universität
innsbruck

BETRIEBSVEREINBARUNG ZUM BETRIEB SOWIE ZUR DIENSTLICHEN UND PRIVATEN NUTZUNG VON INFORMATIONS- UND KOMMUNIKATIONSTECHNOLOGIEN

universität innsbruck

1. Geltungsbereich und Regelungsgegenstand

Diese Betriebsvereinbarung gilt:

a) persönlich:

für alle Mitarbeiter_innen der Universität Innsbruck mitsamt ihren Außenstellen sowie für die Bediensteten des Amtes der Universität Innsbruck, dh für jede vom Rektorat verschiedene natürliche Person (zB auch für Projektmitarbeiter_innen, Ferialarbeitskräfte, Leiharbeitskräfte, „externe" Lehrbeauftragte bzw Lektor_innen etc).

b) sachlich:

für die dienstliche und private Verwendung von Informations- und Kommunikationstechnologien (IKT) der Universität Innsbruck.

c) zeitlich:

ab dem Datum der Unterzeichnung vorerst befristet bis 31.12.2021.

Während dieser Zeit besteht eine Phase der beiderseitigen Prüfung der Anwendbarkeit dieser Vereinbarung, binnen der - auf Wunsch einer Vertragsseite - ergänzende Gespräche mit dem Ziel einer einvernehmlichen Abänderung geführt werden können.

Sollte bis acht Wochen vor Ablauf der Befristung keine Vertragsseite gegenüber der anderen Partei ausdrücklich und schriftlich auf ein Auslaufen der Betriebsvereinbarung mit Fristende bestehen, verlängert sich diese Betriebsvereinbarung jeweils um weitere zwölf Monate.

2. Zielsetzung und rechtliche Grundlagen

Der Einsatz von IKT-Systemen (zB Internet, Mail, Telefonie) ist in einem modernen Arbeitsumfeld unverzichtbar. Gleichzeitig ist die Nutzung dieser Systeme mit Risiken in technischer Hinsicht und in Hinblick auf die Verarbeitung personenbezogener Daten verbunden.

Diese Betriebsvereinbarung formuliert Grundsätze zum Betrieb von IKT-Systemen und zu deren sicherer und verantwortungsvoller Nutzung durch die MitarbeiterInnen.

Die Betriebsvereinbarung wird auf der Grundlage der gesetzlichen Bestimmungen abgeschlossen, insbesondere im Sinne der §§ 96 Abs. 1 Z 3, 96a Abs. 1 Z 1 sowie § 97 Abs. 1 Z 1 und 6 ArbVG sowie der Art 25 Abs. 1 und Art 32 Abs. 1 und 4 der EU-DSGVO.

3. Grundsätze für den Betrieb von IKT-Systemen

Die Mitarbeiter_innen der Universität Innsbruck haben zur Erfüllung ihrer dienstlichen Aufgaben Zugriff zu unterschiedlichen IKT-Systemen. Aus Gründen der Informationssicherheit ist dieser Zugriff so zu gestalten, dass ein Rückschluss auf die Person möglich ist (zB durch die Authentifizierung der Person vor der Verwendung von Computern und Netzwerken oder durch die Registrierung von Endgeräten).

universität innsbruck

3.1. Protokollierung, Einsichtnahme, Auswertung

Die Universität Innsbruck verpflichtet sich, im Regelbetrieb ausschließlich Verkehrs- und Bewegungsdaten zu protokollieren. Zur Wahrung von Datenschutz und Informationssicherheit sowie zur Gewährleistung des operativen Betriebes und der vorausschauenden Planung der IKT-Systeme und IKT-Services können automatisierte Auswertungen von Inhaltsdaten vorgenommen werden. Darüber hinaus gehende Auswertungen und Einsichtnahmen sind nur in folgenden Fällen zulässig:

- auf der Grundlage eines gerichtlichen Beschlusses,
- mit expliziter Zustimmung der Mitarbeiterin/des Mitarbeiters oder
- bei Vorliegen eines hinreichend begründeten Verdachts auf eine strafrechtlich relevante Handlung oder die Verletzung dienstlicher oder vertraglicher Pflichten,
- im Falle des Ablebens der Mitarbeiterin/des Mitarbeiters, bei Ausscheiden oder bei längerer Dienstverhinderung.

In den letzten beiden Fällen erfolgt die Einsichtnahme durch die/den Datenschutzkoordinator_in und im Beisein einer Vertreterin/eines Vertreters des zuständigen Betriebsrates. Als privat gekennzeichnete Inhalte sind in diesen beiden Fällen von der Einsichtnahme ausgeschlossen.

Personenbezogene Auswertungen über die Nutzung von IKT-Systemen, insbesondere zur Leistungs- und Verhaltenskontrolle, sind unzulässig.

3.2. Datenschutz und Informationssicherheit / Technische Maßnahmen

Die Universität verpflichtet sich, IKT-Systeme entsprechend dem Stand der Technik zu schützen (zB durch Firewalls, Virenüberprüfung auf Servern und auf bereitgestellten Endgeräten, automatisiertes Löschen von Spam- und Phishing-Mails) und eine Filterung von Inhalten ausschließlich zu diesem Zweck vorzunehmen.

Öffentliche oder gemeinsam genutzte Arbeitsplätze sind so zu gestalten, dass auf die von den Nutzer_innen generierten Inhalte wie E-Mails, Suchverlauf im Internet sowie heruntergeladene oder erstellte Dateien durch andere Nutzer_innen nicht zugegriffen werden kann. Dies erfolgt beispielsweise durch die Verwendung unterschiedlicher Benutzer_innenkonten oder das Löschen temporärer Dateien auf sog Kiosk-PCs.

3.3. Sperren von IKT-Systemen

Die Nutzung von IKT-Systemen der Universität Innsbruck ist auf die Dauer der Anstellung beschränkt.

Die Universität Innsbruck kann den Zugang zu IKT-Systemen für einzelne Mitarbeiter_innen insbesondere aus folgenden Gründen vorübergehend sperren:

- Beim Anfallen unverhältnismäßiger Kosten.
- Beim Drohen eines materiellen oder immateriellen Schadens für die Universität.
- Zur Wahrung von Datenschutz und zur Gewährleistung der Informationssicherheit.

In diesen Fällen wird die/der Mitarbeiter_in zur Klärung des Sachverhaltes unverzüglich kontaktiert. Auf Wunsch der Mitarbeiterin/des Mitarbeiters ist der zuständige Betriebsrat bei der Klärung hinzuzuziehen.

universität innsbruck

3.4. Fernwartung und Fernzugriff

Zur Wartung von universitätseigenen IKT-Systemen (PCs, Laptops, Handys etc) wird Software eingesetzt, die automatisiert Programme installiert, aktualisiert, deinstalliert oder konfiguriert.

Für die Planung von Investitionen und Betriebsmitteln, Verwaltung von Software- und Hardware-Lizenzen, Fehleranalysen, Kapazitätsplanung, Gewährleistung von Datenschutz und Informationssicherheit und für die Unterstützung der IKT-Serviceerbringung setzt die Universität Software ein, die automatisiert Informationen über installierte Programme, eingesetzte Hardware, Peripheriegeräte und Leistungsdaten (zB Speicherbelegung oder Systemauslastung) erfasst. Nicht ausgelesen werden Ordner, die zur persönlichen Nutzung vorgesehen sind (zB „Home Verzeichnisse"), der Papierkorb und Download-Verzeichnisse.

Zur Servicierung der IKT-Systeme installiert der ZID standardmäßig Fernwartungswerkzeuge, über die der aktuelle Bildschirminhalt eines Rechners auf Rechnern von IKT-Mitarbeiter_innen angezeigt und Interaktionen ermöglicht werden. Ein derartiger Zugriff erfolgt ausschließlich mit Wissen der Nutzerin/des Nutzers und muss von dieser/diesem im System freigegeben werden. Der Zugriff wird protokolliert.

4. Grundsätze für die dienstliche Nutzung von IKT-Systemen

Die Beschäftigten sind zu einem sorgsamen und verantwortungsvollen Umgang mit den zur Verfügung gestellten Systemen und Services verpflichtet. Dies umfasst insbesondere die Wahrung der materiellen und immateriellen Interessen der Arbeitgeberin sowie die Beachtung von Richtlinien der Universität Innsbruck, die zur Gewährleistung von Datenschutz und Informationssicherheit erlassen werden.

Die Universität schult die Beschäftigten bezüglich eines sicheren und verantwortungsvollen Umgangs mit IKT-Systemen.

Jedenfalls untersagt ist

- die Weitergabe der persönlichen Zugangsdaten (Benutzer_innenkennung und Passwort) an Dritte,
- jegliche Benutzung der zur Verfügung gestellten Ressourcen im Rahmen eines strafrechtlich relevanten Tatbestandes,
- der Zugriff auf strafrechtlich verbotene oder sonstige gesetzwidrige Inhalte sowie
- der Zugriff auf Inhalte, die herabwürdigende, beleidigende, verleumderische, verfassungsfeindliche, rassistische oder pornografische Äußerungen oder Abbildungen enthalten, sofern der Zugriff nicht zu Forschungs- oder Lehrzwecken erfolgt.

4.1. Dienstliche Nutzung von E-Mails

Für die Kommunikation im Rahmen der Beschäftigung an der Universität Innsbruck ist die von der Universität zur Verfügung gestellte E-Mail-Adresse zu verwenden.

Durch eine geeignete E-Mail Signatur ist der dienstliche Charakter der E-Mails anzuzeigen. Entsprechende Vorlagen werden von der Universität (Büro für Öffentlichkeitsarbeit) zur Verfügung gestellt.

universität innsbruck

Die personenbezogene E-Mail-Adresse und das zugehörige Postfach sind ausschließlich für die Nutzung durch die jeweilige Mitarbeiterin/den jeweiligen Mitarbeiter gedacht. Die Mitarbeiter_innen dürfen Dritten keine Zugriffsberechtigungen am E-Mail System einräumen (ausgenommen Kalenderfunktion).

4.2. Dienstliche Nutzung des Internets

Für externe Webseiten und Internetdienste sind Benutzungskennungen und Passwörter zu verwenden, die sich von den Zugangsdaten an der Universität Innsbruck unterscheiden.

Bei der Verwendung von geistigem Eigentum Dritter ist sicherzustellen, dass deren Rechte gewahrt bleiben (Urheberrecht, Markenrecht, Recht am eigenen Bild etc.). Die Universität bietet den Mitarbeiter_innen Schulungen an, in denen die gesetzlichen Grundlagen im Kontext der universitären Arbeit und Praxis erläutert werden.

4.3. Betrieb und dienstliche Nutzung von Telefonie und anderen Kommunikationssystemen

Den Mitarbeiter_innen stehen für die Kommunikation im Rahmen der Beschäftigung an der Universität Innsbruck neben E-Mail weitere Systeme zur Telefonie, Videokommunikation und Versendung von Textnachrichten (zB Chats) zur Verfügung.

4.3.1. Präsenzstatus

Werden bei Kommunikationssystemen Präsenzinformationen verwendet, so hat die Universität die Mitarbeiter_innen in geeigneter Weise zu informieren.

Den Mitarbeiter_innen muss ermöglicht werden, auf einfache Weise einen neutralen Status („unbekannt") einzustellen bzw den Präsenzstatus zu unterdrücken. Eine verpflichtende Nutzung eines nicht-neutralen Präsenzstatus ist unzulässig.

4.3.2. Gesprächsaufzeichnungen

Das Mithören von Gesprächen oder eine Aufzeichnung von Gesprächen durch die Universität sowie das Erstellen von Kommunikationsprofilen ist unzulässig.

4.3.3. Verrechnung

Aus betrieblichen Gründen (Kostentransparenz, interne Leistungsverrechnung) können die Kosten von Telekommunikationssystemen auf die Organisationseinheiten bzw. Projekte umgelegt und/oder an diese weiterverrechnet werden. In diesen Fällen erhält die Leitung der Organisationseinheit bzw des Projekts eine Auflistung der summierten Kosten pro Person und Nutzungsbereich (zB Inland/Ausland, Telefongespräche/SMS/mobile Daten).

Eine Detailauswertung ist nur zulässig, wenn die Gegenstelle anonymisiert wird. Eine nicht anonymisierte Auswertung darf nur der jeweiligen Nutzerin/dem jeweiligen Nutzer selbst zur Verfügung gestellt werden.

Sofern die private Nutzung von Kommunikationssystemen mehr als geringfügige Kosten erwarten lässt, kann die Universität Innsbruck vorsehen, dass sie von den Mitarbeiter_innen in geeigneter Form zu kennzeichnen ist (zB Vorwählen eines Sterns beim Telefonieren). Die Kosten für eine derart ausgewiesene private Nutzung können an die Mitarbeiterin/den Mitarbeiter verrechnet werden.

universität innsbruck

5. Private Nutzung

Die MitarbeiterInnen dürfen die IKT-Systeme der Universität im Umfang und nach den Regelungen der sog IKT-Nutzungsverordnung des Bundes (siehe Anhang 1) sinngemäß auch privat nutzen.[1]

Innsbruck, am 07. Sep. 2020

Für die Universität:

.....

Rektor
Univ.-Prof. i. R. Dr. Dr. h. c. mult. Tilmann Märk

Vizerektorin für Personal
Univ.-Prof. Dipl.-Psych. Dr. Anna Buchheim
Universität Innsbruck
6020 Innsbruck, Innrain 52

Für den Betriebsrat für das wissenschaftliche Personal:

.....

OR Mag. Christoph Bedenbecker (Vorsitzender)

Für den Betriebsrat der allgemeinen Universitätsbediensteten:

.....

ADir. RgR. Erwin Vones (Vorsitzender)

[1] Vollständige Bezeichnung: Verordnung der Bundesregierung über die private Nutzung der Informations- und Kommunikationstechnik-Infrastruktur des Bundes durch Bedienstete des Bundes (IKT-Nutzungsverordnung – IKT-NV)

universität innsbruck

ANHANG 1: IKT-Nutzungsverordnung zum Stichtag 20.02.2020

Verordnung der Bundesregierung über die private Nutzung der Informations- und Kommunikationstechnik-Infrastruktur des Bundes durch Bedienstete des Bundes (IKT-Nutzungsverordnung – IKT-NV)

Auf Grund des § 79d des Beamten-Dienstrechtsgesetzes 1979, BGBl. Nr. 333, und des § 29n des Vertragsbedienstetengesetzes 1948, BGBl. Nr. 86, beide zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 77/2009 wird verordnet:

§ 1. Begriffsbestimmungen

Im Sinne dieser Verordnung bedeuten die folgenden Begriffe:

1. „IKT" (Informations- und Kommunikationstechnologie oder -technik): alle Einrichtungen zur elektronischen oder nachrichtentechnischen Übermittlung, Speicherung und Verarbeitung von Sprache, Text, Stand- und Bewegbildern sowie Daten,
2. „IKT-Infrastruktur": alle Geräte („Hardware"), die vom Dienstgeber zur Verfügung gestellt werden oder im Einvernehmen mit dem Dienstgeber für dienstliche Zwecke benutzt werden und der Informationsverarbeitung für Zwecke des Dienstgebers dienen, sowie die darauf befindlichen Programme und Daten („Software"),
3. „korrekte Funktionsfähigkeit": Wahrung der Vertraulichkeit, der Integrität und Verfügbarkeit der IKT-Infrastruktur.

§ 2. Gegenstand

Diese Verordnung regelt die private Nutzung der IKT-Infrastruktur durch Bedienstete des Bundes.

§ 3. Allgemeine Grundsätze für die private Nutzung der IKT-Infrastruktur

Die Nutzung der für den Dienstbetrieb zur Verfügung stehenden IKT-Infrastruktur für private Zwecke ist im eingeschränkten Ausmaß zulässig. Sie darf jedoch nicht missbräuchlich erfolgen, dem Ansehen des öffentlichen Dienstes nicht schaden, der Aufrechterhaltung eines geordneten Dienstbetriebes nicht entgegenstehen und die Sicherheit und Leistungsfähigkeit der IKT-Infrastruktur nicht gefährden. Sie darf außerdem nur unter Beachtung sämtlicher weiterer ressort- oder arbeitsplatzspezifischer Nutzungsregelungen erfolgen. Insbesondere ist eine eigenmächtige Veränderung der zur Verfügung gestellten IKT-Infrastruktur (Hard- und Software) unzulässig. Die Bediensteten haben keinen Anspruch auf private Nutzung der vom Dienstgeber für den Dienstbetrieb zur Verfügung gestellten IKT-Infrastruktur.

§ 4. Internet

(1) Die Bediensteten dürfen vom Dienstgeber bereitgestellte Internetdienste für private Zwecke nur dann verwenden, wenn

1. eine Beeinträchtigung des Ansehens des öffentlichen Dienstes,
2. ein mehr als bloß geringfügiger Zeitaufwand während der Dienstzeit,
3. eine Anscheinserweckung, dass die Nutzung im Namen, Interesse oder mit Wissen des Dienstgebers vorgenommen wird,
4. die Erzeugung negativer Rechtsfolgen beim Dienstgeber,
5. eine Verletzung von Geheimhaltungspflichten,
6. eine Verletzung eigener oder fremder Dienstpflichten,
7. eine Verursachung von mehr als bloß geringfügigen Kosten und
8. eine Störung des Dienstbetriebes

ausgeschlossen sind.

(2) Das Abschließen von privaten Geschäften unter Zuhilfenahme der vom Dienstgeber zur Verfügung gestellten technischen Einrichtungen ist nur insoweit zulässig, als dabei in eindeutiger Weise der private Charakter des Vorgangs ersichtlich ist.

(3) Die Bediensteten haben keinen Anspruch auf Nutzung von Internetdiensten, die vom Dienstgeber als für den Dienstbetrieb nicht erforderlich erachtet werden. Der Dienstgeber kann zur Wahrung der in § 3 angeführten Nutzungsgrundsätze die Privatnutzung von Internet-Diensten beschränken oder gänzlich untersagen. Er darf dabei insbesondere Web-Inhalte durch den Einsatz von Filtersoftware sperren.

(4) Jedenfalls untersagt ist

1. der Zugriff auf strafrechtlich verbotene oder sonstige gesetzwidrige Inhalte,
2. jegliche Benutzung der zur Verfügung gestellten Ressourcen im Rahmen eines strafrechtlich relevanten Tatbestandes,
3. der Zugriff auf Internetseiten mit pornografischem Inhalt,
4. der Zugriff auf Seiten, die eine Zahlungsverpflichtung des Dienstgebers verursachen sowie
5. das Herunterladen von bestimmten, besonders für deren Größe oder Anfälligkeit für Schadprogramme bekannten ausführenden Dateitypen.

(5) Bei einem irrtümlichen Zugriff auf Seiten, die unter Abs. 4 fallen, sind diese unverzüglich wieder zu verlassen.

§ 5. E-Mail

(1) Die Bediensteten dürfen die vom Dienstgeber bereitgestellten E-Mail-Dienste für private Zwecke nur unter den für die Internetnutzung angeführten Bedingungen verwenden.

(2) Bedienstete dürfen in privaten E-Mails, die sie unter Verwendung ihrer dienstlichen E-Mail-Adresse versenden, keinen Hinweis auf ihre dienstliche Stellung oder ihre dienstliche Postadresse aufnehmen. Insbesondere das Hinzufügen der dienstlichen E-Mail-Signatur ist unzulässig.

(3) Der Dienstgeber darf private E-Mails in einem für die Abwehr von Schäden an der IKT-Infrastruktur oder zur Gewährleistung ihrer korrekten Funktionsfähigkeit notwendigen Ausmaß auf Schadsoftware und Spam scannen. Als Schadsoftware oder Spam identifizierte E-Mails werden je nach ressortspezifischer Strategie behandelt (Quarantäne, Löschung, etc.), wobei der oder die Bedienstete von mit Schadsoftware identifizierten E-Mails, soweit technisch möglich, unverzüglich in geeigneter Weise in Kenntnis zu setzen ist. Dies gilt in gleichem Maß für ein- und ausgehende E-Mails.

§ 5a. Soziale Medien

(1) Die Bediensteten dürfen die Registrierungen und Profile des Dienstgebers in sozialen Medien nicht für private Zwecke verwenden, soweit nicht durch ressort- oder arbeitsplatzspezifische Nutzungsregelungen Abweichendes festgelegt ist.

(2) Bedienstete dürfen im Rahmen der Verwendung privater Registrierungen und Profile in sozialen Medien nicht den Anschein erwecken, dass die Nutzung im Namen, Interesse oder mit Wissen des Dienstgebers vorgenommen wird.

(3) Darüber hinaus gelten die §§ 3 bis 5 sinngemäß für die Verwendung von Registrierungen und Profilen in sozialen Medien.

§ 6. Weitere Dienste

Beim Einsatz weiterer IKT-Infrastruktur-Dienste sind die §§ 3 bis 5a sinngemäß anzuwenden.

§ 7. Datenspeicherung und Datensicherung

(1) Die Bediensteten haben die Bestimmungen der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 04.05.2016 S. 1, in der Fassung

universität
innsbruck

der Berichtigung ABl. Nr. L 314 vom 22.11.2016 S. 72, des Datenschutzgesetzes, BGBl. I Nr. 165/1999, und der weiteren datenschutzrechtlichen Vorgaben in der jeweils geltenden Fassung einzuhalten.

(2) Ein Recht auf Zurückführung von Daten bei Datenverlust sowie auf ausreichenden Speicherplatz zur Ablage privater Daten oder zur Sicherung dieser Daten besteht nicht. Der Dienstgeber haftet in keinem Fall für den Verlust von privaten Daten.

(3) Der Speicherplatz für private Daten ist von den dienstlichen Bereichen bestmöglich zu trennen und zu kennzeichnen.

§ 8. Schlussbestimmungen

(1) § 5a samt Überschrift, § 6, § 7 Abs. 1 und § 8 samt Überschrift in der Fassung der Verordnung BGBl. II Nr. 107/2018 treten mit 25. Mai 2018 in Kraft.