

# Weisungen

Benutzung der IT-Ressourcen an der Universität Bern

**Klassifikation**

Für internen Gebrauch

**Dokumentenstatus**

Freigegeben

**Weisungen**

Benutzung der IT-Ressourcen an der Universität Bern

## Inhaltsverzeichnis

1.	Allgemeine Bestimmungen	3
1.1	Zweck .....	3
1.2	Begriffe .....	3
2.	Grundsätze zur Benutzung	3
2.1	Allgemeines .....	3
2.2	Bearbeitung von Personendaten.....	3
2.3	Weitergabe persönlicher Daten.....	4
2.4	Präsenz der Universität im Netz.....	4
2.5	Zugang zu den zentralen IT-Ressourcen .....	4
2.6	Campus Account .....	4
2.7	Private oder selbst administrierte IT-Geräte.....	4
3.	Nicht-universitäre Organisationseinheiten	4
4.	Mitglieder anderer akademischer Einrichtungen	5
5.	Missbrauch und Massnahmen bei Missbrauch	5
5.1	Missbrauch .....	5
5.2	Massnahmen bei Missbrauch.....	5
5.3	Stichproben, vorsorgliche Massnahmen, Berichterstattung, Protokollierung .....	6
6.	Schlussbestimmungen	7
6.1	Ausführungsbestimmungen.....	7
6.2	Inkrafttreten .....	7
6.3	Widersprechende Bestimmungen .....	7

**Weisungen**

Benutzung der IT-Ressourcen an der Universität Bern

*Die Universitätsleitung,*

gestützt auf Art. 3 Abs. 3 des Gesetzes vom 5. September 1996 über die Universität (UniG) und Art. 24 Abs. 2 Bst. i des Universitätsstatuts vom 7. Juni 2011 (UniSt),

*beschliesst:*

## **1. Allgemeine Bestimmungen**

### **1.1 Zweck**

Diese Weisungen regeln die Benutzung der IT-Ressourcen an der Universität Bern durch die berechtigten Benutzenden.

### **1.2 Begriffe**

IT-Ressourcen	beinhalten IT-Mittel, Informationen und IT-Dienste
IT-Mittel	sind alle Geräte, Einrichtungen und Programme materieller und immaterieller Art, die der elektronischen Verarbeitung, Speicherung, Übermittlung oder Vernichtung von Informationen dienen, namentlich: a) Computersystem und Smart Devices b) Peripherie-Geräte (z.B. Speichermedien) c) Netzwerke (wired und unwired) sowie Netzwerk-Geräte (wie z.B. Router, Repeater, Security-Devices, Wireless Access Points) d) Software
Informationen	sind Sach- und Personendaten
IT-Dienste	beinhalten zentrale Dienste, welche den berechtigten Benutzenden zur Verfügung stehen (z.B. E-Mail, DNS, Web-Services, Digital Libraries etc.)
Zentrale IT-Ressourcen	beinhalten IT-Mittel, Informationen und IT-Dienste, welche von den Informatikdiensten universitätsweit angeboten werden.

## **2. Grundsätze zur Benutzung**

### **2.1 Allgemeines**

Die IT-Ressourcen dürfen grundsätzlich nur zur Erfüllung universitärer Aufgaben verwendet werden.

Die Verwendung der IT-Ressourcen zu privaten Zwecken ist für die Mitarbeitenden der Universität Bern nur ausserhalb der Arbeitszeit erlaubt, sofern die vorliegenden Weisungen eingehalten werden.

Einer Bewilligung der Universitätsleitung bedürfen:

- a) die Nutzung der IT-Ressourcen zu privaten kommerziellen und zu privaten Werbezwecken
- b) der Umgang mit Daten mit rassistischem, sexistischem oder pornographischem Inhalt zu Lehr- und Forschungszwecken

Die Benutzung der IT-Ressourcen zwecks Erfüllung universitärer Aufgaben sowie für Lehre und Forschung hat gegenüber anderen Benutzungszwecken stets Vorrang.

### **2.2 Bearbeitung von Personendaten**

Die Bearbeitung von Personendaten ist nur im Rahmen der Erfüllung universitärer Aufgaben sowie unter Einhaltung der Datenschutzgesetzgebung zulässig.

Ist bekannt oder wird vermutet, dass Daten im Sinne der Datenschutzgesetzgebung in einer

## **Weisungen**

Benutzung der IT-Ressourcen an der Universität Bern

Organisationseinheit bearbeitet werden, muss eine Analyse respektive ein Konzept zu Informationssicherheit und Datenschutz (ISDS-Analyse / ISDS-Konzept) gemäss den Vorgaben des Amts für Informatik und Organisation (KAIO) erstellt werden.

### **2.3 Weitergabe persönlicher Daten**

Für den Zugriff auf Applikationen, welche über SWITCHaai authentifiziert und autorisiert werden, erfolgt ein Transfer von systemrelevanten Attributen, welche auch persönliche Daten enthalten. Diese Daten werden ausschliesslich für den bestimmten Zweck verwendet und dienen der Berechtigungsprüfung. Durch die Benutzung von Applikationen, auf welche der Zugriff via SWITCHaai erfolgt, gibt der Nutzende die Zustimmung zum Datentransfer.

Die persönlichen Daten stellen sich aus folgenden Attributen zusammen:

- Vorname
- Nachname
- E-Mail
- Geschlecht
- Bevorzugte Sprache
- Zugehörigkeit (faculty, student, staff, alum, member, affiliate, library-walk-in)
- Heimorganisation
- Typ der Heimorganisation (university)

### **2.4 Präsenz der Universität im Netz**

Die Universitätsleitung erlässt Weisungen und Empfehlungen über das Erscheinungsbild der Universität Bern im weltweiten und im universitätsinternen Netz.

### **2.5 Zugang zu den zentralen IT-Ressourcen**

Der Zugang zu den zentralen IT-Ressourcen ist nur mit einem Campus Account (Login-Name und Passwort) möglich.

### **2.6 Campus Account**

Der Campus Account ist persönlich und nicht übertragbar.

Die auf den Campus Account eingetragene Person ist für dessen Geheimhaltung unter Beachtung aller Vorsichtsmassnahmen verantwortlich. Besteht die Vermutung, dass ein Campus Account von Unbefugten benutzt wird, muss dies umgehend dem IT-Sicherheitsbeauftragten der Universität Bern oder den Konto-Verantwortlichen der zuständigen Organisationseinheit mitgeteilt werden.

Die Campus Accounts sind zu bewirtschaften. Dabei ist insbesondere die Existenzberechtigung der Campus Accounts regelmässig zu überprüfen. Campus Accounts ohne diese Berechtigung sind umgehend zu löschen. Die Leitungen der Organisationseinheiten bestimmen zu diesem Zweck die Konto-Verantwortlichen.

Weitere Regelungen zur Verwaltung der Campus Accounts werden in der Richtlinie „zur Verwaltung und Verwendung von Campus-Accounts“ festgelegt.

### **2.7 Private oder selbst administrierte IT-Geräte**

Die Unileitung begrüsst die Verwendung und Anbindung von privaten Geräten. Die Rahmenbedingungen sind in der „Weisung zur Anbindung von privaten oder selbst administrierten IT-Geräten an das allgemeine universitäre Netzwerk“ festgehalten.

## **3. Nicht-universitäre Organisationseinheiten**

Bei Organisationseinheiten, welche nicht der Universität Bern angehören, wird die Benutzung der IT-Ressourcen durch spezielle Vereinbarungen mit der Universität Bern geregelt.

## **Weisungen**

Benutzung der IT-Ressourcen an der Universität Bern

## **4. Mitglieder anderer akademischer Einrichtungen**

Mitglieder von anderen akademischen Einrichtungen können die IT-Ressourcen der Universität Bern gemäss gegenseitig akzeptierten Leistungsvereinbarungen benutzen.

## **5. Missbrauch und Massnahmen bei Missbrauch**

### **5.1 Missbrauch**

Missbräuchlich ist jede Verwendung der IT-Ressourcen, die:

- im Widerspruch zu den gesetzlichen Bestimmungen der universitären Gesetzgebung, insbesondere über die Erfüllung der universitären Aufgaben, steht
- gegen diese Weisungen verstösst
- gegen andere Bestimmungen der Rechtsordnung verstösst
- Rechte Dritter verletzt

Missbräuchlich sind insbesondere die folgenden Handlungen:

- a) Verarbeitung, Speicherung oder Übermittlung von Daten mit rassistischem, sexistischem oder pornographischem Inhalt, vorbehältlich 2.1 Abs. b)
- b) widerrechtliches Kopieren, Verändern und Löschen von Daten jeglicher Art
- c) Erstellen oder Verbreiten von schädlichen Programmcodes (wie z.B. Viren, Trojaner, Würmer)
- d) Hacking, namentlich
  - unbefugtes Eindringen bzw. versuchtes Eindringen in fremde Computersysteme
  - Treffen von Vorkehrungen zur Störung des Betriebs von Computern oder Netzwerken (*Denial of Service Attacks*)
  - Nicht authentifiziertes Absuchen von internen oder externen Netzwerken und Computern auf Schwachstellen (*Port-Scanning*)
  - Ausspionieren von Passwörtern
- e) Verwenden von vorgetäuschten IP- oder MAC-Adressen (*Spoofing*)
- f) Versenden von E-Mails mit vorgetäuschten E-Mail-Absender Adressen
- g) Veränderungen oder Erweiterungen von Netzwerk-Komponenten im Netzwerk der Universität ohne ausdrückliche Erlaubnis der Abteilung Informatikdienste (gemäss den *Weisungen über das Netzwerk der Universität Bern*)
- h) Registrieren von Nicht-UNIBE.CH Domains bei Drittprovidern auf Adressen des Netzwerks der Universität ohne ausdrückliche Erlaubnis des Ausschusses der Kommission für Informatikdienste (gemäss den *Richtlinien der Informatikdienste für Domain Name System (DNS), dynamische Adressvergabe (DHCP) und Fremddomains im Netzwerk der Universität Bern*)
- i) Massenversand von E-Mails im Sinne von unverlangten und unerwünschten E-Mails
- j) Belästigung anderer Personen durch Nutzung der IT-Ressourcen
- k) Manipulation von universitären IT-Ressourcen
- l) Verwendung der IT-Mittel in einer Weise, welche die Verletzung von Immaterialgüter- und Lauterkeitsrechten zur Folge hat

### **5.2 Massnahmen bei Missbrauch**

Die Benutzenden sind für die Verwendung der IT-Ressourcen unter Einhaltung der geltenden Rechtsordnung und dieser Weisungen persönlich verantwortlich. Insbesondere ist die auf den Login-Namen eingetragene Person für die Folgen der Verwendung der IT-Ressourcen, die unter Eingabe ihres Passwortes erfolgt, persönlich verantwortlich.

Bei Verstoss gegen die Rechtsordnung im Zusammenhang mit dem Gebrauch von universitären IT-Ressourcen oder bei Verstoss gegen diese Weisungen kann die Universitätsleitung alle zur Aufrechterhaltung bzw. Wiederherstellung des rechtmässigen Zustandes erforderlichen Massnahmen treffen, namentlich:

**Weisungen**

Benutzung der IT-Ressourcen an der Universität Bern

- a) Sperren des Zugangs zu den IT-Ressourcen oder andere Einschränkungen der Benutzung der IT-Ressourcen
- b) Hausverbot
- c) Löschen von Daten und Sperren von Homepages

Überdies können universitäts- bzw. personalrechtlich vorgesehene Sanktionen ergriffen werden. Die Strafverfolgung und die Geltendmachung zivilrechtlicher Ansprüche bleiben vorbehalten.

### 5.3 **Stichproben, vorsorgliche Massnahmen, Berichterstattung, Protokollierung**

Die IT-Sicherheitsbeauftragten können in Zusammenarbeit mit den IT-Verantwortlichen der universitären Einheiten anonyme Plausibilitätskontrollen (Stichproben) durchführen, um den Vollzug dieser Weisungen zu überprüfen.

Besteht der Verdacht auf Missbrauch von IT-Ressourcen, beantragen die IT-Sicherheitsbeauftragten der Universitätsleitung die Durchführung einer angekündigten, zeitlich befristeten Kontrolle gegenüber einem begrenzten Personenkreis. Die IT-Sicherheitsbeauftragten können vorsorglich den Zugang zu den IT-Mitteln sperren sowie verdächtige Informationen sichern.

Die IT-Sicherheitsbeauftragten erstatten der Universitätsleitung umgehend Bericht über die durchgeführte Untersuchung und allenfalls getroffenen vorsorglichen Massnahmen. Zudem beantragen sie bei der Universitätsleitung weitere Massnahmen zur Aufrechterhaltung bzw. Wiederherstellung des rechtmässigen Zustands auf dem Netz.

Erhalten die IT-Sicherheitsbeauftragten Kenntnis von Upload-Aktivitäten urheberrechtlich geschützter Daten (z.B. mittels Peer-to-Peer-Software) vom universitären Netzwerk aus, dürfen sie die hinter der Netzwerk-Adresse stehende Person, falls notwendig unter Mithilfe des Technik-Verantwortlichen der betreffenden Organisationseinheit, identifizieren und abmahnen. Im bestätigten Wiederholungsfall von Upload-Aktivitäten spricht die gemäss Universitäts- bzw. Personalgesetzgebung zuständige Person einen Verweis aus. Weitere Massnahmen sind nach Berichterstattung durch die IT-Sicherheitsbeauftragten von der Universitätsleitung zu bewilligen.

Die Aktivitäten, welche mit IT-Ressourcen der Universität Bern ausgeführt werden, werden von den Informatikdiensten aufgezeichnet und als sogenannte Randdaten gemäss dem Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs [BÜPF; SR 780.1] bzw. der Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs [VÜPF; SR 780.11], sechs Monate lang aufbewahrt.

Die Technik-Verantwortlichen der Institute sind verpflichtet, die Aktivitäten mit ihren IT-Ressourcen aufzuzeichnen und gemäss BÜPF bzw. VÜPF sechs Monate lang aufzubewahren.

Bern, 20.12.2016

**Weisungen**

Benutzung der IT-Ressourcen an der Universität Bern

## **6. Schlussbestimmungen**

### **6.1 Ausführungsbestimmungen**

Die Universitätsleitung kann weitere Ausführungsbestimmungen als Anhänge zu diesen Weisungen erlassen, die Artikel dieser Weisungen detaillieren.

Die Kommission für Informatikdienste (KID) kann im Rahmen ihrer Zuständigkeiten weitere Ausführungsbestimmungen in Weisungsform erlassen.

Diese Ausführungsbestimmungen bedürfen der Genehmigung durch die Universitätsleitung.

### **6.2 Inkrafttreten**

Die vorliegenden Weisungen treten mit ihrer Genehmigung in Kraft. Sie ersetzen die Weisungen über die Benutzung der IT-Ressourcen an der Universität Bern vom 27.10.2015

### **6.3 Widersprechende Bestimmungen**

Bestehende, diesen Weisungen widersprechende Bestimmungen werden hiermit aufgehoben.

Bern, 20.12.2016

Im Namen der Universitätsleitung

Der Rektor:



Prof. Dr. Christian Leumann