

12. 02. 2008
mit Änderungen
vom 09.06.2009

Weisungen über die 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. 68 Abs. 2 Bst. c des Universitätsstatuts vom 17. Dezember 1997 (UniSt),

beschliesst:

I. Allgemeine Bestimmungen

Zweck	Art. 1 Diese Weisungen regeln die Benutzung der IT-Ressourcen an der Universität Bern durch berechnigte Benutzerinnen und Benutzer.
Begriffe	Art. 2 IT-Mittel sind alle Geräte, Einrichtungen und Programme materieller und immaterieller Art, die der elektronischen Verarbeitung, Speicherung, Übermittlung oder Vernichtung von Informationen dienen, namentlich:
1. IT-Mittel	<ul style="list-style-type: none">a Computersysteme und Smart Devices;b Peripherie-Geräte (wie z.B. Speichermedien, Bandstationen etc.);c Netzwerke (wired und wireless) und Netzwerk-Geräte (wie z.B. Router, Repeater, Security-Devices, Wireless Access Points);d Software.
2. Informationen	Informationen sind Sach- und Personendaten.
3. IT-Dienste	IT-Dienste beinhalten zentrale Dienste, welche den berechtigten Benutzerinnen und Benutzern zur Verfügung stehen, wie E-Mail, DNS, Web-Services, Digital Libraries etc.
4. IT-Ressourcen	IT-Ressourcen beinhalten IT-Mittel, Informationen und IT-Dienste.
5. Zentrale IT-Ressourcen	Zentrale IT-Ressourcen beinhalten IT-Mittel, Informationen und IT-Dienste, welche von den Informatikdiensten universitätsweit angeboten werden.

II. Grundsätze zur Benutzung

Allgemeines

Art. 3 ¹ Die IT-Ressourcen dürfen grundsätzlich nur zur Erfüllung universitärer Aufgaben verwendet werden.

² Die Verwendung der IT-Ressourcen zu privaten Zwecken ist für Mitarbeiterinnen und Mitarbeiter der Universität Bern nur ausserhalb der Arbeitszeit erlaubt, sofern die vorliegenden Weisungen eingehalten werden.

³ 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.

⁴ Die Benutzung der IT-Ressourcen zwecks Erfüllung universitärer Aufgaben sowie für Lehre und Forschung hat gegenüber anderen Benutzungszwecken stets Vorrang.

Bearbeitung von
Personendaten

Art. 4 ¹ Die Bearbeitung von Personendaten ist nur im Rahmen der Erfüllung universitärer Aufgaben sowie unter Einhaltung der Datenschutzgesetzgebung zulässig.

² Wird vermutet, dass solche Daten in einer Organisationseinheit bearbeitet werden, muss eine ISDS-Analyse (Analyse zu Informationssicherheit und Datenschutz) gemäss den Vorgaben des Amts für Informatik und Organisation des Kantons Bern (KAIO) erstellt werden. *[Eingefügt am 9.6.2009]*

Präsenz der
Universität im Netz

Art. 5 Die Universitätsleitung erlässt Weisungen und Empfehlungen über das Erscheinungsbild der Universität Bern im weltweiten und im universitätsinternen Netz.

Zugang zu IT-
Ressourcen

Art. 6 ¹ Der Zugang zu den zentralen IT-Ressourcen, welche nur einem beschränkten Benutzerkreis zur Verfügung stehen, ist grundsätzlich nur mit einem Zugangskonto (Login-Name und Passwort, persönliches Zertifikat, Smart Card, Token etc.) möglich.

² Der Zugang zu IT-Ressourcen von Organisationseinheiten der Universität Bern, welche nur einem beschränkten Benutzerkreis zur Verfügung stehen, wird grundsätzlich nur mit einem Zugangskonto gestattet. Die Zugangskonten der IT-Ressourcen der Organisationseinheiten werden von den Organisationseinheiten erstellt, zugeteilt und verwaltet. Falls technisch möglich, können die Organisationseinheiten anstelle eigener Zugangskonten die Zugangskonten der zentralen IT-Ressourcen benutzen.

Zugangskonto

Art. 7 ¹ Die Verantwortung für die Erstellung, Pflege und Löschung von Zugangskonten liegt grundsätzlich:

- bei den Informatikdiensten für
 - immatrikulierte Studierende
 - Mitarbeitende mit einer Anstellung an der Universität
- beim Zentrum Lehre für
 - Alumni
- bei den Leitungen (Institutsdirektor/in, Abteilungsvorsteher/in etc.) der Organisationseinheiten für
 - alle übrigen Personengruppen

² Das Zugangskonto ist persönlich und nicht übertragbar.

³ Die auf das Zugangskonto eingetragene Person ist für dessen Geheimhaltung unter Beachtung aller zumutbaren Vorsichtsmassnahmen verantwortlich. Besteht die Vermutung, dass ein Zugangskonto von Unbefugten benutzt wird, muss dies umgehend der bzw. dem IT-Sicherheitsverantwortlichen der Universität Bern oder der bzw. dem EDV-Verantwortlichen der zuständigen Organisationseinheit mitgeteilt werden.

⁴ Die Zugangskonten sind zu bewirtschaften. Dabei ist insbesondere die Existenzberechtigung der Zugangskonten mindestens einmal monatlich zu überprüfen. Zugangskonten ohne diese Berechtigung sind umgehend zu löschen. Diese Überprüfung muss auch für die Zugangskonten für die IT-Ressourcen der Organisationseinheiten durchgeführt werden. Die Leitungen der Organisationseinheiten bestimmen zu diesem Zweck Systemverantwortliche. Die/der Systemverantwortliche ist auch für die Verwaltung und die Dokumentation der Berechtigungen für die Zugriffe von Administratoren auf die Systeme der Organisationseinheiten verantwortlich.

⁵ Weitere Regelungen zur Verwaltung der Zugangskonten zur Verwendung der zentralen IT-Ressourcen der Universität Bern werden in Anhang A (Bestimmungen zwecks Verwaltung von Zugangskonten für die zentralen IT-Ressourcen der Universität Bern) festgelegt.

III. Missbrauch und Massnahmen bei Missbrauch

Missbrauch

Art. 8 ¹ Missbräuchlich ist jede Verwendung der IT-Ressourcen, die

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

² Missbräuchlich sind insbesondere die folgenden Handlungen:

- a Verarbeitung, Speicherung oder Übermittlung von Daten mit rassistischem, sexistischem oder pornographischem Inhalt;
- 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*);
 - unauthentifiziertes 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-Absenderadressen;
- 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 über Fremddomains an der Universität Bern*);
- i Massenversand von E-Mails zu nicht-universitären Zwecken im Sinne von *Mail-Spamming*;
- k Belästigung anderer Personen mit IT-Ressourcen;
- l Manipulation von universitären IT-Ressourcen;
- m Verwendung der IT-Mittel in einer Weise, welche die Verletzung von Immaterialgüter- und Lauterkeitsrechten zur Folge hat.

Massnahmen bei
Missbrauch

Art. 9 ¹ Die Benutzerinnen und Benutzer 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, sofern nicht nachgewiesen werden kann, dass ihr Passwort ohne eigenes Verschulden unbefugt verwendet worden ist.

² 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:

- 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.

³ Überdies können universitäts- bzw. personalrechtlich vorgesehene Sanktionen ergriffen werden. Die Strafverfolgung und die Geltendmachung zivilrechtlicher Ansprüche bleiben vorbehalten.

Stichproben,
vorsorgliche
Massnahmen,
Berichterstattung,
Protokollierung

Art. 10 ¹ Die bzw. der IT-Sicherheitsbeauftragte führt in Zusammenarbeit mit den Informatikverantwortlichen der universitären Einheiten regelmässig anonyme Plausibilitätskontrollen (Stichproben) durch, um den Vollzug dieser Weisungen zu überprüfen.

² Besteht der Verdacht auf Missbrauch von IT-Ressourcen, beantragt die bzw. der IT-Sicherheitsbeauftragte der Universitätsleitung die Durchführung einer angekündigten, zeitlich befristeten Kontrolle gegenüber einem begrenzten Personenkreis. Die bzw. der IT-Sicherheitsbeauftragte kann vorsorglich den Zugang zu den IT-Mitteln sperren sowie verdächtige Informationen sichern.

³ Die bzw. der IT-Sicherheitsbeauftragte erstattet der Universitätsleitung umgehend Bericht über die durchgeführte Untersuchung und allenfalls getroffenen vorsorglichen Massnahmen. Sie oder er beantragt der Universitätsleitung weitere Massnahmen zur Aufrechterhaltung bzw. Wiederherstellung des rechtmässigen Zustands auf dem Netz.

⁴ Erhält die bzw. der IT-Sicherheitsbeauftragte Kenntnis von Upload-Aktivitäten copyright-geschützter Daten z.B. mittels Peer-to-Peer-Software vom universitären Netzwerk aus, darf sie bzw. er die hinter der Netzwerk-Adresse stehende Person, falls notwendig unter Mithilfe des IT-Verantwortlichen der betreffenden Einheit, 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 bzw. den IT-Sicherheitsbeauftragten von der Universitätsleitung zu bewilligen. *[Eingefügt am 9.6.2009]*

⁵ 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 (6) Monate lang aufbewahrt. *[Absätze 5 und 6 entsprechen den*

bisherigen Absätzen 4 und 5]

⁶ Die Verantwortlichen der IT-Ressourcen der Institute sind verpflichtet, die Aktivitäten mit ihren IT-Ressourcen aufzuzeichnen und gemäss BÜPF bzw. VÜPF sechs (6) Monate lang aufzubewahren. *[Absätze 5 und 6 entsprechen den bisherigen Absätzen 4 und 5]*

IV. Schlussbestimmungen

Ausführungs-
bestimmungen

Art. 11 ¹Die Universitätsleitung kann weitere Ausführungsbestimmungen als Anhänge zu dieser Weisung erlassen, welche Artikel dieser Weisung detaillieren.

² Die Kommission für Informatikdienste (KID) kann im Rahmen ihrer Zuständigkeiten weitere Ausführungsbestimmungen in Weisungsform erlassen.

³ Diese Ausführungsbestimmungen bedürfen der Genehmigung durch die Universitätsleitung.

Übergangs-
bestimmung

Art. 12 Die Zuteilung der Zugangskonten gemäss Art. 7 erfolgt schrittweise; diese Bestimmung findet nur Anwendung auf Personen, die bereits im Besitz eines Zugangskontos sind.

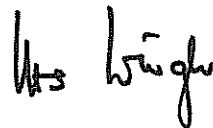
Inkrafttreten

Art. 13 Die vorliegenden Weisungen treten mit Genehmigung durch die Universitätsleitung in Kraft. Sie ersetzen die Weisungen über die Benutzung der Informatikmittel an der Universität Bern vom 26. April 2005.

Bern, 12.02.2008

Im Namen der Universitätsleitung

Der Rektor:



Prof. Dr. Urs Würigler

Änderungen

Inkrafttreten

Änderung vom 09.06.2009, in Kraft am 01.07.2009

Anhang A: Bestimmungen zwecks Verwaltung von Zugangskonten für die zentralen IT-Ressourcen der Universität Bern

Grundsatz

Der Gebrauch der zentralen IT-Ressourcen der Universität Bern ist für Personen vorgesehen, welche diese IT-Ressourcen im Rahmen ihres Studiums, ihrer Weiterbildung, ihrer Konferenzteilnahme oder ihrer Tätigkeit an bzw. für die Universität Bern nutzen.

Dieser Anhang regelt insbesondere den Ablauf der Verwaltung von Zugangskonten für die zentralen IT-Ressourcen an der Universität Bern sowie die Ahndung und Rechenschaftspflichten der verantwortlichen Person im Missbrauchsfall.

Zudem stellen die Regelungen dieses Anhangs sicher, dass nur Berechtigte Zugriff auf eingeschränkte Ressourcen erhalten und keine Vertragsauflagen oder Rechtsgrundlagen verletzt werden,

Die Erstellung, Pflege und Löschung von Zugangskonten liegt grundsätzlich in der Verantwortung

- der Informatikdienste (ID) für
 - immatrikulierte Studierende
 - Mitarbeitende mit einer Anstellung an der Universität
- des Zentrums Lehre für
 - Alumni
- der Leitungen (Institutsdirektor/in, Abteilungsvorsteher/in etc.) der Organisationseinheiten für
 - alle übrigen Personengruppen

Verantwortlichkeiten bei Vergabe und Verwaltung der Zugangskonten durch die Leitungen der Organisationseinheiten

Konto-Gruppen (inkl. E-Mail-Domänen) können beantragt werden für Organisationseinheiten der Universität, welche durch eine Kostenstelle charakterisiert sind. *[Eingefügt am 9.6.2009]*

Neuanträge für Gruppen ohne Kostenstellen oder Namensänderungen von bestehenden Gruppen mit/ohne zugehörige/r Kostenstelle müssen von einer Bewilligung der Universitätsleitung begleitet sein. Für Lehr- und Forschungsbereiche, sogenannte „Centers“, können ebenfalls Gruppen eingerichtet werden. Der Antrag muss von der Dekanin oder dem Dekan der zuständigen Fakultät oder der geschäftsführenden Direktorin oder des geschäftsführenden Direktors des zuständigen Instituts gestellt werden und unterliegt ebenfalls der Bewilligung der Universitätsleitung. Die Mitarbeiter des Centers sind berechtigt, neben ihrer Mailadresse des Instituts die Mailadresse des Centers als zweite Mailadresse zu führen. Diese Regelung gilt nicht für einzelne Projekte. Für die Löschung einer Gruppe ist sinngemäss der Antragsteller zuständig. *[Eingefügt am 9.6.2009]*

Die Verwaltung der Zugangskonten durch die Organisationseinheiten selbst obliegt deren Leitung. Die Zugangskonto-Verwaltung kann von der Leitung einer Organisationseinheit an eine oder mehrere Personen (z.B. die Ansprechpersonen für die Personal-Administration) delegiert werden. Alle Personen mit Anrecht zur Zugangskonten-Verwaltung werden im Folgenden als Konto-Verantwortliche bezeichnet. Änderungen der Konto-Verantwortlichen einer Organisationseinheit (z.B. personelle Wechsel, zusätzliche Personen) sind den ID umgehend schriftlich durch die Leitung der Organisationseinheit mitzuteilen. Ein Wechsel in der Leitung der Organisationseinheit selbst wird den ID durch die neue Leitung mitgeteilt.

Zugangskontoinhaber-Gruppen verwaltet durch die Organisationseinheiten

Die Konto-Verantwortlichen sind verpflichtet, die Zugehörigkeit der zukünftigen Inhaberinnen und Inhaber eines Zugangskontos zu einer der im Folgenden aufgeführten Gruppen korrekt anzugeben. Die Erstellung eines Zugangskontos für eine Person beinhaltet ebenfalls die Aufnahme dieser Person in das Partnerinformationssystem der Universität Bern.

Angehörige einer Organisationseinheit ohne Anstellung an der Universität Bern

Im Falle von weiteren Angehörigen einer Organisationseinheit ohne Anstellung an der Universität Bern (Projektpartnerinnen und Projektpartner, Gastdozierende, nicht angestellte Lehrbeauftragte, Mitarbeiterinnen und Mitarbeiter von Drittfirmen mit temporären Aufträgen für IT-Ressourcen der Universität Bern etc.) können Zugangskonten mit grundsätzlich eingeschränkten Rechten (z.B. online Journal-Zugang, Netzwerk-Zugang etc.) ebenfalls durch die Konto-Verantwortlichen der Organisationseinheiten befristet erstellt werden (bis zu einer Laufzeit von 12 Monaten [Fassung vom 9.6.2009], mehrfache Verlängerungen jeweils um weitere 12 Monate [Fassung vom 9.6.2009] möglich). Die Konto-Verantwortlichen können optional auch eMail-Adressen ihres Instituts für diese Personen vergeben.

Kumulative Voraussetzungen für die Vergabe und Aufrechterhaltung von Zugangskonten sind:

- Die Zugangskonto-Inhaberin oder der -Inhaber benötigt den Zugang zu IT-Ressourcen der Universität Bern, um eine Tätigkeit an oder zu Gunsten der Universität Bern durchführen zu können oder die Sichtbarkeit der Zugangskonto-Inhaberin bzw. des -Inhabers als Mitglied der Universität Bern ist der Reputation der Universität klar förderlich (z.B. eMail-Adressen bei Publizierenden) *und*
- die Benutzungsbedingungen der Universität Bern bezüglich IT-Ressourcen werden akzeptiert und eingehalten (u.a. keine rechtswidrige, kommerzielle oder private Benutzung des Zugangskontos) *und*
- die Lizenzbestimmungen der durch die Zugangskonto-Inhaberin benützten IT-Ressourcen werden nicht verletzt.

Für den allfälligen Missbrauch von IT-Ressourcen ist neben der Zugangskonto-Inhaberin bzw. des -Inhabers die Leitung der Organisationseinheit verantwortlich, falls das Zugangskonto regelwidrig erstellt wurde. Die Vergabep Praxis von Zugangskonten kann durch die Informatikdienste in Zusammenarbeit mit der Abteilung Personal auditiert werden. Im Falle einer missbräuchlichen Vergabep Praxis der Organisationseinheit kann das Recht auf eigenständige Vergabe von Zugangskonten entzogen werden.

Gäste, Kurs- und Konferenzteilnehmer

Die Konto-Verantwortlichen können für Gäste, Kurs- und Konferenz-Teilnehmende, Angehörige von Firmen (im Rahmen von Präsentationen oder Dienstleistungsaufträgen), etc Zugangskonten mit eingeschränkten Rechten (grundsätzlich nur Netzwerk-Zugang)

vergeben. Diese Zugangskonten haben eine maximale Laufzeit von einer Woche und werden anschliessend automatisch gelöscht. Zugangskonten für Kurs- und Konferenzteilnehmende können anonyme Usernamen haben (z.B. GUEST003), jedoch müssen die Konto-Verantwortlichen, welche das Zugangskonto vergeben haben, im Missbrauchsfall während einer Dauer von 6 Monaten eindeutig auf die Inhaberin oder den Inhaber des Zugangskontos zurück schliessen und diese Information den ID mitteilen können.

Nachdiplomstudierende

Nachdiplomstudierende für Studiengänge mit mehr als 60 ECTS-Punkten werden automatisch durch die Immatrikulationsdienste erfasst und erhalten damit ein Zugangskonto für die Dauer ihres Studiums. Für Teilnehmende von Nachdiplomstudien mit weniger als 60 ECTS-Punkten können die Konto-Verantwortlichen ein Zugangskonto mit eingeschränkten Rechten sowie unter Angabe des Endes des Nachdiplomstudiengangs erstellen. Das Konto wird nach dem Ende des Nachdiplomstudiengangs zusammen mit allfälligen persönlichen Postfächern, Fileablagen und Websites endgültig gelöscht.

Ehemalige Mitarbeitende im Publikationsprozess

Ehemalige Mitarbeitende der Universität Bern, welche noch im Publikationsprozess stehen, sind auf Datenzugriff und ihre publizierte eMail-Adresse angewiesen. Die Konto-Verantwortlichen können ihr Zugangskonto nach Ablauf des Anstellungsverhältnisses an der Universität Bern für jeweils weitere 6 Monate bis zu einer Maximaldauer von 18 Monaten verlängern lassen. Einfache eMail-Weiterleitungen können auf begründeten Antrag an die Konto-Verantwortlichen bis maximal 3 Jahre bestehen bleiben. Einfache eMail-Weiterleitungen können von den Konto-Verantwortlichen auch für andere ehemalige Mitarbeiter für die Dauer von 1 Jahr eingerichtet werden.

Emeriti und andere ehemalige Mitarbeitende im Ruhestand

Für ehemalige Mitarbeitende der Universität im Ruhestand können die Konto-Verantwortlichen ein Zugangskonto mit eingeschränkten Rechten erstellen. Die Emeriti sowie die ehemaligen Mitarbeitenden werden in der Regel in zwei separaten eMail-Domänen geführt. Falls die Leitung einer Organisationseinheit dies wünscht, können Mitarbeitende im Ruhestand auf begründeten Antrag an die Konto-Verantwortlichen die alten eMail-Konten behalten.

Zugangskontoinhaber-Gruppen verwaltet durch die Informatikdienste

Mitarbeitende mit einer Anstellung an der Universität Bern

Im Falle von zukünftigen Mitarbeitenden der Universität Bern können durch die Konto-Verantwortlichen befristete Zugangskonten mit einer maximalen Laufzeit von 2 Monaten erstellt werden, bevor der/die Mitarbeitende in die PERSISKA¹-Datenbank aufgenommen ist. Sobald die Daten via PERSISKA gemeldet werden, wird das Zugangskonto automatisch für die Dauer der Anstellung oder unbefristet verlängert. Nach Ablauf der Anstellungsdauer gemäss PERSISKA wird das Konto automatisch gesperrt. 6 Monate nach Ablauf der Anstellungsdauer wird das Konto zusammen mit persönlichen Daten wie Postfächern, Fileablagen und Websites gelöscht werden. Temporär erstellte Konten, welche vor deren Ablauf nicht durch eine Rückmeldung von PERSISKA bestätigt werden, werden automatisch gesperrt und nach weiteren 6

¹ PERSISKA ist das kantonale Gehaltsverarbeitungssystem

Monaten wiederum zusammen mit den persönlichen Postfächern und Files gelöscht werden.

Studierende

Die Studierenden erhalten automatisch ein Zugangskonto, sobald die Personalien nach der Voranmeldung kontrolliert sind. Das Zugangskonto bleibt für die Dauer des Studiums aktiv. Nach der Exmatrikulation bleibt das Zugangskonto 180 Tage gültig. Anschliessend wird es gelöscht.

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.

Mitglieder anderer akademischer Einrichtungen

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

Änderungsvorbehalt durch ID und Universitätsleitung

Die ID behalten sich vor, beim Vorliegen von wichtigen Gründen diese Zugangskonto-Bestimmungen in Absprache mit der Universitätsleitung jederzeit anpassen zu können.