

Rahmenbedingungen für den Zugang zum WiFi-Netzwerk mit der SSID "public-unifr"

Diese Rahmenbedingungen gelten als angenommen, sobald die Benutzerin oder der Benutzer ihr/sein Endgerät für den Zugang zum WiFi-Netzwerk mit der SSID "public-unifr" konfiguriert.

Dieser Internetzugang ist gebührenfrei.

Der Zugangscode (SMS) ist vertraulich und darf nur durch die beantragende Benutzerin / den beantragenden Benutzer selbst verwendet werden.

Die Infrastruktur dieses Dienstes wird nach bestem Wissen und Gewissen gepflegt. Die Universität kann jedoch kein ununterbrochenes Funktionieren der Infrastruktur garantieren, insbesondere nicht ausserhalb der üblichen Bürozeiten.

Jede Nutzerin und jeder Nutzer des Netzwerks trägt die Verantwortung für ihre/seine Handlungen ausschliesslich selbst.

Bei Missbrauch oder Missbrauchsverdacht, vorsätzlicher oder nicht vorsätzlicher Internetpiraterie sowie bei Vorliegen anderer Tatbestände kann die Universität einer Benutzerin oder einem Benutzer den Zugang sperren.

Obschon die Universität über Massnahmen zum Schutz ihres Netzwerks verfügt, kann sie keinen absoluten Schutz garantieren. Die Benutzenden sind dazu angehalten, ihre Endgeräte sorgfältig zu verwalten (durch regelmässiges Erstellen von Backups, Aktualisieren der Programmversionen, Verwenden eines Antivirusprogramms und Wachsamkeit bei unüblichem Verhalten des Geräts).

Die Universität kann nicht garantieren, dass alle Geräte technisch in der Lage sind, dieses Netzwerk zu nutzen. Die neueren, gängigen Modelle der wichtigsten Hersteller können jedoch problemlos angeschlossen werden.

Verschlüsselung (Vertraulichkeit der Kommunikation über das WiFi-Netzwerk der Universität). Mit SSID "public-unifr":

- Die Kommunikation wird nur mit einem schwachen (WEP) WiFi-Protokoll verschlüsselt, das nicht als ausreichend sicher angesehen werden kann.
- Es ist daher ratsam, dass Benutzerinnen und Benutzer verschlüsselte TCP-IP-Protokolle hoher Qualität verwenden (z.B. HTTPS für Zugriffe auf Websites).
- Wenn möglich sollten die Benutzer/innen das Netzwerk mit der SSID "eduroam" verwenden.

Aus technischen und rechtlichen Gründen setzt die Nutzung des WiFi der Universität eine Registrierung und die Speicherung u.a. der folgenden Daten voraus:

- Ihre Telefonnummer;
- Die MAC-Adressen der verwendeten Endgeräte (Smartphones, Tablets usw.);
- Ihre Zugangsdaten:
 - Datum und Uhrzeit Verbindungsbeginn,
 - Datum und Uhrzeit Verbindungsende,
 - Übertragene Datenvolumen,
 - Verwendete WiFi-Antenne.

Im Rahmen der geltenden datenschutzrechtlichen Bestimmungen werden diese Daten sechs Monate lang aufbewahrt und danach vernichtet. Bei Bedarf können sie anonymisiert zu statistischen Zwecken ausgewertet werden.

Der Internetzugang an der Universität Freiburg geschieht über einen Firewall der neuen Generation. Diese neue Generation erlaubt die Blockierung von gewissen Webseiten.

Das Rektorat hat entschieden, den Datenverkehr, welcher Malware enthält (z.B. von kontaminierten Webseiten) sowie den Zugang zu Webseiten von spezifischen Kategorien zu blockieren. Die blockierten Webseiten sind vom Rektorat festgelegt, unter Berücksichtigung des schweizerischen Strafrechts, der kantonalen Gesetzgebung sowie der internen Reglemente der Universität.

Gemäss diesen gesetzlichen Bestimmungen zeichnet das neue System Informationen über den blockierten Datenverkehr auf (angewählte URL, Kategorie der angewählten URL, Zeit, Datum, Quell-IP-Adresse, Ziel-IP-Adresse und je nach Fall den Benutzernamen). Nach einer Frist von sechs Monaten werden diese Informationen vernichtet. Bei Bedarf können sie anonymisiert zu statistischen Zwecken ausgewertet werden.

Generell gelten die Bestimmungen im "Reglement vom 7. Oktober 2003 über die Informatiksicherheit". Siehe unten.

Es gilt das schweizerische Recht. Gerichtsstand ist Freiburg.

Freiburg, 10. November 2017.

Directives

du 7 octobre 2003

sur l'utilisation des ressources informatiques de l'Université de Fribourg

Le Rectorat de l'Université

Vu l'art. 65 al. 4 lit. b des Statuts du 31 mars 2000 de l'Université de Fribourg;

Sur proposition de la Commission d'informatique,

Décide:

Article premier Principe

¹ Les présentes directives définissent les règles d'utilisation des ressources informatiques de l'Université de Fribourg.

² Elles concernent tous les utilisateurs et utilisatrices ayant accès à ces ressources.

³ L'Université de Fribourg met tout en œuvre pour assurer la protection de ses installations informatiques.

⁴ L'utilisation des ressources informatiques de l'Université de Fribourg entraîne l'acceptation des dispositions du présent document ainsi que des recommandations techniques publiées sur l'intranet à l'adresse <http://www.unifr.ch/siuf/user-policy>.

Art. 2 Accès aux comptes et aux ressources

¹ Un compte informatique est attribué par le Service Informatique de l'Université de Fribourg (ci-après: SIUF) à chaque utilisateur et utilisatrice; celui-ci permet l'accès à des ressources générales. Selon les besoins, une personne peut avoir plusieurs comptes.

² Un nom d'utilisateur ou d'utilisatrice et

Richtlinien

vom 7. Oktober 2003

für die Benutzung der Informatikmittel der Universität Freiburg

Das Rektorat der Universität

gestützt auf Art. 65 Abs. 4 Bst. b der Statuten der Universität Freiburg vom 31. März 2000;

auf Vorschlag der Informatikkommission,

beschliesst:

Artikel 1 Grundsatz

¹ Die vorliegenden Richtlinien legen die Regeln für die Benutzung der Informatikmittel der Universität Freiburg fest.

² Sie gelten für alle BenutzerInnen, welche zu diesen Informatikmitteln Zugang haben.

³ Die Universität Freiburg unternimmt alle erforderlichen Massnahmen, um die Sicherheit der Informatikmittel zu gewährleisten.

⁴ Die Benutzung der Informatikmittel gilt als Zustimmung zum Inhalt des vorliegenden Dokumentes sowie der unter der Adresse <http://www.unifr.ch/siuf/user-policy> im Intranet zur Verfügung stehenden technischen Empfehlungen.

Art. 2 Zugang zu Konten und Ressourcen

¹ Der Informatikdienst der Universität Freiburg (nachfolgend: IDUF) weist den BenutzerInnen ein Informatikkonto zu, das den Zugang zu den allgemeinen Ressourcen erlaubt. Je nach Bedarf kann eine Person über mehrere Konten verfügen.

² Jedem Benutzerkonto sind ein Benutzer-

un mot de passe sont associés à chaque compte.

³ Les ressources associées à un compte sont limitées selon le statut de l'utilisateur ou de l'utilisatrice.

⁴ L'utilisateur ou l'utilisatrice protège son compte par un mot de passe approprié.

⁵ Le mot de passe ne doit pas être divulgué à des tiers. Une dérogation est possible vis-à-vis du personnel du support ou de sécurité cité à l'art. 5 al. 1 pour autant que l'utilisateur ou l'utilisatrice estime la demande justifiée.

Art. 3 Cadre d'utilisation

¹ L'utilisation des ressources informatiques a pour but la réalisation du travail professionnel ou étudiant.

² L'utilisateur ou l'utilisatrice ne doit pas essayer d'accéder sans autorisation à des comptes, à des données ou à toute autre ressource et ne doit pas exploiter d'éventuelles failles de sécurité.

³ L'utilisateur ou l'utilisatrice est invité-e à informer le support informatique (cf. art. 5 al. 1) de tout abus ou utilisation non conforme qu'il ou elle pourrait constater au sein de l'Université. Si il ou elle estime déceler un grave problème de sécurité, il ou elle peut, toujours via le support, demander à contacter le ou la responsable de la sécurité informatique.

⁴ L'utilisateur ou l'utilisatrice doit respecter les lois en vigueur, notamment en ce qui concerne les copyrights, les droits d'auteur-e-s, les licences d'utilisation ainsi que la loi sur la protection des données [1].

⁵ L'utilisateur ou l'utilisatrice respectera les règles en vigueur à l'Université de Fribourg [2], y compris les dispositions relatives à des ressources spécifiques telles que, par exemple, les salles publiques.

⁶ L'utilisateur ou l'utilisatrice veillera à ne pas nuire à l'image de l'Université, ni porter préjudice aux ressources informatiques.

⁷ L'utilisateur ou l'utilisatrice se conformera aux dispositions de l'*Acceptable Use Policy* de Switch [3], ainsi qu'à celles de la *Netiquette* [4].

name und ein Benutzerpasswort zugeordnet.

³ Die Ressourcen eines Benutzerkontos werden dem Benutzerstatus entsprechend beschränkt.

⁴ Der/die BenutzerIn schützt sein/ihr Konto durch ein passendes Passwort.

⁵ Das Passwort darf nicht an Dritte weitergegeben werden. Ausgenommen sind die unter Art. 5 Abs. 1 erwähnten Support- oder Sicherheitsmitarbeiter, insofern der/die BenutzerIn dies für angemessen hält.

Art. 3 Benutzungsrahmen

¹ Informatikressourcen dienen der Erfüllung von beruflichen oder in Zusammenhang mit dem Studium stehenden Arbeiten.

² Der/die BenutzerIn darf nicht versuchen auf Konten, Daten oder andere Ressourcen zuzugreifen, für die er keine Berechtigung besitzt. Allfällige Sicherheitslücken dürfen nicht ausgenützt werden.

³ Der/die BenutzerIn wird aufgefordert, jeden Missbrauch oder sonstigen unangebrachten Gebrauch dem Informatiksupport (vgl. Art. 5 Abs. 1) zu melden. Besteht der Verdacht auf eine schwerwiegende Sicherheitslücke, kann der/die Sicherheitsbeauftragte via Informatiksupport kontaktiert werden.

⁴ Der/die BenutzerIn muss sich an die gesetzlichen Bestimmungen halten, insbesondere betreffend Copyright, Urheberrechten, Softwarelizenzen und Datenschutz [1].

⁵ Der/die BenutzerIn hält sich an die an der Universität Freiburg geltenden Regeln [2]. Darunter fallen unter anderem die Bestimmungen betreffend spezifischer Ressourcen wie z.B. die öffentlichen Computerräume.

⁶ Der/die BenutzerIn bemüht sich, dem Image der Universität nicht zu schaden und keinen absichtlichen Schaden an den Informatikmitteln zu zufügen.

⁷ Der/die BenutzerIn hält sich an die Bestimmungen der *Acceptable Use Policy* von Switch [3] sowie der *Netiquette* [4].

⁸ L'utilisation à titre privée est tolérée si:

- a) elle n'entraîne qu'un coût négligeable d'utilisation des ressources;
- b) elle ne relève pas d'une activité à but lucratif ou de propagande;
- c) pour le personnel de l'Université, elle s'effectue en dehors du temps de travail.

Art. 4 Responsabilité

¹ L'utilisateur ou l'utilisatrice est responsable de la mise en application de la sécurité informatique à son niveau.

² L'utilisateur ou l'utilisatrice est responsable de toute action effectuée sous l'identité de son compte. Le cas des comptes partagés sur certaines machines pour des raisons spécifiques est réservé.

³ L'utilisateur ou l'utilisatrice est responsable de la sauvegarde des données qu'il ou elle traite, ainsi que de leur intégrité.

⁴ L'utilisateur ou l'utilisatrice est responsable des informations qu'il ou elle rend accessible aux autres.

Art. 5 Information, formation et support

¹ Les utilisateurs et utilisatrices peuvent obtenir du support auprès des organes suivants :

- a) pour le personnel de l'Université :
 - le correspondant ou la correspondante informatique assigné-e à l'unité organisationnelle à laquelle appartient l'utilisateur ou l'utilisatrice;
 - le help desk du SIUF [5];
- b) pour les étudiants: Micromus [6];
- c) dans les salles publiques: le ou la surveillant-e, ainsi que l'administrateur ou l'administratrice des machines de ladite salle.

² Les utilisateurs et utilisatrices peuvent bénéficier de cours de perfectionnement auprès des organes suivants:

- a) pour le personnel de l'Université: au SIUF [7];
- b) pour les étudiant-e-s: Micromus.

⁸ Die Verwendung zu privaten Zwecken wird toleriert, sofern:

- a) keine massgeblichen zusätzlichen Betriebskosten entstehen.
- b) weder Erwerbstätigkeit noch Propaganda nachgegangen wird.
- c) dies, für das Personal der Universität Freiburg, ausserhalb der Arbeitszeit geschieht.

Art. 4 Verantwortung

¹ Der/die BenutzerIn ist für die Umsetzung der Informatiksicherheit auf seiner/ihrer Ebene verantwortlich.

² Der/die BenutzerIn ist für sämtliche unter seiner/ihrer Kontokennung ausgeführten Vorgänge verantwortlich. Ausgenommen sind gemeinsam genutzte Konten auf bestimmten Rechnern.

³ Der/die BenutzerIn ist für die Sicherung und Integrität der Daten verantwortlich, die er/sie verarbeitet.

⁴ Der/die BenutzerIn ist verantwortlich für Daten, welche er oder sie für andere Personen zugänglich macht.

Art. 5 Information, Weiterbildung und Support

¹ Die BenutzerInnen erhalten Unterstützung bei folgenden Organen:

- a) Personal der Universität:
 - bei den Informatik-KorrespondentInnen der Organisationseinheit, welcher die BenutzerInnen angehören.
 - beim Helpdesk vom IDUF [5];
- b) StudentInnen: bei Micromus [6];
- c) BenutzerInnen der öffentlichen Computerräume: beim zugewiesenen Betreuer oder beim Verantwortlichen.

² Die BenutzerInnen können die Weiterbildungsangebote folgender Stellen nutzen:

- a) Personal der Universität: beim IDUF [7];
- b) Studierenden: bei Micromus.

Art. 6 Sanctions

Toute violation des présentes directives ou d'une règle y relative peut être dénoncée à l'autorité compétente en vue de sanctions administratives et disciplinaires.

Art. 7 Entrée en vigueur

Les présentes directives entrent en vigueur dès leur adoption par le Rectorat.

Adoptées par le Rectorat de l'Université le 7 octobre 2003.

[1] Autorité cantonale de surveillance en matière de protection des données:
<http://www.fr.ch/sprd/>

[2] Règlements en vigueur à l'Université de Fribourg:
<http://www.unifr.ch/rectorat/reglements>

[3] Acceptable Use Policy de Switch, en version française:
<http://www.switch.ch/fr/network/aup.html>

[4] Netiquette, règles à observer lors de l'utilisation de l'Internet, version de référence en anglais:
<http://sunsite.cnlab-switch.ch/ftp/doc/standard/rfc/18xx/1855>

[5] Help desk du SIUF:
<http://www.unifr.ch/siuf/helpdesk>

[6] Micromus:
<http://www.unifr.ch/micromus>

[7] Cours du SIUF:
<http://www.unifr.ch/siuf/services/cours.html>

Art. 6 Sanktionen

Jede Zuwiderhandlung gegen diese Richtlinien oder gegen die sie begleitenden Regeln kann der zuständigen Autorität gemeldet werden und wird durch administrative und disziplinarische Sanktionen geahndet.

Art. 7 Inkrafttreten

Die vorliegenden Richtlinien treten mit ihrer Annahme durch das Rektorat in Kraft.

Angenommen durch das Rektorat der Universität am 7. Oktober 2003.

[1] Kantonale Überwachungsbehörde betreffend Datenschutz:
<http://www.fr.ch/sprd/de>

[2] Geltende Reglemente der Universität Freiburg:
<http://www.unifr.ch/rectorat/reglements>

[3] Acceptable Use Policy von Switch in deutscher Fassung:
<http://switch.ch/de/network/aup.html>

[4] Netiquette, bei der Internetbenutzung zu beachtende Regeln, Referenzfassung in Englisch:
<http://sunsite.cnlab-switch.ch/ftp/doc/standard/rfc/18xx/1855>

[5] Helpdesk vom IDUF:
<http://www.unifr.ch/siuf/helpdesk>

[6] Micromus:
<http://www.unifr.ch/micromus>

[7] IDUF-Kursprogramm:
<http://www.unifr.ch/siuf/services/cours-d.html>