UNIVERSITÄT BIELEFELD

Informationssicherheitsbeauftragter

Basisschutzregelungen Informationssicherheit (BRI)

Maßnahmen Beschäftigte

Version: 1.0.2

Stand: 22.07.2024

Verabschiedung Rektorat: 08.06.2021

Vertraulichkeit: Öffentlich

Inhaltsverzeichnis

Vorwort

Sehr geehrte Mitarbeiter*innen,
liebe Kolleg*innen!

Erfolgreiche Forschung, Lehre und Verwaltung sind auf zuverlässige Prozesse und sichere Informationstechnik (IT) angewiesen.

Vor über zehn Jahren ist die erste Fassung der IT-Basisschutz Regelungen durch das Rektorat verabschiedet worden. Seitdem hat sich viel verändert: Die Digitalisierung ist deutlich fortgeschritten und neue Technologien und Arbeitsweisen sind hinzugekommen. Gleichzeitig sind aber auch die Bedrohungen gewachsen und die Universität ist verletzlicher für Angriffe auf ihre digitale Infrastruktur geworden. Viele von Ihnen haben in den letzten Jahren auch persönlich Erfahrungen mit Viren und „Phishing"-Angriffen gemacht. Solche Ereignisse haben vor allem die Beschäftigten der Universität Bielefeld im Visier.

Aus diesen Gründen ist es wichtig, dass Sie sich als Teil der Informationssicherheit verstehen. Sie sind die wichtigste*n Verbündete*n der Informationssicherheit wenn es um die richtige Reaktion auf Bedrohungen geht. Um diese wichtige Aufgabe erfüllen zu können, möchten wir Sie mit diesen Regelungen nicht nur bestmöglich unterstützen, Risiken zu vermeiden, zu erkennen wenn diese Auftreten und durch umsichtiges und richtiges Handeln Schaden von der Universität abzuwenden. Auch in Ihrem persönlichen Umfeld kann sich ein sicherer Umgang mit ihren wertvollen Daten auszahlen.

Wir wünschen Ihnen eine anregende Lektüre der überarbeiteten Basisschutzregelungen Informationssicherheit. Fragen oder Anregungen nimmt die Stabsstelle Informationssicherheit gerne entgegen.

Dokumentenhistorie

Version	Datum	Ereignis	Beteiligte
1.0	08.06.2021	Verabschiedung der Erstfassung	ISO, Rektorat
1.0.1	31.08.2021	Schärfung personengebundene Login-Kennungen (B11)	ISO, CIO-Gremium
1.0.2	22.07.2024	Korrektur Speicherung von Daten (B07)	ISO, Kanzler

B01 Ansprechpersonen

Ansprechperson	Durchwahl	E-Mail Adresse
Informationssicherheitsbeauftragte*r	3032	informationssicherheit@uni-bielefeld.de
Datenschutzbeauftragte*r	5225	datenschutzbeauftragte@uni-bielefeld.de
EDV-Betreuung (Fakultäten und Einrichtungen)	siehe PEVZ	siehe PEVZ
EDV-Betreuung (Zentralverwaltung)	6000	servicedesk@uni-bielefeld.de
BITS-Beratung	12777	bits@uni-bielefeld.de
Datenschutz- und Informationssicherheits-koordinator*innen (DISK)	siehe PEVZ	siehe PEVZ

B02 Vorgehen bei Informationssicherheitsvorfällen

Ein Informationssicherheitsvorfall ist gekennzeichnet durch den Verlust von Vertraulichkeit, Verfügbarkeit und/oder Integrität. In einem solchen Fall erhalten unbefugte Personen Zugriff auf dienstliche Daten (z.B. durch einen Passwortdiebstahl – Verlust von Vertraulichkeit), die Daten gehen verloren (z.B. durch einen Befall mit Schadsoftware – Verlust von Verfügbarkeit) und/oder die Daten liegen nicht mehr korrekt vor (z.B. durch eine absichtliche Manipulation – Verlust von Integrität).

Bei einem solchen Ereignis ist Folgendes zu beachten:

- Versuchen Sie nicht, auftretende Probleme eigenständig zu lösen.
- Verständigen Sie umgehend die für Sie zuständige EDV-Betreuung (zu finden im PEVZ) über den Vorfall und folgen Sie deren Anweisungen.
- Sofern ein Gerät betroffen ist, schalten Sie es nicht aus. Schalten Sie das WLAN ab und/oder trennen Sie das LAN-Kabel vom Gerät, sofern Ihnen die entsprechenden Mechanismen vertraut sind.
- Informieren Sie Ihre*n Vorgesetzte*n und den zuständigen DISK.

B03 Schlüssel und Raumsicherheit

Um ihren Arbeitsplatz angemessen zu schützen, beachten Sie Folgendes:

- Wenn Sie Ihren Raum verlassen, und sei es nur für kurze Zeit, schließen Sie diesen ab. Ein Diebstahl von Daten oder Gegenständen kann in kürzester Zeit geschehen.
- Lassen Sie vertrauliche Dokumente und Wertgegenstände nicht offen liegen. Räume können meist von mehreren Personen betreten werden (z.B. anderen Beschäftigten aus Ihrem Bereich, technischen Beschäftigten oder auch dem Reinigungsdienst).
- Lassen Sie dienstliche Schlüssel, Ausweise oder Zutrittskarten nicht an Orten liegen die für Unbefugte leicht zugänglich sind. Vermeiden Sie nach Möglichkeit, diese in der Freizeit bei sich zu führen. Melden Sie einen Verlust umgehend der verantwortlichen Ausgabestelle.

- Lassen Sie Unbefugte wie bspw. Gäste nicht unbeaufsichtigt an Ihren Arbeitsplatz. Das ist insbesondere dann wichtig, wenn Sie dort vertrauliche Daten verarbeiten.
- Wenn Sie Personen Zutritt zu geschlossenen Bereichen gewähren, stellen Sie sicher, dass diese berechtigt sind sich dort aufzuhalten oder begleiten Sie diese ggf. zu der Person, mit welcher sie verabredet ist. Sozialer Druck und Höflichkeit (z.B. Sie halten einer unbefugten Person die Tür auf, die anschließend Zugang zu einem geschlossenen Bereich erhält) werden oft verwendet um Sicherheitsmaßnahmen zu umgehen (sogenanntes Social Engineering).
- Sollten Sie an Ihrem Arbeitsplatz verdächtige, angeschlossene Geräte finden, bei denen es sich um Schadhardware handeln könnte (z.B. Geräte die Ihre Tastatureingaben aufzeichnen (Keylogger)), melden Sie diese umgehend Ihrer EDV-Betreuung (zu finden im PEVZ).

B04 Zugriffsschutz

Zum Schutz vor unbefugtem Zugriff auf Daten und IT-Geräte ist Folgendes zu beachten:

- Die Weitergabe von Passwörtern ist nicht gestattet.
- Das Arbeiten mit den Zugangsdaten anderer Personen ist nicht gestattet.
- Wenn Sie Ihren Arbeitsplatz (auch kurz) verlassen, sperren Sie Ihren Computer:
  - Windows: ⊞ Taste + L
  - MacOS: Steuerung + Shift + Auswerfen
  - Linux: Steuerung + Shift + L (kann abweichen)
- Aktivieren Sie einen Bildschirmschoner mit einem Passwortschutz, welcher nach einer kurzen Zeit der Inaktivität automatisch gestartet wird (falls nicht bereits vorhanden).
- Sofern neben einem Passwort zusätzlich die Nutzung einer „Zwei-Faktor-Authentisierung“ möglich ist (vergleichbar mit der TAN beim Homebanking wie z. B. mittels eines weiteren Bestätigungscodes welcher vom Smartphone erzeugt wird), sollte diese genutzt werden.
- Ändern Sie Ihr Passwort unverzüglich, wenn der Verdacht besteht, dass es unbefugten Personen bekannt geworden sein könnte. (siehe in diesem Fall: B02 - Vorgehen bei Informationssicherheitsvorfällen).
- Sofern Ihr Computer nicht dauerhaft eingeschaltet bleiben muss, schalten Sie ihn nach Beendigung der Arbeit aus.

B05 Software am Arbeitsplatz

Dienstliche Geräte werden in der Regel von der zuständigen EDV-Betreuung verwaltet. Diese ist für folgende Aufgaben zuständig, die nur von ihr ausgeführt werden dürfen:

- Einrichtung, Wartung und Betreuung von IT
- Installation und Pflege von Software (Ausnahme sind vom BITS bereitgestellte Programme)
- Umsetzung von Standardsicherheitsmaßnahmen (u.a. Virenschutz, Firewall, Sicherheitsupdates etc.)

Für dienstliche IT-Geräte, die **nicht** durch eine EDV-Betreuung verwaltet werden, ist folgendes zu beachten:

- Software (auch das Betriebssystem) muss immer auf einem sicherheitstechnisch aktuellen Stand gehalten werden. Verwenden Sie ausschließlich Software aus vertrauenswürdigen Quellen, beispielsweise von der Internetseite des Herstellers.
- Installieren Sie ausschließlich Software, die Sie für Ihre Arbeit benötigen. Da jede Software Schwachstellen aufweisen kann, erhöhen Sie damit die Sicherheit Ihres IT-Gerätes.
- Arbeiten Sie standardmäßig mit eingeschränkten Rechten, das Arbeiten als Administrator*in birgt zusätzliche Risiken.
- Eine Firewall und ein Virenscanner müssen aktiviert sein und aktuell gehalten werden. Für alle Beschäftigten stellt das BITS einen kostenlosen Virenscanner zur Verfügung (siehe Servicekatalog des BITS).
- Nutzen Sie ausschließlich Software, für die die Uni Bielefeld eine Lizenz erworben hat. Bei einem Einsatz nicht lizenzierter Software könnten erhebliche Schadenersatzforderungen auf Sie zukommen. Diese Einschränkung gilt nicht für lizenzfreie Software die gewerblich eingesetzt werden darf.

Der dienstliche Einsatz von Software zur Verarbeitung personenbezogener Daten ist mit den zuständigen DISKs abzustimmen.

B06 Handhabung von IT-Geräten

Für dienstliche IT-Geräte sind folgende Sicherheitsmaßnahmen umzusetzen:

- Schützen Sie Ihre IT-Geräte vor unbefugtem Zugriff durch Passwörter, PIN, Biometrie (Fingerabdruck, Gesichtserkennung etc.) oder ähnliche Funktionen.
- Um Diebstählen vorzubeugen, lagern Sie insbesondere mobile IT-Geräte sicher (z.B. in einem abgeschlossenen Schrank) oder nutzen Sie bspw. Laptopschlösser.
- Bei einem Verlust von IT-Geräten beachten Sie das Vorgehen bei Informationssicherheitsvorfällen (siehe Abschnitt B02 Vorgehen bei Informationssicherheitsvorfällen).
- Beachten Sie auch insbesondere die Regelungen zur Speicherung von Daten (siehe Abschnitt B07 Speicherung von Daten).

B07 Speicherung von Daten

Um dienstliche Daten gegen Verlust, ungewollte Veränderungen und unbefugten Zugriff zu schützen, sind diese sicher zu speichern:

- Daten auf lokalen Festplatten können bei einem Defekt der Festplatte vollständig verloren gehen. Speichern Sie Daten deshalb immer mit den angebotenen Speicherdiensten der Uni Bielefeld – beispielsweise auf den Netzlaufwerken oder auf Sciebo[1], der Campus-Cloud.
- Eine Speicherung dienstlicher Daten bei externen Anbietern, mit welchen die Universität nicht die entsprechenden Verträge abgeschlossen hat (z.B. Google, Dropbox, etc.) ist nicht gestattet.
- Die längerfristige Speicherung von Daten sollte grundsätzlich auf den Netzlaufwerken der Uni Bielefeld erfolgen. Klassische Speichermedien wie CDs, DVDs oder USB-Sticks

[1] https://www.uni-bielefeld.de/einrichtungen/bits/services/kuz/sciebo/

eignen sich, aufgrund der Fehleranfälligkeit und einer relativ kurzen Lebenszeit, nicht für eine dauerhafte Speicherung.
- Nutzen Sie Verschlüsselungsmechanismen, um Daten mit hohem Schutzbedarf gegen unbefugte Einsichtnahme zu schützen (siehe Abschnitt B09 Verschlüsselung von Daten).

B08 Handhabung dienstlicher Daten

Dienstliche Daten sind durch folgende Maßnahmen vor einer unbefugten Kenntnisnahme zu schützen:

- Stellen Sie Ihren Monitor nach Möglichkeit so auf, dass Unbefugte keinen Einblick in vertrauliche Daten nehmen können.
- Halten Sie Ihren Schreibtisch, insbesondere nach Arbeitsende, frei von offen liegenden, vertraulichen Unterlagen („clean desk“).
- Lassen Sie Ausdrucke nicht in zentralen Druckern liegen und nutzen Sie für vertrauliche Unterlagen die Funktion „vertrauliches Drucken“.
- Entsorgen Sie Fehldrucke und -kopien ordnungsgemäß (siehe Abschnitt B10 Entsorgung von Daten, Datenträgern und Dokumenten).
- Achten Sie bei einem Versand von vertraulichen Daten per Post auf eindeutige und korrekte Adressierung, vertrauenswürdige Versandwege und Nachverfolgbarkeit.
- Daten auf mobilen IT-Geräten sind besonders gefährdet. Beachten Sie die Regelungen unter Abschnitt B06.

B09 Verschlüsselung von Daten

Bei Daten mit hohem oder sehr hohem Schutzbedarf ist ein besonderes Augenmerk auf Verschlüsselung zu legen. Ihre EDV-Betreuung kann Ihnen Hinweise zu aktuellen Angeboten geben und Sie ggf. zu Lösungen beraten.
Die für eine Verschlüsselung verwendeten Passwörter bzw. Schlüsseldateien sind so zu hinterlegen, dass sie gegen eine unbefugte Kenntnisnahme und Verlust geschützt sind (siehe Abschnitt B14 Umgang mit Passwörtern).

B10 Entsorgung von Daten, Datenträgern und Dokumenten

Sofern Sie Daten haben, die Sie nicht mehr benötigen, muss sichergestellt werden, dass diese nicht in unbefugte Hände gelangen. Dazu müssen die Daten so vernichtet werden, dass sie nicht mehr wiederhergestellt werden können. Das gilt sowohl für elektronische Daten, als auch für solche auf Papier. Die dafür vorgesehenen Anlaufstellen an der Uni Bielefeld sind:

Art der Daten	Ort der Vernichtung
Datenträger, Smartphones, Tablets, Laptops etc.	BITS-Beratung (V0-215)
Arbeitsplatzcomputer	EDV-Betreuung (siehe PEVZ)
Papier (kleinere Mengen)	Aktenvernichter in T7-201
Papier (größere Mengen)	U-01-193 jeden Mittwoch 10:00 Uhr

- **Datenträger bis zur Größe eines Laptops** können im BITS (V0-215) während der Öffnungszeiten (Mo – Fr von 9:30 - bis 16:00 Uhr) über Sicherheitsbehälter entsorgt werden. Darunter fallen: Festplatten, Laptops, Handys, USB-Sticks, CDs, DVDs und ähnliches.
- **Magnet- und Videobänder** oder **größere Mengen kleiner Datenträger** sind bei der Entsorgung mit der Abfallwirtschaft abzustimmen (abfallwirtschaft@uni-bielefeld.de).
- **Arbeitsplatzcomputer und ähnliche Großgeräte** werden durch die EDV-Betreuung entsorgt.
- **Kleinere Mengen Papier** können im UHG im Aktenvernichter in T7-201 vernichtet werden.
- **Akten- und Papiervernichtung in größeren Mengen** erfolgt jeden Mittwoch von 10:00 – 10:30 Uhr in der Fahrstraße im Bereich T-01 (Bucht TLU). Besonders große Mengen (z.B. Archivauflösungen) sollten Sie ebenfalls mit der Abfallwirtschaft absprechen (abfallwirtschaft@uni-bielefeld.de).
- Bereiche außerhalb des UHG haben teils eigene Entsorgungsmöglichkeiten. Diese können bei der lokalen EDV-Betreuung in Erfahrung gebracht werden.
- Wollen Sie Ihre Dokumente selbst vernichten, benötigen Sie einen Aktenvernichter der mindestens die Sicherheitsstufe P4 (DIN 66399) erfüllt.
- Weitere Informationen erhalten sie auf der Webseite der Abfallwirtschaft.

B11 Nutzung von IT-Diensten

Die IT-Dienstleister der Uni Bielefeld bieten eine Reihe von kostenlosen IT-Diensten an. Ihre EDV-Betreuung kann Sie dabei unterstützen, passende Dienste für Ihre Bedarfe zu finden.

- Für die Verarbeitung von dienstlichen Daten sind IT-Dienste zu verwenden, die von der Universität angeboten werden. IT-Dienste, die nicht durch die Uni Bielefeld angeboten werden, können ein Risiko für die Vertraulichkeit, Integrität und Verfügbarkeit der dienstlichen Daten darstellen.
- Zur Nutzung von IT-Diensten sind personengebundene Login-Kennungen zu verwenden.
- Nutzen Sie für Ihren dienstlichen E-Mail-Verkehr ausschließlich E-Maildienste der Uni Bielefeld. Eine automatische Weiterleitung von E-Mails an externe Anbieter (wie beispielsweise Gmail, GMX oder web.de) ist nicht gestattet.
- Sollte bei einer Zusammenarbeit mit externen Partner*innen im Forschungskontext eine Nutzung externer Dienste erforderlich sein, sind die damit verbundenen Risiken für Vertraulichkeit, Integrität und Verfügbarkeit vor einer Nutzung angemessen abzuwägen.

B12 Datennetz

Die Erweiterung der bestehenden Netzinfrastruktur der Uni Bielefeld mit eigenen Geräten wie beispielsweise WLAN Routern, Repeatern oder Switchen, ist nicht gestattet. Beachten Sie ebenfalls die Regelungen des BITS und ggf. lokale Regelungen Ihrer Fakultät oder Einrichtung.

B13 Umgang mit Passwörtern

Sichere Passwörter sind essentiell für den Schutz Ihrer Daten, egal ob dienstlich oder privat. Wenn Sie ein Passwort erstellen, beachten Sie folgendes:

- Eine Mindestlänge von 12 Zeichen (je länger desto besser)
- Verwenden Sie Buchstaben (Groß- und Kleinschreibung) und Zahlen
- Vermeiden Sie leicht zu erratende Passwörter wie „123456“, „qwertzuiopü“, „Anna85!“ oder „Christian96“

Folgendes sollten Sie im Umgang mit Passwörtern beachten:

- Verwenden Sie verschiedene Passwörter für unterschiedliche Accounts
- Verwenden Sie einen Passwortmanager wie bspw. KeePass (https://keepass.info/) zur einfachen und sicheren Verwaltung Ihrer Passwörter. Von einer Speicherung Ihrer Passwörter im Browser sollte abgesehen werden
- Geben Sie Passwörter niemals an Dritte weiter (auch nicht an die EDV-Betreuung)

Tipps und Tricks:

- Passwortmerksätze sind bei der Erstellung von Passwörtern hilfreich. Beispiel: „Ich schaue aus dem Fenster und zähle 13 große schwarze Dohlen.“ wird zu „IsadFuz13gsD.“
- Aussprechbare Passwörter sind oft einfacher zu merken: „§3Absatz4Unterstrich2“

Alternativ können Sie, sofern technisch möglich, auch einen langen Satz oder eine Verkettung von mindestens drei zufälligen Worten als Passwort verwenden: „PferdTraktorSpatenstich“