UNIVERSITÄT BIELEFELD

Informationssicherheitsbeauftragter

Basisschutzregelungen Informationssicherheit (BRI)

Maßnahmen Führungskräfte

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.

F1 Verantwortlichkeiten

Die Universitätsleitung ist gesamtverantwortlich für die Informationssicherheit an der Universität Bielefeld. In Fragen der Informationssicherheit wird die Universitätsleitung durch die*den Kanzler*in vertreten.
Die Verantwortung für die Informationssicherheit jeder Fakultät oder Einrichtung liegt bei der jeweiligen Leitung. Leitungskräfte auf jeder Ebene übernehmen eine Vorbildfunktion und etablieren in ihrem Bereich angemessene Maßnahmen und passen diese bei Bedarf an neue Gegebenheiten an. Ihnen obliegt hierfür die Verantwortung in technischer, organisatorischer und personeller Hinsicht.

F2 Technische und organisatorische Maßnahmen

F2.1 Revision der Informationssicherheitsmaßnahmen

Die Maßnahmen der Fakultäten und Einrichtungen zur Informationssicherheit sind regelmäßig auf ihre Angemessenheit und Aktualität zu überprüfen.
Die Verantwortung zur Durchführung der Revision liegt bei den Dekan*innen der Fakultäten bzw. der Leitung der Einrichtungen. Diese Revision kann an Beschäftigte delegiert werden, die Verantwortung nicht.

F2.2 Zugriffsberechtigungen

Beschäftigte erhalten nur auf die Daten und Dienste der Universität Zugriff, die für ihre Tätigkeiten erforderlich sind. Um welche Daten und Dienste es sich dabei handelt wird – sofern nicht automatisiert durch IT-Systeme vorausgewählt – von den jeweiligen Vorgesetzten oder der*den Prozess-/Verfahrensverantwortlichen definiert, genehmigt und von der verantwortlichen Administration umgesetzt.
Die zuständige EDV-Betreuung ist rechtzeitig über notwendige Änderungen oder den Entzug von Berechtigungen zu informieren, die z.B. durch Änderungen von Aufgaben zustande kommen.

F2.3 Verantwortlichkeiten IT-Verfahren und Rollentrennung

Für jedes IT-Verfahren sind verantwortliche Personen festzulegen. Eine Rollentrennung von operativen und kontrollierenden Funktionen ist sicherzustellen (zum Beispiel von Systemadministration und Verfahrensverantwortlichen).

F2.4 Grundsätze für die Einführung neuer IT-Verfahren

Bei der Einführung neuer IT-Verfahren ist eine Schutzbedarfsfeststellung zu erstellen und ggf. auch eine Risikoanalyse durchzuführen. Die Ergebnisse sind wie auch die getroffenen Sicherheitsmaßnahmen von den zuständigen Verfahrensverantwortlichen zu dokumentieren und einer regelmäßigen Revision zu unterziehen. Weitere Aspekte sind den Regelungen für das IT-Personal zu entnehmen.

Bei der Verarbeitung von Daten durch Dritte sind darüber hinaus weitere Regelungen zu beachten (siehe Abschnitt F2.5 Datenverarbeitung durch Dritte).
IT-Verfahren mit einem hohen oder sehr hohen Schutzbedarf benötigen des Weiteren einen Maßnahmenplan der festlegt, wie in einem Notfall adäquat reagiert werden kann.

F2.5 Dokumentation / Inventarisierung

In der IT ist eine angemessene und prüffähige Dokumentation und Inventarisierung zu etablieren. Dafür verantwortlich ist die EDV-Betreuung der einzelnen Bereiche.

F2.6 Datenverarbeitung durch Dritte

Werden externe Unternehmen mit IT-Dienstleistungen beauftragt, sind die Anforderungen der Informationssicherheit und des Datenschutzes zu beachten.

- Wird der Prozess durch die Beschaffungsabteilung der Universität Bielefeld unterstützt, werden die hierfür notwendigen Verträge dort abgeschlossen.
- Handelt es sich um einen Prozess, der ohne Unterstützung der Beschaffungsabteilung umgesetzt wird, hat die*der Verfahrensverantwortliche die Anforderungen des Datenschutzes und der Informationssicherheit zu beachten. Bei der Verarbeitung personenbezogener Daten muss ein Vertrag zur Auftragsverarbeitung abgeschlossen werden.

F3 Personalmaßnahmen

F3.1 Personalausstattung

Zur Erfüllung der Pflichten im Bereich Informationssicherheit ist auf eine angemessene Personalausstattung zu achten, insbesondere auch im Hinblick auf die Sicherstellung eines stabilen und sicheren Betriebs und angemessenen Vertretungsregelungen (siehe Abschnitt F3.4 Vertretungsregelungen).

F3.2 Qualifizierung des Personals

Die Führungskräfte stellen sicher, dass die Beschäftigten in Ihrem Bereich stets über die für sie geltenden Regelungen zur Informationssicherheit und zum Datenschutz informiert sind. Darüber hinaus ist sicherzustellen, dass diese durch eine regelmäßige Teilnahme an Schulungen bzw. Fortbildungen zum Thema Informationssicherheit und Datenschutz über einen für Ihren Arbeitskontext adäquaten Wissensstand verfügen.

F3.3 Einweisung und Beaufsichtigung von Fremdpersonal

Personen, die nicht zur jeweiligen IT-Organisation gehören, sind bei Arbeiten in Räumen mit hohem Schutzbedarf angemessen einzuweisen und soweit organisatorisch möglich auch zu beaufsichtigen. Arbeiten von externen Firmen sind darüber hinaus zu dokumentieren.

Wenn bei Arbeiten durch externe Dienstleister die Möglichkeit des Zugriffs auf personenbezogene Daten besteht, muss ein Vertrag zur Auftragsverarbeitung abgeschlossen werden.

F3.4 Vertretungsregelungen

Für kritische Betreuungs- und Administrationsfunktionen ist in der IT eine Abwesenheitsvertretung zu organisieren.
Es ist zu beachten, dass Vertretungen die notwendigen Tätigkeiten ausreichend beherrschen und ggf. auf schriftliche Arbeitsanweisungen zurückgreifen können. Die Vertretung sollte technisch so im System abgebildet sein, dass eine Weitergabe von Zugangsdaten nicht notwendig ist.
Bei der Auswahl der Vertretung ist zu beachten, dass die Rollentrennung nicht unterlaufen wird (siehe Abschnitt F2.2 Verantwortlichkeiten IT-Verfahren und Rollentrennung).

F3.5 Ausscheiden von Beschäftigten

Scheiden Beschäftigte aus dem Arbeitsverhältnis aus oder wechseln sie den Zuständigkeitsbereich, ist durch die verantwortlichen Führungskräfte sicherzustellen, dass das dafür zuständige Personal rechtzeitig informiert wird, um insbesondere folgende Maßnahmen in die Wege zu leiten:

- Ausgehändigte Schlüssel müssen an die ausgebende Stelle zurückgegeben werden.
- Zugangsrechte müssen entzogen bzw. neu vergeben werden.
- Es ist sicherzustellen, dass Daten, die nach dem Ausscheiden weiterhin in dem Bereich benötigt werden, geregelt an zuständige Personen übergegeben werden.
- Nach dem Ausscheiden unterliegen die sonstigen dienstlichen Daten der Aufbewahrungsrichtlinie der Uni Bielefeld.
- Sicherheitsrelevante Aufgaben und Funktionen müssen von anderem Personal weiter erfüllt werden. Eventuell ist eine Einweisung der nachfolgenden Person durch die ausscheidende Person notwendig.
- Es ist darauf hinzuweisen, dass Verschwiegenheitserklärungen auch nach dem Ausscheiden bestehen bleiben und dass die im Rahmen der Tätigkeit erhaltenen Informationen nicht weitergegeben werden dürfen.