In Kraft getreten: 25.01.2022

Richtlinie zur Informationssicherheit und Datenschutz

für alle Mitarbeiter*innen der ABPU

Version 1.3 – intern

ANTON BRUCKNER PRIVATUNIVERSITÄT für Musik, Schauspiel und Tanz

Alice-Harnoncourt-Platz 1 | 4040 Linz | Austria | T +43 732 701000 | E information@bruckneruni.at | W www.bruckneruni.at

Historie der Dokumentversionen

Version	Datum	Autor*in	Freigabe durch	Änderungsgrund / Bemerkung
1.0	19.01.2022	Informationssicherheit & Datenschutz	-	Ersterstellung
1.1	20.01.2022	Rektor	-	Korrekturen
1.2	22.10.2024	Grimberger	Beschluss Präsidium 30.10.2024 Aufgehoben durch Beschluss Präsidium 07.11.2024	Einarbeitung der Empfehlung des Oö. Landesrechnungshofs (Berichtspunkt 32) sowie der Ergänzungen des Präsidiums in der Sitzung vom 16.10.2024
1.3	05.11.2024	Grimberger	Beschluss Präsidium 13.11.2024	Einarbeitung der Empfehlung des Oö. Landesrechnungshofs (Berichtspunkt 32) sowie der Ergänzungen des Präsidiums in der Sitzung vom 16.10.2024. Klarstellungen hinsichtlich der Nutzung dienstlicher Geräte sowie der privaten Nutzung des E-Mail-Accounts nach Feedback von ZID und Senat

Inhaltsverzeichnis

Historie der Dokumentversionen 2
1 Einleitung 3
2 Kennwörter und Zugangsdaten 3
3 Nutzung privater und dienstlicher IT-Geräte 4
4 Nutzung der IT-Infrastruktur der ABPU 5
5 Zutritt und physische Sicherheit 6
6 E-Mail-Nutzung 6
7 Sichere Verhaltensweisen 7
8 Datenschutz 8
9 Entsorgung und Vernichtung 10
10 Social Media und Veröffentlichung 10
11 Verstoß gegen die Vorgaben 11
12 Inkrafttreten und Revision 11

1 Einleitung

Die Sicherheit von Informationen beruht auf einem ausgewogenen Zusammenspiel zwischen Technik, Prozessen & Menschen. In der zunehmenden Digitalisierung ist auch **der MENSCH** ein wesentlicher Bestandteil jeder Sicherheitsstrategie, sozusagen „**The Human-Firewall**“. Auch die Anton Bruckner Privatuniversität (ABPU) ist auf sichere Verhaltensweisen von Anwender*innen angewiesen, um den **Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen** gewährleisten zu können.

Die nachfolgenden Vorgaben halten die wesentlichen Verhaltens- und Nutzungsregeln fest – bitte bedenken Sie: Diese Grundsätze treffen nicht nur für das Arbeitsleben an der ABPU zu, sondern sind auch in Ihrem persönlichen, privaten Umfeld anwendbar!

2 Kennwörter und Zugangsdaten

- Die Kriterien für sichere Passwörter sind im bonline unter <Kennwort ändern> festgelegt und sind einzuhalten.
- Kennwörter sind mindestens einmal jährlich zu ändern. In besonderen Fällen (z.B. Kompromittierung eines Accounts) ist es dem ZID gestattet eine vorzeitige Änderung von Kennwörtern zu verlangen.
- Für dienstliche und private Zwecke sind unterschiedliche Kennwörter zu verwenden.
- Kennwörter sind sicher zu verwahren, sodass der Zugang für Dritte nicht möglich ist.
- Kennwörter dürfen unter keinen Umständen an Dritte weitergegeben werden.
- Bei Kompromittierung (auch im Verdachtsfall) von Kennwörtern oder Zugangsdaten sind diese umgehend zu ändern, und der ZID ist zu informieren.

3 Nutzung privater und dienstlicher IT-Geräte

Hinweis: Unter dem Begriff „IT-Geräte“ sind sämtliche elektronische Speichermedien subsumiert: Notebooks, Rechner, Tablets, Handys, Smartphones, USB-Sticks, (externe) Festplatten, Aufnahmegeräte, Festplatten von Druckern, etc.

- Bei allen IT-Geräten ist eine Zugriffssperre (z.B. Kennwort, PIN, Wischmuster, Fingerabdruck) einzurichten.
- Beim Verlassen des Arbeitsplatzes ist der Rechner zu sperren (Tastenkombination ⊞ + L).
- Es ist bei allen IT-Geräten eine automatische Geräte-/Bildschirmsperre einzurichten.
- Geräte dürfen zu keinem Zeitpunkt – insbesondere in öffentlichen Bereichen – unbeaufsichtigt zurückgelassen werden.
- Der Verlust eines Gerätes, auf dem dienstliche Daten gespeichert sind, ist umgehend dem ZID zu melden.

Hinweis: Zeitnahe Meldung ist besonders wichtig, damit die ABPU ggf. ihren gesetzlichen und/oder vertraglichen Verpflichtungen nachkommen kann. Ein Beispiel für eine gesetzliche Verpflichtung ist die Meldung einer Datenschutzverletzung an die Datenschutzbehörde, die spätestens 72 Stunden (!) nach Erkennen zu erfolgen hat.

- Es wird dringend empfohlen private Geräte, die für dienstliche Zwecke verwendet werden, mit aktueller Anti-Viren-Software auszustatten. Updates sollen regelmäßig eingespielt werden.
- Benutzer*innen, die private Geräte für dienstliche Zwecke verwenden, haben auf eigene Verantwortung für eine sichere Löschung bzw. Entsorgung dieser Geräte zu sorgen.

Hinweis: Einfaches Löschen von Dateien oder Zurücksetzen eines Systems sind nicht ausreichend! Unter Umständen können mit relativ einfachen Mitteln Daten wiederhergestellt werden.

- Unter keinen Umständen dürfen private Geräte, die dienstliche Informationen speichern, ohne weitere Sicherheitsmaßnahmen an Dritte weitergegeben oder über den normalen Hausmüll entsorgt werden.
- Benutzer*innen, die private Geräte für dienstliche Zwecke verwenden, haben dafür zu sorgen, dass Daten auf diesen Geräten regelmäßig gesichert werden, um möglichen Datenverlust zu vermeiden.
- Auf privaten Geräten ist dafür zu sorgen, dass Dritte nicht auf dienstliche Daten Zugriff erhalten (wenn beispielsweise ein Gerät von mehreren Familienmitgliedern genutzt wird).

---

*Hinweis: Die Zugriffstrennung kann z.B. dadurch erreicht werden, indem am Rechner für jede*n Benutzer*in ein eigenes Benutzer-Konto angelegt wird.*

Anleitung zur Einrichtung weiterer Benutzerkonto:

*Drücken Sie die Windows-Taste → Tippen und wählen Sie „**Systemsteuerung**“ → Navigieren Sie zu „**Benutzerkonten**“ → Fügen Sie unter „**Benutzerkonten verwalten**“ oder „**Anderes Konto verwalten**“ ein neues Konto hinzu.*

---

4 Nutzung der IT-Infrastruktur der ABPU

- Jegliche missbräuchliche Verwendung der IT-Infrastruktur der ABPU ist untersagt. Beispiele sind:
  - Versendung von Massen-/Spam-E-Mails oder Schadsoftware
  - Internet-Surfen auf gewalttätigen, rassistischen oder pornografischen Webseiten, Seiten mit Inhalten zur nationalsozialistischen Wiederbetätigung etc.
  - Download, Verbreitung oder Zurverfügungstellung von unerlaubten Inhalten (z.B. urheberrechtlich geschützte Werken)
- Dienstliche Informationen von Mitarbeiter*innen der Administration sind jedenfalls auf den IT-Systemen der ABPU (Cloud bzw. Netzlaufwerke) zu speichern (Ausnahme: private Smartphones mit Dual-Sim zur Nutzung der dienstlichen Mobilnummer).
  Eine zusätzliche Speicherung einzelner dienstlicher Informationen (z.B. Synchronisation des

Outlook-Postfachs, Webex-Nachrichten o.ä.) auf einem privaten Endgerät während eines aufrechten Dienstverhältnisses bleibt davon unbenommen.

- Dienstliche Informationen des künstlerischen und wissenschaftlichen Personals sind vorrangig auf den IT-Systemen der ABPU (v.a. Cloud) zu speichern.
- Der ZID sorgt für regelmäßige Datensicherung der IT-Systeme der ABPU, um möglichem Datenverlust entgegenzuwirken.

5 Zutritt und physische Sicherheit

- Räumlichkeiten, die nicht der Öffentlichkeit zugänglich sein sollen, sind beim Verlassen zu schließen bzw. zu versperren.
- Räumlichkeiten, die nicht der Öffentlichkeit zugänglich sein sollen, dürfen nicht durch Hilfsmittel (z.B. Einklemmen von Mülleimern) offengehalten werden.
- Zutrittskarten/-chips sind vorwiegend personalisiert ausgestellt und dürfen niemals an Dritte weitergegeben werden. Das Weitergabeverbot gilt auch für nicht-personalisierte Zutrittskarten/-chips.
- Der/die Besitzer*in einer/s Zutrittskarte-/chips trägt für alle Aktivitäten, die damit ausgeführt werden, die Verantwortung.

6 E-Mail-Nutzung

- Der E-Mail-Dienst der ABPU ist ein technisches Werkzeug, das die ABPU den Benutzer*innen kostenlos zur Verfügung stellt.
  Ausmaß und Rahmen einer geringfügigen privaten Nutzung des E-Mail-Accounts wird in der Rahmenbetriebsvereinbarung über die Verarbeitung personenbezogener Mitarbeiter*innendaten (Pkt. 9.4) geregelt.

- Der ZID ist aus sicherheitstechnischen Gründen bemächtigt, bei ein- und ausgehendem E-Mail-Verkehr mittels automatisierter Filtersysteme schadhafte E-Mails (z.B. Phishing-Mails) zu blockieren oder potentiell gefährliche Anhänge zu entfernen.
- Im Falle von Angriffen (z.B. Ransomware-Attacken) hat der ZID die Bemächtigung derartige E-Mails aus den Postfächern der Benutzer*innen zu entfernen.
- Links, Dateianhänge, etc. sind vor dem Anklicken bzw. dem Öffnen kritisch auf ihre Plausibilität und Echtheit zu prüfen – Achtung vor Phishing-Angriffen!
- Im Zweifelsfall ist mit dem ZID Rücksprache zu halten.
- Wurde ein schadhafter Link oder Anhang geöffnet oder installiert, ist dies umgehend dem ZID zu melden.

7 Sichere Verhaltensweisen

- Im Homeoffice oder beim Arbeiten außerhalb der ABPU gelten dieselben Sicherheits- und Datenschutzvorgaben wie am Arbeitsplatz.
- Geräte und Unterlagen im Zusammenhang mit der ABPU sind vor dem Zugriff Unberechtigter (z.B. Familienmitglieder, Besucher*innen, Freunde, Unbekannte) zu schützen.
- Nur wirklich notwendige Unterlagen dürfen ins Homeoffice mitgenommen werden und sind danach wieder an die ABPU zurückzubringen. Sie dürfen unter keinen Umständen mit dem normalen Haushaltsmüll entsorgt werden.
- Bei Gesprächen oder beim Arbeiten in öffentlichen Bereichen (z.B. öffentlichen Verkehrsmitteln, Cafe, Restaurant, Hotel) ist zu gewährleisten, dass vertrauliche Informationen „stillen Zuhörer*innen/ Beobachter*innen“ nicht zugänglich gemacht werden. Es ist auch auf geöffnete Fenster oder Türen zu achten.
- Neben E-Mails werden auch SMS, WhatsApp, SnapChat, div. Messenger-Dienste oder Soziale Netzwerke als Werkzeuge für Phishing-Angriffe verwendet. Erhöhte Achtsamkeit und kritisches Hinterfragen sind beim Öffnen von Dateien oder Klicken auf Links gefordert!

- Neben den Inhalten von Nachrichten sollte immer die Plausibilität von vermeintlichen Absender*innen kritisch geprüft und hinterfragt werden. *Beispiel: Warum erhalte ich vom „Helpdesk“ der ABPU eine Nachricht mit einer Aufforderung mich bei bonline anzumelden, obwohl an der ABPU kein Helpdesk eingerichtet ist?*

8 Datenschutz

Hinweis: Datenschutz bezieht sich auf den Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten. Die Grundsätze und Vorgaben sollen gewährleisten, dass die Grundrechte und Grundfreiheiten der Betroffenen gewahrt bleiben.

- **Rechtmäßigkeit und Zweckbindung**: Für jede Datenverarbeitung muss sowohl ein rechtmäßiger Grund als auch klare Zweckbestimmung vorliegen.
- **Transparenz**: Im Sinne der Transparenz sind alle Informationen zu Verarbeitungen leicht zugänglich und in einfacher, klarer Sprache zur Verfügung zu stellen.
- **Datenminimierung**: Es dürfen ausschließlich jene Daten von natürlichen Personen erhoben und verarbeitet, die für die Zweckerfüllung notwendig sind.
- **Richtigkeit und Verhältnismäßigkeit**: Bei jeder Datenerhebung und -verarbeitung ist zu prüfen, ob die Daten sachlich richtig und für die Zweckerreichung verhältnismäßig sind. Im Sinne von „Sind die Daten korrekt und tatsächlich für die Zweck-/Zielerreichung erforderlich oder kann ich das Ziel/den Zweck auch mit gelinderen Mitteln erreichen?“
- **Speicherbegrenzung**: Wenn Daten nicht mehr benötigt werden, die Zweckbindung nicht mehr gegeben ist und keine Aufbewahrungspflichten vorliegen, sind diese zu löschen bzw. zu vernichten.
- **Vertraulichkeit und Integrität**:

  Alle Mitarbeiter*innen sind zur Einhaltung des Datengeheimnisses verpflichtet. Dies inkludiert:

  - die Verschwiegenheit über alle Daten, die Mitarbeiter*innen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut worden sind bzw. werden,

- dafür zu sorgen, dass Unbefugte keinen Zugang zu derartigen Daten erhalten können,
- Daten, die Mitarbeiter*innen in Ausübung ihres Dienstes bekannt geworden sind/werden, nur zu dem zum jeweiligen rechtmäßigen Aufgabenvollzug gehörenden Zweck zu verwenden,
- Daten nur aufgrund einer ausdrücklichen Anordnung, eines Anordnungsbefugten zu übermitteln, wobei sich eine ausdrückliche Anordnung auch aus der Tätigkeitsbeschreibung ergeben kann,
- diese Verpflichtungen auch nach Beendigung des Dienstverhältnisses einzuhalten.

Personenbezogene Daten sind derart zu verwahren, dass unberechtigten Dritten der Zugang dazu verwehrt ist. Zudem sind diese Daten vor unbeabsichtigter Manipulation zu schützen.

Hinweis: Datenschutz betrifft sowohl elektronische als auch haptische Daten, also Informationen auf papierähnlichen Materialien (z.B. Ausdrucke).

- Weiterleitung oder Offenlegung von personenbezogenen Daten darf nur in rechtmäßig begründeten Fällen (und sofern für die Zweckerfüllung notwendig) erfolgen.
- Prüfen Sie vor dem Weiterleiten/Absenden von E-Mails, ob die Empfänger*innen korrekt eingetragen sind (Stichwort: „Antworten“ vs. „Allen Antworten“) und ob neu hinzugefügte Empfänger*innen den vorhergegangenen Kommunikationsverlauf einsehen dürfen.
- Die Funktion „Allen Antworten“ nur wenn absolut notwendig verwenden.
- Vermeiden Sie unnötigen „Mail-Ping-Pong“ (unübersichtlicher, lang gezogener E-Mail-Verkehr) bzw. Ketten-E-Mails.
- Insbesondere bei Datenübermittlung in Nicht-EU-Länder ist sicherzustellen, dass die Empfänger*innen entsprechende Garantien zum Datenschutz nach DSGVO gewährleisten.

Hinweis: Die Nutzung von Google Docs, OneDrive, etc. stellt bereits solche Datenübermittlungen dar.

- Jegliche Vorfälle, die eine Datenschutzverletzung darstellen können, wie bspw. der Verlust oder die unbeabsichtigte Offenlegung von personenbezogenen Daten, sind unmittelbar nach dem Erkennen an den Datenschutzkoordinator unter datenschutz@bruckneruni.at und an den ZID zu melden.
- Bei besonderen Kategorien personenbezogener Daten (z.B. Gesundheitsdaten, biometrische/genetische Daten, Gewerkschaftszugehörigkeit, Daten über ethnische Herkunft, politische Meinungen) ist erhöhte Vorsicht geboten, und deren Verarbeitung ist **grundsätzlich untersagt**. Eine Verarbeitung erfordert somit einen ausdrücklichen Ausnahmetatbestand und rechtmäßige Begründung.
- Pseudonymisierung und Anonymisierung von Daten sind wesentliche Sicherheitsmaßnahmen zum Datenschutz und sind – wo sinnvoll und machbar – anzuwenden.

9 Entsorgung und Vernichtung

- Vertrauliche und personenbezogene Informationen (z.B. Bewerbungsunterlagen, Benotungen, Beurteilungen, Finanzunterlagen, Protokolle) dürfen unter keinen Umständen zum „normalen“ Altpapier gelangen. Sie sind sicher zu entsorgen.
- Haptische (gedruckte) Unterlagen sind mittels Schredder zu vernichten.
- Private IT-Geräte, die dienstliche Informationen speichern, sind sicher zu löschen bzw. zu überschreiben oder physisch zu zerstören (siehe dazu auch Punkt 3).
- Dienstliche IT-Geräte sind bei Ausscheiden aus dem Dienststand dem ZID vollumfänglich zurückzugeben.

10 Social Media und Veröffentlichung

- Postings in Social Media Kanälen der ABPU oder Veröffentlichungen auf der Homepage sind mit den jeweils zuständigen Abteilungsleiter*innen oder Institutsdirektor*innen sowie mit der Abteilung Kommunikation & Marketing abzustimmen.

- Es dürfen keine vertraulichen Informationen oder Informationen, die negative Auswirkungen auf die ABPU oder ihre Mitarbeiter*innen / Studierenden haben können, veröffentlicht oder weitergegeben werden.
- Neben der Wahrung der Vertraulichkeit sind überdies das Datenschutzrecht und die DSGVO, Urheberrechte etc. einzuhalten.
- Negative, diffamierende oder destruktive Aussagen auf den Social Media Kanälen der ABPU (z.B. Falschaussagen eines Blog-Besuchers) sind umgehend den dafür zuständigen Abteilungen oder Instituten zu melden.

11 Verstoß gegen die Vorgaben

- Bei mutwilliger Nicht-Einhaltung der Vorgaben erfolgt eine schriftliche Abmahnung durch die Universitätsleitung mit der Aufforderung bestimmtes Verhalten zu unterlassen.
- Die Universitätsleitung behält sich weitere arbeitsrechtliche Schritte und / oder den Entzug von Zugriffs- und Zutrittsberechtigungen vor.

12 Inkrafttreten und Revision

(1) Diese Richtlinie tritt mit dem Beschluss durch das Präsidium der ABPU am 25. Januar 2022 in Kraft.

(2) Die Änderungen der Richtlinie mit Beschluss des Präsidiums vom 13.11.2024 treten mit 01.01.2025 in Kraft.

(3) Diese Richtlinie wird spätestens im Dezember 2027 einer Überprüfung unterzogen.