zum Verantwortlichen vom Mandat innerhalb der Universität Freiburg zurückzukehren. Er wird es gegenzeichnen und dann das Original an das Sekretariat des DIT weiterleiten, an folgende Adresse: Universität Freiburg, Direktion der IT-Dienste, Bd de Pérolles 90, 1700 Freiburg.

Für die Universität Freiburg

Für die externe Firma

Verantwortlicher vom Mandat

Rechtsvertreter

Name: _____

Name: _____

Funktion: _____

Funktion: _____

Datum: _____

Datum: _____

Unterschrift: _____

Unterschrift: _____

Das Formular der Richtlinie DIT-17 wird nur dann als gültig angesehen werden, wenn sie die Unterschrift des Direktors der IT-Services oder der von ihm designierten Person beinhaltet:

Direktion der IT Dienste

Name: _____

Datum: _____

Funktion: _____

Unterschrift: _____

Mit den drei oben genannten Unterschriften ist dieses Dokument für die Dauer des Mandats gültig, ab dem Zeitpunkt der Unterzeichnung durch den Leiter der IT Dienste.

Diese Vereinbarung wird in drei Exemplaren erstellt, eines für die mandatierte Firma, eines für den Verantwortlichen des Mandats, und eines für die DIT (IT-Direktion der Universität Freiburg).

⁵ In Ausnahmefällen, bei welchen die Bewilligung schnell erteilt werden muss und dieses Dokument nicht direkt durch einen Rechtsvertreter der Firma unterzeichnet werden kann, besteht die Möglichkeit dieses Dokument durch den Unterzeichnenden ausfüllen zu lassen. Die Gültigkeitsdauer einer persönlichen Bewilligung beträgt einen Monat. Das Ausstellen einer temporären, persönlichen Bewilligung entbindet die verantwortliche Firma nicht das Formular auf den Namen der Firma zu erstellen.

Anhang 2. Meldung über Datenvernichtung

Die Firma wird dem Mandatsverantwortlichen der Universität Freiburg einen Brief (vgl. nachfolgendes Beispiel hierzu) übermitteln welchen dieser für seine eigenen Dossiers kopiert (und übergibt diese, auf Anfrage dem Datenverantwortlichen) und das Original dem Sekretariat der DIT übermitteln wird.

Basismodell für eine Meldung zur Datenvernichtung. Dieser Brief muss durch einen Rechtsvertreter unterzeichnet sein.

Betrifft: Meldung über die Vernichtung von Daten welche der Universität Freiburg gehören

Sehr geehrte Damen und Herren,

Im Rahmen des Mandates informieren wir sie hiermit dass die vom bis zum verwendeten Daten welche der Universität Freiburg gehören vernichtet worden sind.

Diese Daten wurden von allen unseren Servern und Testinstallationen gelöscht.

Die Sicherungen dieser Daten wurden ebenfalls gelöscht.

Die Medien für den Datentransfer wie Magnetbänder, CD, DVD wurden ebenfalls vernichtet.

[je nach Fall] Wir haben diese Daten keinen Drittfirmen (Zusammenarbeit und Weitergabe von Aufträgen).

[je nach Fall] Die Firma , an welche wir die Aufträge Weitergegeben haben, hat ihrerseits alle Daten der Universität Freiburg vernichtet, wie sie dies in der beigefügten Deklaration bestätigt [Die ausführende Firma, von weitergegeben Aufträgen, verwendet die gleiche Briefvorlage].

< Unterschrift durch einen Rechtsvertreter der Firma >