# Weisung über den Umgang mit IT-Ressourcen an der Berner Fachhochschule

*Der Rektor der Berner Fachhochschule (BFH),*

gestützt auf Artikel 35 Absatz 2 Buchstabe h des Gesetzes vom 19. Juni 2003 über die Berner Fachhochschule (FaG[1]),

*beschliesst:*

## 1 Allgemeine Bestimmungen

### Art. 1 Zweck und Geltungsbereich

[1] Diese Weisung regelt den Umgang mit IT-Ressourcen durch berechtigte Nutzerinnen und Nutzer an der BFH.

[2] Diese Weisung gilt für alle Nutzerinnen und Nutzer von IT-Ressourcen der BFH.

### Art. 2 Begriffe

[1] *IT-Mittel* sind alle Geräte, Einrichtungen und Computerprogramme, die der elektronischen Bearbeitung von Informationen dienen, insbesondere:

- *a* Computersysteme und Smart Devices,
- *b* Peripheriegeräte (z.B. Drucker, externe Laufwerke, Speichermedien etc.),
- *c* Netzwerke (kabelgebunden und drahtlos) sowie Netzwerkgeräte (z.B. Router, WLAN Access Points, Security Devices etc.), und
- *d* Software.

[2] *Informationen* umfassen Sach- und Personendaten.

[3] *Randdaten* umfassen Informationen über die Nutzung von IT-Mittel.

[4] Das *Bearbeiten* von Personendaten umfasst jeden Umgang mit Personendaten, wie das Beschaffen, Aufbewahren, Verändern, Verknüpfen, Bekanntgeben oder Vernichten.

[5] *Bekanntgeben* ist jedes Zugänglichmachen von Personendaten, wie das Einsichtgewähren, Auskunftgeben, Weitergeben oder Veröffentlichen.

[6] *IT-Dienste* sind durch IT-Services betriebene Dienste, welche den Nutzerinnen und Nutzer zur Verfügung stehen (z.B. DNS, E-Mail, Verzeichnisdienste etc.) sowie durch die Departemente betriebene IT-Dienste und Dienste, welche durch Angehörige der BFH an oder für die BFH betrieben werden.

[7] *IT-Administratorinnen und IT-Administratoren* sind Personen, welche für den Betrieb der IT-Dienste zuständig sind.

[8] *IT-Ressourcen* beinhalten IT-Mittel, Informationen und IT-Dienste.

[9] *Nutzerinnen und Nutzer* sind alle Personen, welche IT-Ressourcen der BFH nutzen, insbesondere:

- *a* Angehörige der BFH gemäss Fachhochschulverordnung[2];
- *b* Personen, die im Anstellungsverhältnis von externen Organisationen stehen, welche im Auftrag oder als Partner der BFH Tätigkeiten an oder für die BFH verrichten (z.B. Forschungstätigkeiten, Support-, Wartungs- oder Entwicklungsarbeiten etc.);
- *c* Angehörige anderer akademischen Einrichtungen mit denen Vereinbarungen bestehen;
- *d* weitere Personen, welche an Anlässen teilnehmen und für eine definierte Zeit IT-Ressourcen der BFH nutzen.

[1] BSG 435.411.
[2] BSG 436.811.

## 2 Nutzung von IT-Mitteln an der BFH

### Art. 3 IT-Ressourcen

[1] IT-Ressourcen sind ausschliesslich für die Erfüllung der an der BFH anfallenden Aufgaben zu nutzen.

[2] Die private, persönliche, nicht kommerzielle Nutzung von IT-Ressourcen ist erlaubt, soweit sie die Erfüllung der Arbeits- und Studienpflichten sowie den Betrieb nicht beeinträchtigen.

[3] Die Nutzung von IT-Ressourcen für die Erfüllung der an der BFH anfallenden Aufgaben, insbesondere Lehre und Forschung, hat gegenüber allen anderen Nutzungszwecken stets Vorrang.

[4] Folgende Nutzungsarten bedürfen einer vorgängigen Bewilligung durch die Departementsleiterin oder den Departementsleiter und die Leiterin oder den Leiter IT-Services:

- *a* die Nutzung von IT-Ressourcen zu privaten Zwecken mit kommerziellem Ziel (z.B. SpinOff);
- *b* die Nutzung von IT-Ressourcen, welche im Regelfall als missbräuchlich im Sinne von Art. 7 anzusehen ist, soweit dies für die Erfüllung des Lehr- oder Forschungsauftrags unerlässlich ist.

[5] Die Nutzung der IT-Ressourcen durch Organisationseinheiten, welche nicht der BFH angehören, sowie die Nutzung gemäss Abs. 4 lit. a ist entschädigungspflichtig und wird in speziellen Vereinbarungen geregelt.

[6] Werden IT-Dienste nicht durch IT-Services, jedoch innerhalb des BFH Netzwerkes oder für die BFH betrieben, so obliegen sie denselben Anforderungen betreffend Datenschutz, Nutzungsbedingungen und Aufbewahrung der Randdaten.

[7] Auf offiziellen BFH-Geräten mit BFH-Clientsetup, welche durch die BFH bereitgestellt und unterhalten werden, dürfen keine Änderungen an sicherheitsrelevanten Einstellungen und Software vorgenommen werden.

[8] Der Diebstahl von IT-Geräten sowie weitere sicherheitsrelevante Beobachtungen im Zusammenhang mit IT-Ressourcen sind unverzüglich den IT-Services und der oder dem IT-Sicherheitsbeauftragten zu melden.

[9] Die Entsorgung von Informationen, welche auf Datenträgern gespeichert sind, wird durch die Weisung «Weisung über die Entsorgung von Datenträgern und die vorgängige Behandlung von Informationen an der Berner Fachhochschule» geregelt.

### Art. 4 Benutzeraccount

[1] Der Zugang zu IT-Ressourcen ist bis auf wenige Ausnahmen nur mit einem Benutzeraccount der BFH (Login-Name und Passwort) möglich.

[2] Der Benutzeraccount ist persönlich und nicht übertragbar.

[3] Die auf den Benutzeraccount eingetragene Person ist für dessen Geheimhaltung unter Beachtung aller zumutbaren Vorsichtsmassnahmen verantwortlich.

[4] Besteht die Vermutung, dass ein Benutzeraccount von Unbefugten benutzt wird, muss dies sofort den IT-Services via IT-Servicedesk mitgeteilt werden.

### Art. 4a Zugriff auf Benutzeraccounts

[1] Der direkte Zugriff auf Inhalte des Benutzeraccounts inklusive persönliche Mailbox durch andere Personen als die auf den Account eingetragene Person ist nicht erlaubt. Vorbehalten bleiben notwendige Vorkehrungen im Aufgabengebiet von IT-Administratorinnen und IT-Administratoren, bei welchen eine Kenntnisnahme der Inhalte so weit wie möglich zu vermeiden ist.

[2] Vorgesetzte dürfen von Mitarbeitenden Rechenschaft über den dienstlichen E-Mail-Verkehr verlangen und bei Anhaltspunkten für Pflichtverletzungen personalrechtliche Massnahmen ergreifen, in deren Rahmen eine Einsichtnahme in einen Benutzeraccount unter Beachtung von Absatz 6 zulässig ist.

[3] Bei Abwesenheit von längerer oder nicht absehbarer Dauer ist durch Mitarbeitende eine automatische Abwesenheitsmeldung einzurichten. Erfolgt dies nicht, ist die vorgesetzte Person ermächtigt, diese einrichten zu lassen.

[4] Wird vermutet, dass sich geschäftliche Daten, die für die gesetzliche Aufgabenerfüllung notwendig sind, im Benutzeraccount eines ehemaligen oder abwesenden Mitarbeitenden befinden, ist dieser zu kontaktieren und unter Fristansetzung aufzufordern, die Daten am regulären BFH Arbeitsort zur Verfügung zu stellen oder sein Einverständnis zu einem Zugriff auf die Daten auf die Benutzeraccounts zu geben.

[5] Kann der Mitarbeitende nicht kontaktiert werden oder kommt er den Aufforderungen gemäss Absatz 4 nicht nach, kann im Rahmen einer Ersatzvornahme Einsicht in die benötigten Daten genommen werden. Der Mitarbeitende ist bei der Fristansetzung auf die drohende Ersatzvornahme hinzuweisen. Auf die Fristansetzung kann verzichtet werden, wenn Gefahr im Verzug ist oder wenn feststeht, dass der Mitarbeitende die Verpflichtung nicht innert vernünftiger Frist erfüllen wird.

[6] Jeder Zugriff auf die Daten eines Benutzeraccounts muss verhältnismässig sein und durch die oder in Begleitung der vorgesetzten Person erfolgen. Private und geschäftliche Daten sind, soweit möglich, zu trennen, so dass eine Kenntnisnahme von privaten Inhalten vermieden wird. Die betroffene Person ist nach erfolgtem Zugriff über den Zeitpunkt, die erfolgten Schritte der Massnahme und die dabei anwesenden Personen zu informieren.

**Art. 5 Private oder selbstadministrierte IT-Geräte**

[1] Der Einsatz von Geräten, welche durch die Nutzerinnen oder die Nutzer selbst administriert werden oder der Einsatz von privaten Geräten ist mit Einschränkungen zulässig.

[2] Für den konformen Einsatz ist die Nutzerin oder der Nutzer selbst verantwortlich und zuständig.

[3] Ein solches Gerät darf nur ans Netzwerk (z.B. BFH LAN, BFH WLAN, VPN etc.) angeschlossen werden, wenn alle nachfolgenden Bedingungen erfüllt sind:

- *a* Das Gerät muss softwaretechnisch (Betriebssystem und Applikationen) bezüglich Sicherheitsupdates immer auf dem aktuellsten Stand sein.
- *b* Die auf dem Gerät eingesetzte Software muss aktiv mit Sicherheitsupdates versorgt werden (keine “End of Support/Life” Software).
- *c* Jede auf dem Gerät vorhandene oder installierte Software muss legal erworben und korrekt lizensiert sein sowie lizenztechnisch gemäss den jeweiligen Lizenz- und Nutzungsbestimmungen konform eingesetzt werden. Dies gilt sowohl für privat organisierte als auch für durch die BFH zur Verfügung gestellte Software.
- *d* Das Gerät muss mittels notwendiger Schutzmassnahmen, namentlich Antiviren-Software, Malwareschutz, lokaler Firewall und geeigneter Konfiguration, gesichert sein. Stellt das Betriebssystem des Geräts eine Funktion zur Verschlüsselung des Datenspeichers zur Verfügung, muss diese in einer dem Stand der Technik entsprechenden Konfiguration genutzt werden.
- *e* Die Nutzerin oder der Nutzer hilft bei der Klärung von IT-Vorfällen, falls sie oder er oder das entsprechende Gerät involviert ist, aktiv mit.

[4] IT-Services bieten „best effort“ Support für private oder selbstadministrierte Geräte. Weiter besteht kein Anspruch auf Support.

[5] Der Einsatz erfolgt auf eigene Gefahr. Die BFH lehnt jegliche Haftung durch die Nutzung solcher Geräte ab.

[6] Wird das private oder selbstadministrierte Gerät an eine dritte Partei weitergegeben (z.B. Entsorgung, Verkauf, Reparatur etc.) oder verlässt die Person die BFH, müssen vorgängig alle folgenden Bedingungen durch die Nutzerin oder den Nutzer sichergestellt werden:

- *a* Sämtliche auf dem Gerät gespeicherten Informationen der BFH sind der BFH zu übergeben.
- *b* Sämtliche auf dem Gerät gespeicherten Informationen der BFH sind nicht wiederherstellbar zu löschen.
- *c* Sämtliche Software, für welche die jeweiligen Lizenzbestimmungen eine Weiternutzung nicht explizit erlauben, ist zu deinstallieren.

## 3 Verantwortlichkeit und Haftung

### Art. 6 Compliance

[1] Jede Nutzerin oder jeder Nutzer hält sich immer an alle aktuell geltenden Gesetze und Reglemente, namentlich im Datenschutz- und Urheberrecht[3].

[2] Vor der Nutzung von IT-Ressourcen, insbesondere Software, informiert sich die Nutzerin oder der Nutzer über die dafür geltenden Lizenzbestimmungen und hält diese ein.

[3] Die Bearbeitung von Personendaten ist nur im Rahmen der gesetzlich verankerten Aufgaben der BFH unter Einhaltung der gesetzlichen Datenschutzbestimmungen, insbesondere des kantonalen Datenschutzgesetzes (KDSG)[4] und der davon abgeleitete Datenschutzverordnung (DSV)[5], erlaubt.

### Art. 7 Missbrauch

[1] Missbräuchlich ist jede Nutzung von IT-Ressourcen der BFH, welche die Vorschriften dieser Weisung missachtet, gegen übergeordnetes Recht verstösst oder die Rechte Dritter verletzt. Diese beinhaltet insbesondere folgende Handlungen, vorbehaltlich der explizit bewilligten Ausnahmen gemäss Art. 3 Abs. 4 dieser Weisung:

- *a* Die Bearbeitung von Informationen mit widerrechtlichem oder unsittlichem Inhalt, insbesondere Gewaltdarstellungen, Pornographie, Aufforderung zu Verbrechen oder Gewalttätigkeit, Störung der Glaubens- und Kultusfreiheit sowie Rassendiskriminierungen.
- *b* Die Herstellung, die Anleitung zur Herstellung oder die absichtliche Verbreitung von schädlichen Programmen oder Programmteilen (z.B. Viren, Würmer, Trojaner etc.).
- *c* Das unbefugte Eindringen in ein Datenverarbeitungssystem innerhalb oder ausserhalb der BFH („Hacking“), insbesondere das Ausspionieren von Passwörtern, nicht durch IT-Services autorisiertes Absuchen von BFH-internen und -externen Netzwerken sowie IT-Diensten auf Schwachstellen (z.B. Port-Scanning etc.), Vorkehrungen und Durchführung von Massnahmen zur Störung von Netzwerken und IT-Diensten (z.B. Denial of Service Attacks).
- *d* Informationsdiebstahl sowie widerrechtliches Bearbeiten von Informationen, insbesondere Kopieren, Verändern, und Löschen.
- *e* Verfügbarmachen von Inhalten auf BFH-internen oder -externen IT-Diensten, wenn dadurch gegen geltendes Recht verstossen oder das Ansehen der BFH gefährdet wird. Insbesondere darf kein urheberrechtlich geschütztes Material weiterverbreitet werden.
- *f* Die Nutzung von IT-Mitteln der BFH in absichtlicher Verletzung von Lizenzbestimmungen oder Urheberrechten.
- *g* Das Beschaffen, Speichern, Installieren, Aktivieren oder Verwenden von jeglicher nicht legal erworbenen Software, Lizenzen oder Dienste.
- *h* Das Versenden von Mitteilungen mit vorgetäuschten oder irreführenden Absenderangaben (inkl. technischer Adresse) oder von unverlangten Massen-E-Mails (z.B. Spam).
- *i* Die Belästigung oder Irreführung von Angehörigen der BFH oder Dritten durch Nutzung der IT-Ressourcen (z. B. E-Mail mit beleidigenden oder diskriminierenden Inhalten).
- *j* Die Erweiterung oder Veränderung von Netzwerkkomponenten der BFH (z.B. Modem, WLAN Access Points).
- *k* Das Verwenden von IT-Mittel zum Errechnen von digitalen Zahlungsmitteln, wie z.B. Bitcoin.
- *l* Die Nutzung von IT-Ressourcen zu privaten Zwecken mit kommerziellem Ziel (z.B. SpinOff)

### Art. 8 Konsequenzen bei Missbrauch

[1] Alle Nutzerinnen und Nutzer sind direkt und persönlich dafür verantwortlich, dass die Benutzung der IT-Ressourcen, insbesondere unter Verwendung des persönlichen Benutzeraccounts, nicht gegen diese Weisung oder gegen übergeordnetes Recht verstösst.

---

[3] SR 231.1.
[4] BSG 152.04.
[5] BSG 152.040.1.

[2] Wird ein Missbrauch oder ein konkreter Verdacht eines Missbrauchs von IT-Ressourcen festgestellt, so kann IT-Services alle notwendigen Massnahmen zur Wiederherstellung des rechtmässigen Zustands treffen, insbesondere:

*a* Vorsorgliche Sperrung des Zugangs zu den betroffenen IT-Ressourcen.
*b* Sicherstellung der missbräuchlichen Informationen und deren Sicherung oder Aufbewahrung zu Beweiszwecken.
*c* Löschung der missbräuchlichen Informationen, soweit dies aus Sicherheitsgründen erforderlich ist.
*d* IT-Services meldet die Umsetzung der oben aufgeführten Massnahmen der jeweilig betroffenen vorgesetzten Stelle.

[3] Bei einem Missbrauch können personal- oder studienrechtlich vorgesehene Sanktionen gegen die entsprechenden Nutzerinnen oder Nutzer ergriffen werden.

[4] Vorbehalten bleiben die Strafverfolgung und Ansprüche zivilrechtlicher Natur.

**Art. 9 Privacy**

[1] Zur Sicherstellung des Vollzugs dieser Weisung können durch die IT-Sicherheitsbeauftragten in Zusammenarbeit mit den zuständigen Verantwortlichen anonyme Plausibilitätskontrollen (Stichproben) durchgeführt werden.

[2] Zur Sicherstellung des Betriebs von IT-Diensten werden im Störungsfall und zur regelmässigen Prüfung der korrekten technischen Funktion Protokolldaten ausgewertet.

[3] Bei einem Verdacht auf Missbrauch von IT-Ressourcen beantragt die IT-Leitung bei der Rektorin oder dem Rektor die Durchführung einer angekündigten, zeitlich befristeten und auf einen definierten Personenkreis eingeschränkte Kontrolle.

[4] Aktivitäten durch die Nutzung der IT-Ressourcen können aufgezeichnet werden. Die dadurch anfallenden Randdaten werden zwecks Nachvollziehbarkeit der technischen Funktion und Beweissicherung aufbewahrt.
[5] Die Randdatenverordnung[6] findet soweit anwendbar, auf den Zugriff und die Auswertung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur aufgezeichnet werden (Randdaten), Verwendung.
[6] Randdaten, welche Personendaten beinhalten, werden mindestens 6 Monate und maximal 1 Jahr lang aufbewahrt. Eine abweichende Aufbewahrung ist zulässig, wenn gesetzliche oder reglementarische Vorgaben, namentlich die Randdatenverordnung[6] es gebieten oder dies zu Beweiszwecken notwendig ist. Für die Umsetzung gilt eine Übergangsfrist bis am 31.12.2021.

**Art. 10 Haftungsausschluss**

Die BFH übernimmt keine Haftung für Schäden, die aus Mängeln an oder bei der Benutzung von IT-Mitteln entstehen.

**4 Schlussbestimmungen**

**Art. 11 Schlussbestimmungen**

[1] Einzelne Artikel dieser Weisung können durch Anhänge weiter ausgeführt werden. Diese sind durch den Rektor zu genehmigen.

[2] Die vorliegende Weisung ersetzt die Version über den Umgang mit IT-Ressourcen an der Berner Fachhochschule vom 13. Juli 2016 und tritt per 01. Januar 2021 in Kraft.

Bern, 1. Januar 2021

Berner Fachhochschule
Sig.
Prof. Dr. Sebastian Wörwag
Rektor

[6] BSG 153.011.5.