UNIVERSITÄT BIELEFELD

Informationssicherheitsbeauftragter

Basisschutzregelungen Informationssicherheit (BRI)

Maßnahmen IT-Personal

Version: 1.0

Stand: 28.05.2021

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.

IT1 Physische Sicherheit

IT1.1 Klimatisierung, Wasserschäden und Brandschutz

IT-Technik wie Server, Router usw. sind vorzugsweise in IT-Räumen (Technik- oder Serverräumen) der IT-Dienstleister der Universität unterzubringen. Darüber hinaus darf IT-Technik nur in dafür geeigneten IT-Räumen untergebracht werden. Geeignete Räume müssen mindestens folgenden Anforderungen entsprechen:

- Die zulässige Betriebstemperatur und Luftfeuchtigkeit von IT-Räumen ist durch den Einsatz von ausreichend dimensionierten Klimatisierungsgeräten herzustellen. Für eine fachgerechte Aufstellung und Wartung der Geräte ist das Dezernat FM verantwortlich.
- IT-Systeme sind nicht in direkter Nähe oder unterhalb von wasserführenden Leitungen aufzustellen. Es dürfen nur wasserführende Leitungen verlegt werden welche der in den IT-Räumen aufgebauten Technik dienen (in der Regel Kühltechnik). Auch bei einem Wassereinbruch muss der weitere Betrieb der IT-Systeme gewährleistet sein. Dies gilt insbesondere dann, wenn die IT-Systeme in Kellerräumen aufgestellt werden.
- Die Regeln des vorbeugenden Brandschutzes sind zu beachten und einzuhalten. Für Hinweise und eine umfassende Beratung steht die Stabsstelle AGUS zur Verfügung.

IT1.2 Unterbrechungsfreie Stromversorgung (USV) und Überspannungsschutz

IT-Systeme mit hohen Anforderungen an Integrität und Verfügbarkeit sind an einer redundanten, ausreichend dimensionierten und gegen Überspannung abgesicherten Stromversorgung zu betreiben. Diese ist in Zusammenarbeit mit dem Dezernat FM herzustellen. Die Dimensionierung der USV muss mindestens ein rechtzeitiges und kontrolliertes Herunterfahren der durch sie geschützten Systeme sicherstellen. Die für den Betrieb notwendigen Unterlagen und Informationen zur elektrischen Versorgung, sind den Verantwortlichen des Bereichs durch das Dezernat FM auf Anfrage zur Verfügung zu stellen.

IT1.3 Verkabelung

Die Netzwerkadministration muss einen vollständigen Überblick über das von ihr betriebene LAN-Netz haben. Zu diesem Zweck muss sowohl die Anschlussbelegung der einzelnen Komponenten, als auch die physische Verkabelung klar strukturiert und übersichtlich vorgenommen, sowie angemessen dokumentiert werden. Für die Verkabelung ist das Dezernat FM verantwortlich.
Unbefugter Zugriff auf die Verkabelung muss verhindert werden. Erweiterungen und Veränderungen an der Gebäudeverkabelung sind mit dem Dezernat FM abzustimmen.
Netzwerkzugänge über die fest installierte Verkabelung müssen von der Netzwerkadministration automatisch abgeschaltet werden, wenn sie nicht genutzt werden. Ist abzusehen, dass ein Netzwerkzugang permanent nicht mehr verwendet wird (z.B. weil ein Büro nicht mehr genutzt wird) muss die Deaktivierung des Zugangs durch die EDV-Betreuung des Bereichs umgehend beauftragt werden.

IT1.4 Netzzugänge

Der Anschluss von IT-Systemen an das Datennetz der Universität Bielefeld darf ausschließlich über die dafür vorgesehene Infrastruktur erfolgen. Maßnahmen und Eingriffe, die den Betrieb der Datennetz-Infrastruktur stören, sind zu unterlassen bzw. unverzüglich zu beseitigen. Eine Einrichtung von zusätzlichen Verbindungsmöglichkeiten am Netz der Universität Bielefeld ist nicht gestattet. Dazu zählen insbesondere:

- eigene WLAN Access Points
- eigene DSL-Anschlüsse oder andere Zugangsmechanismen, die an das Netz der Universität angeschlossen werden und auf diesem Weg eine Verbindung zwischen zwei Netzen herstellen können

Ausnahmen von dieser Regelung bedürfen der Zustimmung des BITS.

IT1.5 Ausfallsicherheit

Maßnahmen zur Ausfallsicherheit der IT-Systeme sind entsprechend den Anforderungen an ihre Verfügbarkeit umzusetzen.

IT1.6 Sicherung von IT-Räumen

Der unbefugte Zutritt zu IT-Räumen, wie beispielsweise Technik- und Serverräumen, muss durch angemessene Maßnahmen verhindert werden. Je nach Schutzbedarf sowie in Abhängigkeit von äußeren Bedingungen (öffentlich zugänglicher Bereich, Lage zur Straße usw.) sind besondere bauliche Maßnahmen, wie zum Beispiel einbruchsichere Fenster und Türen, Bewegungsmelder, Alarmanlagen o. ä. zur Verhinderung von gewaltsamem Eindringen zu realisieren.
IT-Räume dürfen nur durch geeignete Schließsysteme zu öffnen sein und müssen selbstständig schließende Türen haben. Verwendete Schlüssel müssen kopiergeschützt sein. Der Zutritt ist auf diejenigen Personen zu begrenzen, deren Arbeitsaufgaben dies erfordern. Die Schlüsselverwaltung muss sicherstellen, dass Schlüssel bzw. elektronische Schließberechtigungen nur an befugte Personen vergeben werden. Die Schließberechtigung für Räume ist nachvollziehbar zu dokumentieren.
Reinigungspersonal sollte die IT-Räume nur unter Aufsicht bzw. zu festgelegten Zeiten betreten.

IT1.7 Ausgabe von IT-Geräten

IT-Geräte sind durch ihre hohe Mobilität Sicherheitsrisiken ausgesetzt, die gesonderte Maßnahmen erfordern:

- Bei der Übergabe dienstlicher IT-Geräte sind die Beschäftigten für die Risiken der Geräte zu sensibilisieren und über die Pflichten bei der Nutzung aufzuklären.
- Die Verwaltung, Wartung und Weitergabe der Geräte ist durch die einzelnen Bereiche eindeutig zu regeln.
- Es muss durch die Umsetzung des Abschnittes IT3.3 Patches, Updates, Malwareschutz sichergestellt werden, dass von solchen Geräten keine Gefährdungen für dienstliche Daten, andere IT-Systeme oder das Datennetz ausgehen. Geräte, die ein

Sicherheitsrisiko darstellen (z.B. durch veraltete Hardware die keine Sicherheitsupdates mehr zulässt), müssen zeitnah ausgetauscht werden.
- Verarbeiten die IT-Geräte Daten mit hohem oder sehr hohem Schutzbedarf ist der Abschnitt IT2.4 Verschlüsselungssysteme zu beachten.

IT2 Zugriff

IT2.1 Kennungen, Zugriffsrechte und administrative Accounts

Für den Zugang zu IT-Systemen ist mindestens eine Anmeldung mit Kennung und Passwort (bzw. analoge Authentisierungsmechanismen wie z. B. ein SSH-Key) notwendig. Personen sind nur mit den Zugriffsberechtigungen auszustatten, die sie unmittelbar für die Erledigung ihrer Aufgaben benötigen. Vergabe bzw. Änderung und Entzug von Zugriffsberechtigungen sind durch einen verbindlichen Prozess zu regeln und nachvollziehbar zu dokumentieren.
Dies gilt insbesondere auch für Administratorrechte. Sind diese nicht notwendig, sind sie unabhängig von Status und Hierarchie nicht zu gewähren. Für alltägliche Arbeiten ist eine Kennung ohne Administratorrechte zu verwenden.

IT2.2 Passwörter (IT)

Für die Sicherheit von IT-Systemen sind – sofern technisch möglich – die folgenden Anforderungen an Passwörter einzuhalten:
- Die Mindestlänge beträgt 12 Zeichen.
- Leicht zu erratende Passwörter müssen technisch verhindert werden.
- Für eine Erstanmeldung oder das Zurücksetzen eines Passwortes sollten Initialpasswörter vergeben werden (Passwörter, die nach einmaligem Gebrauch gewechselt werden müssen).
- Bei der Zurücksetzung eines Passwortes sollten Maßnahmen zur Verifikation der Identität der Betroffenen greifen (Informationen, die nur der Person bekannt sein sollten wie beispielsweise die Uni-ID).
- Die Passwörter dürfen im System nicht im Klartext gespeichert werden, beispielsweise durch den Einsatz einer adäquaten Einwegverschlüsselung.
- Passwörter müssen verschlüsselt übertragen werden.
- Bei der Eingabe sollte das Passwort grundsätzlich nicht im Klartext einsehbar sein. Eine Funktion zur Anzeige im Klartext ist gestattet.
- Anmeldeversuche sollten nach einer bestimmten Anzahl von Fehlversuchen automatisch unterbunden werden, beispielsweise durch eine temporäre Sperre.
- Benutzer*innen müssen ihr Passwort jederzeit ändern können.
- Zentrale Authentisierungsdienste wie Shibboleth oder Active Directory sind vorrangig zu nutzen.

IT2.3 Sperre bei Inaktivität

IT-Systeme müssen so konfiguriert sein, dass sie spätestens nach 10-minütiger Inaktivität automatisch gesperrt und erst nach erneuter Authentisierung wieder genutzt werden können.

IT2.4 Verschlüsselungssysteme

Dienstliche Daten mit hohem oder sehr hohem Schutzbedarf sind durch geeignete und angemessene Verschlüsselungslösungen zu schützen bzw. solche Bedarfe auf Seiten der Beschäftigten durch die EDV-Betreuung zu unterstützen (sofern diese nicht durch Mechanismen des Betriebssystems bereits gewährleistet wird wie beispielsweise durch Android- oder iOS-Mechanismen).

IT3 Software

IT3.1 Installation von Software

Alle dienstlichen IT-Systeme der Universität Bielefeld, die von der EDV-Betreuung administriert werden, sind gegen eine unbefugte Installation von Software zu schützen.

IT3.2 Beschaffung von Soft- und Hardware

Die EDV-Betreuung ist bei der Beschaffung von Soft- und Hardware für die Einhaltung von Standards und Sicherheitsanforderungen verantwortlich. Entsprechende Anforderungen können bei der Beschaffung in Erfahrung gebracht werden.

IT3.3 Patches, Updates, Malwareschutz

Um Soft- und Hardwareprodukte vor potentiellen Angriffen zu schützen, sind Patches und Updates der Hersteller in Abhängigkeit von ihrer Kritikalität schnellstmöglich zu installieren. Neben dem Betriebssystem sind auch sämtliche Applikationen (einschließlich ihrer Erweiterungen) stets aktuell zu halten. Das verantwortliche IT-Personal sollte sich regelmäßig über bekannt gewordene Schwachstellen informieren.
Der Betrieb von IT-Systemen, die von der Universität bereitgestellt werden, ist ohne angemessene Basisschutz-Maßnahmen wie Virenscanner, Firewall und aktuelle Software- und Betriebssystemversionen nicht gestattet. Ausnahmen von dieser Regelung, beispielsweise für Laborgeräte, sind mit den Datenschutz- und Informationssicherheitskoordinator*innen (DISK) abzustimmen und zu dokumentieren.

IT3.4 Entwicklung von Software

Bei der Entwicklung von Software sind - in Abhängigkeit vom Schutzbedarf der durch die Software verarbeiteten Daten - bewährte Prinzipien wie der Einsatz von Software-Tests und Dokumentation sowie Code Review zu berücksichtigen.
Software-Entwicklungen, die aufgrund ihrer Größenordnung Projektcharakter haben und die Geschäftsprozesse der Universität Bielefeld unterstützen, müssen nach standardisierten Verfahren (Vorgehensmodellen) durchgeführt werden.
Vor dem Einsatz muss die Erfüllung der funktionalen Anforderungen durch hinreichende Tests sichergestellt werden. Der Testverlauf und das Testergebnis sind zu dokumentieren.

Entwicklung, Tests oder Anpassung von Software dürfen in der Regel nur mit Daten erfolgen, die keinen Personenbezug haben (anonymisierte Daten). Ausnahmen hiervon müssen mit der* dem Datenschutzbeauftragen abgestimmt werden.

IT3.5 Protokollierung (Logging)

Bei dem Einsatz von Software müssen alle sicherheitsrelevanten Aktivitäten protokolliert werden. Dies dient unter anderem dem frühzeitigen Erkennen und Beheben von Fehlern und der Identifikation von Angriffen.
Die Protokollierung muss sich in ihrer Ausführung nach dem Schutzbedarf des Verfahrens richten und kann je nach Anforderung auf sicherheitsrelevante Ereignisse beschränkt werden. Eine Sichtung bzw. Auswertung des Logs muss zeitnah und mit geeigneten Werkzeugen geschehen.
Es ist sicher zu stellen, dass nur die Personen Zugriff auf die Logs haben, die diese für ihre Aufgabenerfüllung zwingend benötigen. Das Prinzip der Zweckbindung und der Datensparsamkeit nach der Datenschutzgesetzgebung ist zu beachten (auch in Bezug auf die Aufbewahrungsfristen).

IT3.6 Dokumentation von IT-Verfahren

IT-Verfahren sind in folgenden Punkten von den jeweils verantwortlichen Personen (in Klammern) zu dokumentieren:

- Zweck des IT-Verfahrens bzw. Zielsetzung (Verfahrensverantwortliche)
- Durchführung einer Schutzbedarfsfeststellung (Verfahrensverantwortliche)
- Ggf. Durchführung einer Risikoanalyse ab einem hohen Schutzbedarf (Verfahrensverantwortliche, EDV-Betreuung, DISK)
- Beschreibung der Rollen und Berechtigungen (ggf. in Form eines Berechtigungskonzepts) (Verfahrensverantwortliche, EDV-Betreuung)
- Festlegung von technischen und organisatorischen Maßnahmen (TOMs) (Verfahrensverantwortliche, EDV-Betreuung, DISK)
- Notfallregelungen (EDV-Betreuung, DISK)
- Bei größeren Verfahren ist die Erstellung von Betriebs- und Sicherheitskonzepten notwendig, welche u.a. umfassend die getroffenen Sicherheitsmaßnahmen sowie Vertretungs- und Notfallregelungen darstellen (EDV-Betreuung, DISK)
- Festlegung von Vertretungsregelungen, insbesondere im Administrationsbereich (Führungskräfte)

Für den Fall, dass personenbezogene Daten verarbeitet werden, ist in Abstimmung mit der* dem Datenschutzbeauftragten u.a. ein Verzeichnis der Verarbeitungstätigkeiten (VVT) zu erstellen.
Es dürfen ausschließlich dokumentierte Verfahren in einen Produktiv-/Regelbetrieb überführt werden.
Fragen zu Art und Umfang der Dokumentation sind an die*den Informationssicherheitsbeauftrage*n zu richten.

IT3.7 Organisation und Durchführung von Datensicherungen

Die Datensicherung muss nach einem angemessenen und dokumentierten Datensicherungskonzept erfolgen, das dem Schutzbedarf der zu sichernden Daten entspricht. Das Datensicherungskonzept umfasst mindestens:

- Umfang und Art der zu sichernden Daten
- Verantwortliche Personen
- Zugriffsberechtigte Personen
- Sicherungsmethode
- Sicherungsintervalle
- Anzahl der aufzubewahrenden Generationen / Speichermedien
- Ggf. Verschlüsselung der Datensicherung
- Lagerung bzw. Handhabung und Aufstellung der Sicherungsdatenträger

Die Sicherung von Daten muss in angemessenen Intervallen erfolgen. Auch System- und Programmdaten sind nach Veränderungen zu sichern. Zur Datensicherung sind geeignete Werkzeuge zu verwenden, die eine Datensicherung nach dem Generationenprinzip unterstützen.
Die Lesbarkeit der Datensicherung sollte regelmäßig überprüft werden. Die Wiedereinspielbarkeit der Daten muss mindestens einmal vollständig getestet worden sein und bedarf einer Überprüfung nach jeder Änderung des Sicherungsverfahrens.
Bei der Sicherung personenbezogener Daten sind die geforderten Aufbewahrungsfristen zu beachten.

IT3.8 Sicheres Löschen und Weitergabe von Datenträgern

Verlassen elektronische Datenträger und Speichermedien den dienstlichen Gebrauch, müssen sie entweder fachgerecht gelöscht oder entsorgt werden. Datenträger die nicht mehr benötigt werden, können im BITS entsorgt werden (Siehe Abschnitt B10 Entsorgung von Daten, Datenträgern und Dokumenten).
Für eine sichere Löschung reichen die Funktionen des Betriebssystems in der Regel nicht aus. Vielmehr ist je nach Speichermedium eine adäquate Löschmethode zu nutzen.
Sollen Datenträger mit personenbezogenen Daten durch externe Dienstleistende repariert werden, sind die Auftragnehmenden in Abstimmung mit der*dem Datenschutzbeauftragten vertraglich auf die Wahrung des Datenschutzes zu verpflichten.

IT4 Informationssicherheitsvorfälle

IT4.1 Notfall

Für Systeme mit einem hohen oder sehr hohen Schutzbedarf ist ein Maßnahmenplan zu erstellen, der festlegt, wie in einem Notfall adäquat reagiert werden kann. Dieser muss in Abhängigkeit vom IT-System mindestens folgende Aspekte betrachten:

- Verantwortlichkeiten
- Alarmierungsplan (Meldewege)
- Wiederanlaufplanung von IT-Systemen

- Wiederherstellung von Daten (Desaster Recovery)
- Einsatz von Ausweichlösungen (bspw. Ersatzhardware)

IT4.2 Meldung und Dokumentation von Informationssicherheitsvorfällen

Die EDV-Betreuung meldet Informationssicherheitsvorfälle umgehend an die zuständigen DISKs. Diese dokumentieren den Vorfall in Abstimmung mit der EDV-Betreuung und melden ihn der*dem Informationssicherheitsbeauftragten. Ist der*die DISK nicht erreichbar, übernimmt die EDV-Betreuung diese Aufgabe (melden und dokumentieren). Alles Weitere regelt die Richtlinie zur Handhabung von Informationssicherheitsvorfällen.

IT5 Netze

IT5.1 Netzmonitoring

Es müssen geeignete Maßnahmen getroffen werden, um Überlastungen und Störungen im Netzwerk frühzeitig erkennen und lokalisieren zu können.

IT5.2 Kommunikation zwischen Datennetzen

Die gesamte Kommunikation zwischen Datennetzen mit unterschiedlichen Sicherheitsniveaus und insbesondere mit dem Internet darf ausschließlich über kontrollierte Kanäle erfolgen, die durch geeignete Sicherheitsdienste (z.B. Sicherheitsgateway/Firewall) abgesichert werden.
Die Installation und der Betrieb anderer Kommunikationsverbindungen neben diesen Netzverbindungen, sind nicht gestattet. Sollte die Installation anderer Kommunikationswege auf Grund besonderer Umstände unumgänglich sein (z. B. zu Fernwartungszwecken), muss dies zuvor durch die IKM-Verantwortlichen in Abstimmung mit den DISKs genehmigt werden. Alle Zugriffe externer Personen sind zu protokollieren.