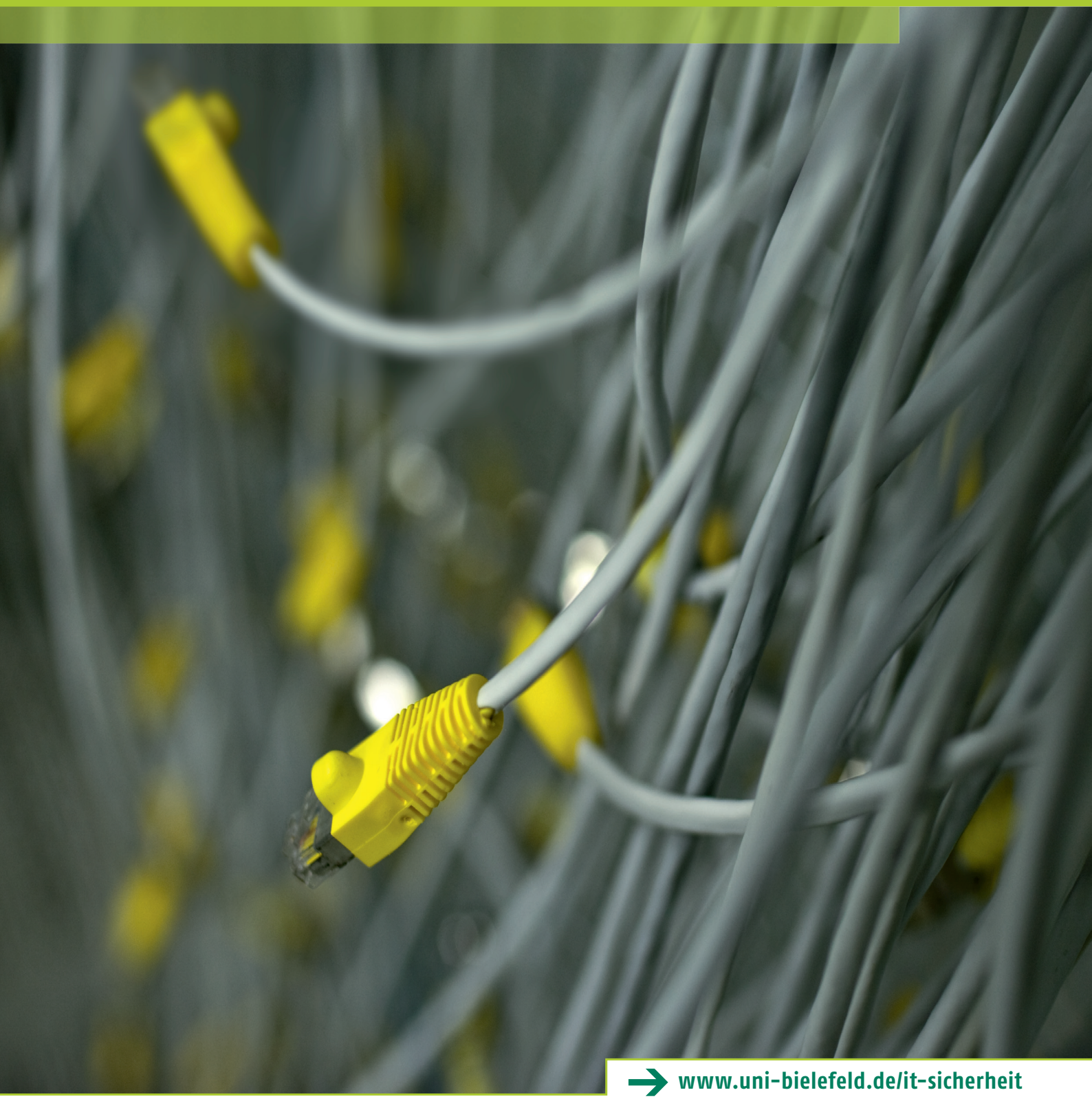
Universität Bielefeld IT-Sicherheit

Regelungen zum IT-Basisschutz
für IT-Personal



www.uni-bielefeld.de/it-sicherheit

Impressum

Herausgeber
Universität Bielefeld
Universitätsstr. 25
33615 Bielefeld

Redaktion
Michael Sundermeyer

Lektorat
Ann-Christin Kegler

Gestaltung
Peter Hoffmann

Stand
15.11.2011

Vorwort

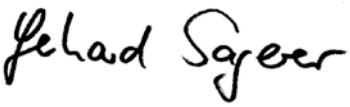
Sehr geehrte Mitarbeiterinnen und Mitarbeiter,

erfolgreiche Forschung und Lehre sowie die Arbeit in der Verwaltung sind auf eine zuverlässige und sichere Informationstechnik (IT) angewiesen. Aus diesem Grund wird das Thema IT-Sicherheit an der Universität Bielefeld seit vielen Jahren aktiv verfolgt. So hat das Rektorat bereits im Jahr 2002 auf die sich schnell verbreitenden Computerviren reagiert und verbindliche Maßnahmen zum Schutz von Computerarbeitsplätzen verabschiedet. Im Zuge dieser Entwicklung wurde 2006 die Position des IT-Sicherheitsbeauftragten geschaffen, die sich inhaltlich und organisatorisch um die Sicherherstellung und Weiterentwicklung des Themas kümmert. Seitdem wurden erfolgreich Strukturen geschaffen und Verfahren und Maßnahmen etabliert, um Integrität, Verfügbarkeit und Vertraulichkeit von Daten und Diensten sicherstellen zu können.

Mit der Verabschiedung des IT-Basisschutzes durch das Rektorat wird nun ein weiterer wichtiger Baustein für die Sicherheit der IT an der Universität Bielefeld in Kraft gesetzt. Die Regelungen bieten allen Mitarbeiterinnen und Mitarbeitern einen verbindlichen Rahmen zur sicheren Nutzung der IT.

Viele von Ihnen haben in den letzten Jahren auch persönlich Erfahrungen mit Spam-Mails, Viren und „Phishing“-Angriffen gemacht. Die konkreten Bedrohungen, die von Angriffen dieser Art ausgehen, verdeutlichen die Gefahren, die aus einer unsicheren oder sorglosen Nutzung der IT erwachsen können.
Es liegt auch an Ihnen als Mitarbeiterin und Mitarbeiter, durch einen verantwortungsvollen Umgang mit der IT, entscheidend zur Sicherheit Ihrer Daten und die der Universität Bielefeld beizutragen. Um diese Aufgabe erfüllen zu können ist es wichtig, bestehende Risiken zu (er)kennen und durch umsichtiges Handeln zu vermeiden. Dabei unterstützt Sie der IT-Basisschutz anhand von entsprechenden Maßnahmen und Empfehlungen.

Hans-Jürgen Simm
Kanzler der Universität Bielefeld



Prof. Dr.-Ing. Gerhard Sagerer
Rektor der Universität Bielefeld

Inhaltsverzeichnis

1. Regelungen zum IT-Basisschutz für IT-Personal

Die in dieser Richtlinie beschriebenen Regelungen sind ein verbindlicher Rahmen für alle Personen, die an der Universität Bielefeld Aufgaben bei der Betreuung der Informationstechnologie (IT) wahrnehmen.
Der „IT-Basisschutz für IT-Personal“ soll einen Rahmen für einen sicheren Umgang mit Informationstechnologie (IT) dienen. Als Mitarbeiterin und Mitarbeiter in der IT, haben Sie eine verantwortungsvolle Aufgabe, wenn es um den sicheren Umgang mit Daten geht. Dafür ist es wichtig zu wissen, und mit welchen Maßnahmen sie Risiken im Betrieb Wirkungsvoll begegnen können. Die Maßnahmen erkennen Sie jeweils an dem vorgestellten Buchstaben „M“.

1.1 Grundsätzliches

Die im Folgenden beschriebenen Maßnahmen gelten für alle Beschäftigten der Univerität Bielefeld, die Aufgaben im Bereich des IT-Betriebs wahrnehmen oder in diesem Zusammenhang Verantwortung in der Organisation tragen. Insbesondere sind dies Zuständige für Verfahren, System- und Netzadministration, Applikationsbetreuung, Benutzerservice, Programmentwicklung. Die dargestellten Maßnahmen des vorangegangenen Abschnitts für IT-Anwendende werden hier vorausgesetzt. Um eine verständliche und übersichtliche Darstellung zu erreichen, werden Maßnahmen teilweise wiederholt und weiter ausgeführt.
Bei bestimmten Aufgabenstellungen kann eine Abweichung in einzelnen Punkten der behandelten Maßnahmen notwendig sein. In jedem Fall sind diese zu dokumentieren und mit den jeweiligen IT-Beauftragten der Fakultät oder Einrichtung abzustimmen.

M 2.1 Grundsätze für den IT-Einsatz

Verantwortlich für Initiierung	→	**Hochschulleitung**
Verantwortlich für Umsetzung	→	**Bereichsleitung, IT-Beauftragte**

Beschaffung, Entwicklung und Einsatz von IT-Anwendungen (beispielsweise Software zur Textverarbeitung) und IT-Systemen (beispielsweise Server- und Speichersysteme oder mobile IT-Geräte) erfolgen nach Maßgabe der an der Universität Bielefeld geltenden Regelungen. Diese können bei der zentralen Beschaffungsabteilung in Erfahrung gebracht werden.

M 2.2 Gesamtverantwortlichkeit

Verantwortlich für Initiierung	→	**Hochschulleitung**
Verantwortlich für Umsetzung	→	**Bereichsleitung, IT-Beauftragte**

Die Verantwortung für die Umsetzung und Einhaltung der für den IT-Einsatz geltenden Regelungen tragen die Leitungen der einzelnen Bereiche (zum Beispiel Dekanate) in den Fakultäten und Einrichtungen und der

zentralen Universitätsverwaltung. Die Leitungen der Fakultäten und Einrichtungen stellen eine adäquate Ausstattung von Personalressourcen für die IT sicher.

1.2 Organisation der IT-Sicherheit

M 2.3 IT-Sicherheitsorganisation

Verantwortlich für Initiierung	→	**Hochschulleitung**
Verantwortlich für Umsetzung	→	**IT-Sicherheitsbeauftragte/r, SMT (Sicherheitsmanagement-Team)**

Die IT-Sicherheitsleitlinie der Universität regelt verbindlich den Aufbau der IT-Sicherheitsorganisation.

M 2.4 Dokumentation von IT-Verfahren

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Verfahrensverantwortliche**

IT-Verfahren[1] sind im Rahmen der IT-Sicherheit in folgenden Punkten zu dokumentieren:

- Zweck des IT-Verfahrens, Zielsetzung,
- Beschreibung der Arbeitsabläufe
- Schutzbedarfsfeststellung mit einer Bewertung auf Grundlage der in der Vorlage dargestellten Bewertungstabelle
- Durchführung einer Risikoanalyse in Abhängigkeit vom Ergebnis der Schutzbedarfsanalyse
- Beschreibung der Rollen; ggf. in Form eines Berechtigungskonzepts
- Festlegung von Vertretungsregelungen, insbesondere im Administrationsbereich
- Zugriffsrechte
- Organisation, Verantwortlichkeit und Durchführung der Datensicherung
- Notfallregelungen
- Ggf. Wartungsvereinbarungen

Für den Fall, dass personenbezogene Daten verarbeitet werden, ist in Abstimmung mit der oder dem Datenschutzbeauftragten eine Vorabkontrolle nach dem Datenschutzgesetz des Landes Nordrhein-Westfalen (DSG NRW) durchzuführen.

Ferner ist zu klären, inwieweit bei der Einführung eines IT-Verfahrens personalvertretungsrechtliche Regelungen zu berücksichtigen sind.

Es dürfen ausschließlich dokumentierte Verfahren in einen Produktivbetrieb/Regelbetrieb überführt werden. Das Verfahren ist produktiv, wenn die Gruppe der Nutzenden uneingeschränkten Zugriff auf das Verfahren hat. Die IT-Beauftragten sind verantwortlich für die Initiierung der Erstellung und Pflege der Dokumentation der IT-Verfahren ihrer Organisationseinheit. Die IT-Verfahrensverantwortlichen sind verantwortlich für die

[1] Siehe Glossar im Anhang

Umsetzung. Die Zuständigen für Systemadministration und Applikationsbetreuung sind zur Mitarbeit verpflichtet. Fragen zur Art und Umfang der Dokumentation sowie zu den IT-Verfahren sind an den oder die IT-Sicherheitsbeauftrage/n zu richten.

M 2.5 Rollentrennung

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Verfahrensverantwortliche, IT-Personal**

Für jedes IT-Verfahren sind verantwortliche Ansprechpersonen festzulegen. Es sollte eine Rollentrennung von operativen und kontrollierenden Funktionen erfolgen (zum Beispiel von IT-Verfahrensverantwortlichen und Systemadministration). Allen Beschäftigten müssen die ihnen übertragenen Verantwortlichkeiten und die sie betreffenden Regelungen bekannt sein. Abgrenzungen und Schnittmengen unterschiedlicher Rollen sind klar zu definieren.

M 2.6 Dokumentation von IT-Sicherheitsvorfällen

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Verfahrensverantwortliche, IT-Personal**

Zu IT-Sicherheitsvorfällen zählen beispielsweise Systemabstürze, Hardwareausfälle oder der unbefugte Zugriff auf Daten. Die Meldungen zu solchen Ereignissen sind an die Bereichs-IT-Sicherheitsbeauftragten (BITS) weiterzuleiten, welche diese dokumentieren und umgehend mit der oder dem IT-Sicherheitsbeauftragten abstimmen. Zuständig für die Meldung sind die Verantwortlichen, in deren Aufgabengebiet das Ereignis eingetreten ist. Beachten Sie auch die Regelungen zum Vorgehen bei IT-Sicherheitsvorfällen (siehe M 1.3).

M 2.7 Datenverarbeitung durch Dritte

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Verfahrensverantwortliche**

Eine schriftliche Vereinbarung ist Voraussetzung für alle im Auftrag der Universität Bielefeld durch Dritte verarbeiteten Daten. Sofern personenbezogene Daten verarbeitet werden, sind die Regelungen zur Datenverarbeitung im Auftrag des Datenschutzgesetzes NRW (DSG NRW) zu beachten. Ferner haben die Dienstleister die für sie geltenden Regelungen zum IT-Basisschutz zu akzeptieren.

M 2.08 Zentrale Serviceleistungen

Verantwortlich für Initiierung	→	**Hochschulleitung**
Verantwortlich für Umsetzung	→	**IT-Dienstleister**

Ein leistungsfähiger Nutzerservice, zentral gesteuerte Datensicherungsmaßnahmen, die Möglichkeit der Ablage von Daten auf zentrale Fileservern sowie die Möglichkeit der abgesicherten Ausführung von Programmen auf Applikationsservern sind wesentliche Voraussetzungen für einen sicheren und reibungslosen IT-Einsatz zur Unterstützung der täglichen Arbeitsprozesse.
Die Software-Verteilung inkl. -installation und -inventarisierung sollte mit Unterstützung entsprechender Werkzeuge erfolgen. Beim Einsatz von im Netzwerk operierender Installations- und Inventarisierungswerkzeuge sind besondere Maßnahmen zum Schutz vor Missbrauch zu ergreifen. Der nutzbare Funktionsumfang der Werkzeuge ist für den Bereich festzulegen und mit den Verantwortlichen für den Netzwerkbetrieb abzustimmen.
Es muss u. a. festgelegt sein, dass die Werkzeuge nur auf dafür bestimmten, besonders abgesicherten Arbeitsplätzen eingesetzt werden. Der Personenkreis, der berechtigt ist, diese Werkzeuge zu nutzen, ist auf das notwendige Maß zu beschränken. Die Anwenderinnen und Anwender sind vor dem Einsatz solcher Werkzeuge zu informieren. Ihr Einsatz muss nachvollziehbar protokolliert und ihr Verwendungszweck dokumentiert werden.

M 2.09 Revision der IT-Sicherheitsmaßnahmen

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal, BITS (Bereichs-IT-Sicherheitsbeauftragte)**

Die Maßnahmen zur IT-Sicherheit sind regelmäßig sowie nach Änderungen des Regelwerks zur IT-Sicherheit auf ihre Angemessenheit und funktionsfähigkeit zu überprüfen. Dies kann von den IT-Bereichen der Universität Bielefeld selbst oder durch externe Dienstleistende durchgeführt werden. Bei der Vergabe dieser Tätigkeit an externe Auftragsnehmerinnen und -nehmer ist besonderer Wert auf deren Seriosität zu legen. In diesem Zusammenhang sollte beispielsweise auf eine unabhängige Zertifizierung der Angebote (beispielsweise BSI bzw. ISO 27001) oder aussagekräftige Referenzen Wert gelegt werden.

M 2.10 Notfallvorsorge

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Verfahrensverantwortliche, IT-Personal**

Bei der Einführung neuer IT-Verfahren werden im Rahmen der Dokumentationspflichten Analysen zur Ermittlung des Schutzbedarfs und ggf. eine Risikoanalyse zur Identifizierung und Begegnung spezifischer Risiken vorgenommen. Basierend auf diesen Erkenntnissen sollte ein Notfallplan erstellt werden, in dem

festgelegt wird, wie auf Notfallsituationen[2] adäquat reagiert werden muss. Dieser sollte insbesondere Regelungen zu Verantwortlichkeiten, zum Wiederanlauf von IT-Systemen, zur Wiederherstellung von Daten sowie zum Einsatz von Ausweichlösungen wie beispielsweise Ersatzhardware enthalten. Darüber hinaus ist es sinnvoll einen Alarmierungsplan zu erstellen, in dem die Meldewege im Notfall beschrieben werden.

1.3 Personelle Maßnahmen

Zahlreiche Untersuchungen und Statistiken über Probleme im IT-Bereich zeigen, dass die größten Risiken durch Irrtum, menschliches Versagen und Überforderung der Mitarbeiterinnen und Mitarbeiter entstehen.

M 2.11 Personalauswahl

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**Bereichsleitung**

Mit Administrationsaufgaben auf Netzwerk- und Systemebene sind ausgewählte, ausreichend qualifizierte, vertrauenswürdige und motivierte Beschäftigte zu betrauen.

M 2.12 Personalausstattung

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**Bereichsleitung**

Zur Erfüllung der Pflichten im Bereich Administration und IT-Sicherheit ist auf eine angemessene Personalausstattung zu achten, insbesondere im Hinblick auf die Sicherstellung eines kontinuierlichen Betriebs und entsprechender Vertretungsregelungen.

M 2.13 Vertretungsregelungen

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**Bereichsleitung**

Für alle Betreuungs- und Administrationsfunktionen in der IT ist die Vertretungsfrage zu regeln. Vertretungen müssen die notwendigen Tätigkeiten ausreichend beherrschen und ggf. auf schriftliche Arbeitsanweisungen und Dokumentationen zurückgreifen können. Die Vertretungsregelung sollte technisch so im System abgebildet sein, dass eine Weitergabe von Zugangsdaten nicht notwendig ist. Eine Ausnahme bilden systemspezifische, nicht personenunabhängige Kennungen (zum Beispiel „root“ bei UNIX-Systemen). Dort

[2] Siehe Glossar im Anhang

soll die Vertretung nur im Bedarfsfall nachvollziehbar auf das an geeigneter Stelle hinterlegte Passwort zurückgreifen können.
Die Voraussetzungen für die Wahrnehmung einer Vertretung sollten möglichst so eingerichtet sein, dass sie im Bedarfsfall sofort zum tragen kommen.
Bei der Auswahl der Vertretung ist zu beachten, dass die Rollentrennung nicht unterlaufen wird (siehe M 2.5).

M 2.14 Qualifizierung des Personals

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**Bereichsleitung**

Eine ausreichende Schulung ist unabdingbar, bevor das IT-Personal mit einem IT-Verfahren arbeiten kann. Dazu gehören ebenfalls Erläuterungen zu den für sie geltenden Sicherheitsmaßnahmen, zu den rechtlichen Rahmenbedingungen sowie ggf. zu den Erfordernissen des Datenschutzes. Durch die Verantwortlichen ist sicherzustellen, dass die angemessene Fortbildung des IT-Personals in allen ihr Aufgabengebiet betreffenden Belangen regelmäßig erfolgt.

1.4 Sicherung der Infrastruktur

M 2.15 Geeignete Aufstellung von IT-Systemen

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal**

Alle IT-Systeme, die typische Serverfunktion erfüllen, einschließlich der Peripheriegeräte (Konsolen, externe Platten, Laufwerke u. ä.), sind in separaten, besonders gesicherten Räumen oder in nicht öffentlich zugänglichen Bereichen verschlossen aufzustellen. Gleiches gilt für die Netzwerkinfrastruktur (Switches, Router, Hubs u. ä.).

M 2.16 Sicherung von Räumen

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal, Dezernat FM**

Der Zutritt Unbefugter zu Räumen mit IT-Infrastruktur muss durch angemessene Maßnahmen zuverlässig verhindert werden. Je nach der Schutzbedarf der betriebenen Verfahren sowie in Abhängigkeit von äußeren Bedingungen (öffentlicher zugänglicher Bereich, Lage zur Straße usw.) sind besondere bauliche

Maßnahmen, wie zum Beispiel einbruchsichere Fenster, einbruchsichere Türen, Bewegungsmelder o. ä. zur Verhinderung von gewaltsamen Eindringen vorzusehen.
Die Türen von Serverräumen dürfen nur durch geeignete Schließsysteme zu öffnen sein und sollen selbsttätig schließen; gegebenenfalls verwendete Schlüssel müssen kopiergeschützt sein. Für die Schlüsselverwaltung sind besondere Regelungen erforderlich, die eine Herausgabe an Unbefugte ausschließen.
Der Zutritt ist auf diejenigen Personen zu begrenzen, deren Arbeitsaufgaben dies erfordert. Reinigungspersonal soll die Serverräume nach Möglichkeit nur unter Aufsicht bzw. zu festgelegten Zeitpunkten betreten. Die Schließberechtigung für Räume ist entsprechend nachvollziehbar zu dokumentieren. Ausnahmen von diesen Regelungen sind mit den Bereichs-IT-Sicherheitsbeauftragten (BITS) abzustimmen und durch die IT-Beauftragten des Bereichs schriftlich zu erteilen und zu dokumentieren.

M 2.17 Verkabelung

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Dienstleistende, IT-Personal, Dezernat FM**

Die Verkabelung des LAN ist soweit technisch möglich klar zu strukturieren sowie aktuell und vollständig zu dokumentieren. Die Netzwerkadministration muss einen vollständigen Überblick über die Kabelverlegung und die Anschlussbelegung zentraler Komponenten haben. Nicht benutzte Netzwerkzugänge sind durch die IT-Betreuung der einzelnen Bereiche zeitnah zu deaktivieren. Bei der Verlegung der Kabel muss darauf geachtet werden, dass Unbefugte keine Möglichkeit des Zugriffs haben. Offen zugänglich verlegte Kabel sollten in Zusammenarbeit mit der für Baumaßnahmen zuständigen Stelle in geeigneter Weise geschützt werden. Erweiterungen und Veränderungen an der Gebäudeverkabelung sind mit den IT-Beauftragten der Bereiche und dem Dezernat Facility Managemement (FM) abzustimmen.

M 2.18 Einweisung und Beaufsichtigung von Fremdpersonal

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal, IT-Dienstleistende**

Fremde Personen, die in gesicherten IT-Räumen (z. B. Serverräume) Arbeiten ausführen müssen, sind einzuweisen und in der Regel zu beaufsichtigen. Personen, die nicht unmittelbar zum IT-Bereich zu zählen sind, aber Zugang zu gesicherten IT-Räumen benötigen, müssen über den Umgang mit IT belehrt werden.
Wenn bei Arbeiten durch externe Firmen, zum Beispiel im Rahmen der Fernwartung, die Möglichkeit des Zugriffs auf personenbezogene Daten besteht, müssen diese Personen gemäß dem Datenschutzgesetz NRW verpflichtet sein. Für die Wartung und Instandhaltung sind Verträge zur Datenverarbeitung im Auftrag zu schließen. Alle Arbeiten, die von externen Firmen durchgeführt werden, sind zu protokollieren.

M 2.19 Unterbrechungsfreie Stromversorgung und Überspannungsschutz

Verantwortlich für Initiierung	→	**IT-Beauftragte, IT-Verfahrensverantwortliche**
Verantwortlich für Umsetzung	→	**IT-Dienstleistende, IT-Personal, Dezernat FM**

IT-Systeme mit hohen Anforderungen an Integrität und Verfügbarkeit, sind an einer ausreichend dimensionierten und gegen Überspannungen abgesicherte Stromversorgung zu betreiben. Eine entsprechende Versorgung ist in Zusammenarbeit mit dem Dezernat FM herzustellen. Die Konfiguration der USV und der durch sie geschützten Systeme muss mindestens ein rechtzeitiges und kontrolliertes Herunterfahren der Systeme sicherstellen. Bei einem Einsatz von Geräten mit redundant ausgelegter Stromversorgung ist darauf zu achten, dass die einzelnen Netzteile über getrennt abgesicherte Stromkreise versorgt werden. Die für den Betrieb von IT notwendigen Unterlagen und Informationen zur elektrischen Versorgung sind den IT-Beauftragten der Bereiche auf Anfrage durch die IT-Dienstleistenden bzw. das Dezernat FM zur Verfügung zu stellen.

M 2.20 Brandschutz

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal, Sicherheitsbeauftragte (Arbeitssicherheit), Dezernat FM**

Die Regeln des vorbeugenden Brandschutzes sind zu beachten und einzuhalten. Insbesondere gilt dies für IT-Räume, wie beispielsweise Technik- oder Serverräume. Für Hinweise und eingehende Beratung wenden Sie sich an die oder den Brandschutzbeauftragte/n ihres Bereiches.

M 2.21 Schutz vor Wasserschäden

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal, Dezernat FM**

IT-Systeme sind nicht in direkter Nähe von oder unter wasserführenden Leitungen aufzustellen. 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.

M 2.22 Klimatisierung

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal, Dezernat FM**

Die Einhaltung der zulässigen Betriebstemperatur von IT-Räumen ist durch den reibungslosen Einsatz von ausreichend dimensionierten Klimatisierungsgeräten herzustellen. Eine fachgerechte Aufstellung und Wartung der Geräte durch das Dezernat FM ist sicherzustellen.

1.5 Hard- und Software-Einsatz

M 2.23 Beschaffung, Software-Entwicklung

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal**

Grundsätzlich ist die Beschaffung von Soft- und Hardware mit den zuständigen IT-Beauftragten und der oder dem IT-Sicherheitsbeauftragten abzustimmen. Diese sind für die Einhaltung von Standards bzw. Sicherheitsanforderungen verantwortlich.
Bei der Entwicklung von Software sind die fachlichen und technischen Anforderungen im Vorfeld zu spezifizieren. Diese Arbeiten sollten in enger Abstimmung mit den betroffenen Organisationseinheiten durchgeführt werden. Des Weiteren sind bei der Umsetzung bewährte Prinzipien wie der Einsatz einer integrierten Entwicklungsumgebung, Software-Tests und Dokumentation sowie Code Review zu Berücksichtigen.

M 2.24 Kontrollierter Einsatz von Software

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal**

IT-Systeme sind soweit möglich gegen eine unbefugte Installation von Software zu schützen. Auf IT-Systemen der Universität Bielefeld darf nur Software installiert werden, die grundsätzlich durch die IT-Beauftragten der Bereiche freigegeben wurde. Bei der Freigabe sollte insbesondere darauf geachtet werden, dass die Software aus zuverlässiger Quelle stammt und ihr Einsatz notwendig ist. Das eigenmächtige Einspielen, insbesondere auch von aus dem Internet heruntergelandener Software, ist nur gestattet, wenn eine Genehmigung der IT-Beauftragten vorliegt oder die Leitung der Organisationseinheit eine pauschale Freigabe für Teilbereiche festgelegt hat.

M 2.25 Entwicklung von Software nach standardisierten Verfahren

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal**

Software-Entwicklungen, die auf Grund ihrer Größenordnung Projektcharakter haben, müssen nach standardisierten Verfahren (Vorgehensmodelle) und nach Maßgabe der für die Universität geltenden Regelungen (u. a. ein klar umrissenes Projektmanagement und eine Qualitätssicherung) durchgeführt werden.

M 2.26 Separate Entwicklungsumgebung

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal**

Entwicklung, Tests oder Anpassung von Software darf in der Regel nur mit Daten erfolgen, die keinen Personenbezug haben (anonymisierte Daten). Die Überführung der Software von der Entwicklung in den Produktivbetrieb bedarf der Freigabe durch die jeweils zuständigen IT-Beauftragten.

M 2.27 Software testen

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal**

Vor dem Einsatz neuer Software oder neuer Versionen muss die Erfüllung der Spezifikation durch hinreichende Tests sichergestellt sein. Der Testverlauf und das Testergebnis sind zu dokumentieren.

M 2.28 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates / Malwareschutz

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal**

Um bekannte Schwachstellen in Software-Produkten und Hardware-Komponenten vor potentiellen Angriffen zu schützen, sind Patche und Updates der Hersteller in Abhängigkeit von ihrer Kritikalität schnellstmöglich zu installieren. Neben dem Betriebssystem sind auch sämtliche Applikationen (einschließlich ihrer Erweiterungen) und Treiber stets aktuell zu halten. Das verantwortliche IT-Personal sollte sich regelmäßig über bekannt gewordene Software-Schwachstellen informieren.
Grundsätzlich ist der Betrieb von IT-Systemen an der IT-Infrastruktur der Universität ohne angemessene Basisschutz-Maßnahmen wie Virenscanner, Firewall und aktuelle Software- und Betriebssystemversionen nicht gestattet. Ausnahmen von dieser Regelung sind mit den Bereichs-IT-Sicherheitsbeauftragten abzustimmen und zu dokumentieren.
Jede Organisationseinheit ist verpflichtet, entsprechende Schutzsoftware anzubieten. Beachten Sie auch die Regelungen zur Dokumentation von IT-Sicherheitsvorfällen (siehe M 2.6).

M 2.29 Dokumentation von IT-Systemen

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal**

Zu jedem IT-System bzw. IT-Verfahren ist eine Dokumentation zu führen. Üblicherweise werden einzelne Systeme, Server oder PCs nicht gesondert dokumentiert, sondern zu größeren Gruppen zusammengefasst. Die Dokumentation sollte Informationen wie den Aufstellungsort, Informationen zur Hard- und Software-Ausstattung enthalten. Darüber hinaus sind Angaben zur Hard- und Software-Konfiguration, zu durchgeführten Reparaturarbeiten, aufgetretenen Problemen, Suche nach Schadprogrammen, Verantwortlichkeiten sowie zur Datensicherung (Umfang, Verfahren, Rhythmus usw.) zu dokumentieren. Weitere Punkte sind dem Abschnitt M 2.4 zu entnehmen.

M 2.30 Ausfallsicherheit

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal**

Maßnahmen zur Ausfallsicherheit der IT-Systeme sind entsprechend den Anforderung an ihre Verfügbarkeit umzusetzen. Alle IT-Systeme, die wichtige oder unverzichtbar für eine Aufrechterhaltung eines geordneten Betriebes sind, müssen durch Ausweichlösungen (redundante Geräteauslegung oder Übernahme durch gleichartige Geräte mit leicht verminderter Leistung) oder Wartungsverträge mit kurzen Reaktionszeiten hinreichend verfügbar gehalten werden.

M 2.31 Einsatz von mobilen IT-Geräten

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal**

Die Nutzung von mobilen IT-Geräten stellt ein Risiko für die Daten und die IT-Infrastruktur dar. Ihre hohe Mobilität macht eine Malwareinfektion, einen Verlust oder Diebstahls wahrscheinlicher als bei herkömmlichen IT-Geräten. Mobile IT-Geräte müssen durch angemessene Maßnahmen gegen Verlust, Manipulation und unberechtigte Einsichtnahme geschützt werden. Insbesondere sind:

- die Verwaltung, Wartung und Weitergabe der Geräte durch die einzelnen Bereiche eindeutig zu regeln
- sensiblen Daten auf den Geräten gegen unbefugten Zugriff zu schützen, beispielsweise Notebooks durch eine Verschlüsselungsfunktion, Smartphones durch eine PIN und Fernlöschmöglichkeiten
- die Geräte gegen Diebstahl zu schützen, beispielsweise Notebooks durch ein Kensington-Lock das den IT-Anwendeden zusammen mit dem Gerät ausgehändigt wird
- Dienste wie W-LAN oder Bluetooth sollten nach Möglichkeit hardwareseitig deaktivierbar sein.

Darüber hinaus muss insbesondere durch die Umsetzung der Regelungen unter M 2.28 sichergestellt werden, dass durch solche Geräte keine Gefährdungen für andere IT-Systeme und Netze ausgehen.

Bei der Übergabe von mobilen IT-Geräten sind die IT-Anwendenden für die Risiken zu sensibilisieren und über ihre Pflichten bei der Nutzung aufzuklären.

1.6 Zugriffsschutz

In der Regel ist der Zugang zum Netz verbunden mit dem potentiellen Zugriff auf Daten, Anwendungsprogramme und weitere Ressourcen.
Es sollten nur die Personen Zugang zu dem Netz und die damit verfügbaren Ressourcen der Universität Bielefeld erhalten, die diese für ihre Arbeit benötigen und zuvor die Erlaubnis zur Nutzung von den dafür zuständigen Stellen erhalten haben. Daher kommt der Authentisierung eine besondere Bedeutung zu.

M 2.32 Bereitstellung von Verschlüsselungssystemen

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Dienstleistende, IT-Personal**

Zur Absicherung besonders schützenswerter Daten, insbesondere auf mobilen IT-Systemen, sind geeignete Verschlüsselungslösungen (Programme oder spezielle Hardware) durch die IT-Dienstleistenden bereitzustellen.

M 2.33 Netzzugänge

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal**

Der Anschluss von 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. Eine Nutzung von zusätzlichen Verbindungsmöglichkeiten ist nicht gestattet. Dazu zählen auch:

- Einrichtung und Betrieb von eigenen Wireless-LAN Access Points am Netz der Universität
- Einrichtung und Betrieb eigener DSL-Anschlüsse, eines Modems oder anderer Zugangsmechanismen, die an das Netz der Universität angeschlossen werden und so eine Verbindung zwischen zwei Netzen herstellen können.

Ausnahmen von dieser Regelung bedürfen der Zustimmung der zuständigen IT-Beauftragten und des Hochschulrechenzentrums. Maßnahmen oder Geräte, die Störungen des Betriebs verursachen, sind nach Aufforderung unverzüglich zu beseitigen.

M 2.34 Personenbezogene Kennungen (Authentisierung)

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal**

Alle IT-Systeme und Anwendungen sind so einzurichten, dass nur berechtigte Benutzerinnen und Benutzer die Möglichkeit haben, mit ihnen zu arbeiten. Infolgedessen ist mindestens eine Anmeldung mit Benutzerkennung und Passwort erforderlich. Die Vergabe von Benutzerkennungen für die Arbeit an IT-Systemen soll in der Regel personenbezogen erfolgen. Die Arbeit unter der Kennung einer anderen Person ist unzulässig. Ebenfalls ist eine Weitergabe von Kennungen und Passwörter untersagt.
Redundanzen bei der Benutzerverwaltung sind zu vermeiden. Die Zuordnung von mehreren Kennungen zu einer Person innerhalb eines IT-Systems sollte nur in begründeten Ausnahmefällen erlaubt sein, wie beispielsweise für die Systemadministration. Die Einrichtung und Freigabe von Benutzerkennungen und Zugriffsberechtigungen dürfen nur in einem geregelten Verfahren erfolgen. Diese sind zu dokumentieren.

M 2.35 Zugriffsrechte

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Dienstleistende, IT-Personal**

Über Zugriffsrechte wird geregelt, welche Person im Rahmen ihrer Funktionen die Berechtigung hat, IT-Systeme, IT-Anwendungen oder Daten zu nutzen. IT-Anwendende sind nur mit den Zugriffsrechten auszustatten, die sie unmittelbar für die Erledigung ihrer Aufgaben benötigen (Prinzip der kleinstmöglichen Berechtigungen). Die Vergabe bzw. Änderung und der Entzug von Zugriffsrechten ist verbindlich zu regeln und schriftlich zu dokumentieren.
Im organisatorischen Ablauf muss zuverlässig verankert werden, dass das zuständige IT-Personal über die notwendige Änderung der Berechtigungen von IT-Anwendenden, z. B. in Folge von Änderungen der Aufgaben, rechtzeitig informiert wird, um die Berechtigungsänderungen im System abzubilden und zu dokumentieren.

M 2.36 Administrative Accounts

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal**

Das Verwenden von Benutzerkennungen mit weitreichenden Administrationsrechten ist ebenfalls auf die für die Aufgabenerfüllung notwendigen Rechte zu beschränken (Prinzip der kleinstmöglichen Berechtigungen). Die Administration erhält für diese Aufgaben eine persönliche Kennung. Für alltägliche Arbeiten, die ohne diese Berechtigungen auskommen, ist die Standard-Kennung zu verwenden.

M 2.37 Ausscheiden von Beschäftigten

Verantwortlich für Initiierung	→	**Bereichsleitung**
Verantwortlich für Umsetzung	→	**Vorgesetzte, IT-Personal**

Im organisatorischen Ablauf muss zuverlässig verankert sein, wie die zuständigen IT-Beauftragten bzw. Verfahrensverantwortlichen rechtzeitig über das Ausscheiden oder den Wechsel von Beschäftigten informiert werden. Die zuständige Organisationseinheit der Betroffenen hat über die Verwendung der dienstlichen Daten zu entscheiden, die der Kennung der ausscheidenden IT-Anwendenden zugeordnet sind. Vor dem Ausscheiden sind sämtliche interne Unterlagen, die vertrauliche Angaben enthalten sowie ausgehändigte Schlüssel zurück zu fordern. Darüber hinaus sind direkt nach dem Ende des Beschäftigungsverhältnisses sämtliche eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Sollen in Ausnahmefällen Zugangsberechtigungen begründet bestehen bleiben, sind diese durch die IT-Beauftragten zu genehmigen und durch die IT-Betreuung nachvollziehbar zu dokumentieren. Wurde in Ausnahmefällen eine Zugangsberechtigung zu einem IT-System zwischen mehreren Personen geteilt, so ist nach dem Ausscheiden einer der Personen die Zugangsberechtigung zu ändern.
Eine Weiterführung von sicherheitsrelevanten Aufgaben und Funktionen muss auch nach dem Ausscheiden weiter gewährleistet bleiben. Vor dem Ausscheiden ist die Einweisung möglicher nachfolgender Personen sicherzustellen. IT-Anwendende sollten darüber hinaus noch einmal explizit darauf hingewiesen werden, dass Verschwiegenheitserklärungen auch nach dem Ausscheiden in Kraft bleiben und keine während der Arbeit erhaltenen Informationen weitergegeben werden dürfen.

M 2.38 Gebrauch von Passwörtern

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal, IT-Anwendende**

Werden in einem IT-System Passwörter zur Authentisierung gebraucht, so ist die Sicherheit der Zugangs- und Zugriffsrechteverwaltung des Systems entscheidend davon abhängig, dass das Passwort richtig benutzt wird.

Sofern technisch möglich, sollte durch die IT folgende Randbedingungen eingehalten werden:

- Die Wahl von Trivialpasswörtern ("QWERTZAS", "123456") sollte verhindert werden.
- Benutzerinnen und Benutzer müssen ihr eigenes Passwort jederzeit ändern können.
- Für die Erstanmeldung sollten Einmalpasswörter vergeben werden, also Passwörter, die nach einmaligem Gebrauch gewechselt werden müssen. Nach mehrfacher fehlerhafter Passworteingabe muss eine Sperrung erfolgen, die nur durch eine autorisierte Stelle aufgehoben werden kann oder nach Ablauf einer ausreichenden Sperrfrist automatisch aufgehoben wird.
- Bei der Authentisierung in vernetzten Systemen sollten Passwörter nicht unverschlüsselt übertragen werden.
- Bei der Eingabe sollte das Passwort nicht im Klartext auf dem Bildschirm einsehbar sein.
- Anmeldeversuche sollten nach einer bestimmten Anzahl von Fehlversuchen automatisiert unterbunden werden, beispielsweise durch eine Sperre.

- Die Passwörter sollten im System zugriffssicher gespeichert werden, beispielsweise durch den Einsatz einer Einwegverschlüsselung.
- Der Passwortwechsel sollte vom System regelmäßig initiiert werden, als Richtwert gelten mindestens alle 360 Tage. Die wiederholte Nutzung alter Passwörter beim Passwortwechsel sollte vom IT-System verhindert werden.
- Eine Zurücksetzung des Passwortes durch die Administration sollte ausschließlich mit einem Initialkennwort erfolgen, dass die empfangende Person bei der ersten Anmeldung zwingend ändern muss.
- Bei der Zurücksetzung eines Passwortes ist ein ausreichend sicheres Verfahren zur Verifikation der Identität der Benutzerinnen und Benutzer und zur Übermittlung des neuen initialen Kennwortes zu verwenden.

Auf die Einhaltung der Regeln ist insbesondere zu achten, wenn das System diese nicht erzwingt.

M 2.39 Sperre bei Inaktivität

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal**

Soweit es technisch möglich ist, sollten IT-Systeme so konfiguriert sein, dass sie nach längerer Inaktivität (beispielsweise 10 Minuten) automatisch gesperrt und nur nach erneuter Eingabe eines Passwortes wieder genutzt werden können.

1.7 System- und Netzwerkmanagement

Eine angemessene Protokollierung und regelmäßige Audits und Revisionen sind wesentliche Faktoren der System- und Netzsicherheit. Eine Auswertung solcher Protokolle mit geeigneten Hilfsmitteln erlaubt beispielsweise die Erkennung von systematischen Angriffen auf das Netz.
Protokolle dienen dem Erkennen und Beheben von Fehlern. Je nach Schutzbedarf des Verfahrens müssen adäquate Maßnahmen zur Protokollierung getroffen werden, um feststellen zu können, wer wann welche Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit). Für die Verarbeitung personenbezogener Daten ist dies gesetzlich vorgeschrieben. Darüber hinaus sollte eine Protokollierung insbesondere auch sicherheitsrelevante Ereignisse betrachtet. Bei einem Audit werden die Ereignisse mit Hilfe geeigneter Werkzeuge betrachtet und ausgewertet.
Bei der Revision werden die beim (Offline-) Audit gesammelten Daten von einer oder mehreren unabhängigen Personen (4-Augen-Prinzip) überprüft, um Unregelmäßigkeiten beim Betrieb der IT-Systeme aufzudecken.

M 2.40 Protokollierung

Verantwortlich für Initiierung	→	IT-Beauftragte
Verantwortlich für Umsetzung	→	IT-Personal

Abhängig von den technischen Möglichkeiten des IT-Systems sind wichtige Ereignisse wie beispielsweise erfolglose Zugriffsversuche oder das Ändern wichtiger Systemparameter automatisch personenbezogen zu protokollieren. Abhängig von den Anforderungen kann eine Protokollierung auch auf definierte kritische (sicherheitsrelevante) Ereignisse eingeschränkt werden.
Die Protokolle sollten regelmäßig und zeitnah ausgewertet werden. Es ist sicher zu stellen, dass nur die Personen Zugriff auf die Protokolle erlangen können, die dies für ihre Aufgabenerfüllung zwingend benötigen und dafür von der zuständigen Stelle mit den nötigen Rechten ausgestattet wurden. Das Prinzip der Zweckbindung und der Datensparsamkeit nach DSG NRW ist zu beachten.
Die Tätigkeiten der Administration sind je nach Schutzbedarf des Verfahrens bzw. der zu verarbeitenden Daten zu protokollieren.

1.8 Kommunikationssicherheit

Für einen angemessenen Schutz der IT-Infrastruktur der Universität muss der Kommunikation zwischen Bereichen mit unterschiedlichem Schutzbedarf ein besonderes Augenmerk gelten. Die IT-Nutzerschaft der Universität sollte regelmäßig für die besonderen Risken und Gefahren der elektronischen Kommunikation und der Datenübermittlung sensibilisiert werden.

M 2.41 Sichere Netzwerkadministration

Verantwortlich für Initiierung	→	IT-Beauftragte
Verantwortlich für Umsetzung	→	IT-Personal

Anhand von technischen und organisatorischen Maßnahmen muss sichergestellt werden, dass die Administration des lokalen Netzwerks nur von dem dafür vorgesehenen Personal durchgeführt wird. Aktive und passive Netzkomponenten sowie Server und die dazugehörige Dokumentation sind vor dem Zugriff Unbefugter zu schützen.

M 2.42 Netzmonitoring

Verantwortlich für Initiierung	→	IT-Beauftragte
Verantwortlich für Umsetzung	→	IT-Personal

Es müssen geeignete Maßnahmen getroffen werden, um Überlastungen und Störungen im Netzwerk frühzeitig zu erkennen und zu lokalisieren. Darüber hinaus muss sichergestellt werden, dass auf die für diesen Zweck eingesetzten Werkzeuge nur die dazu befugten Personen zugreifen können.

M 2.43 Deaktivierung nicht benötigter Netzwerkzugänge

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal**

Nicht benötigte Netzwerkzugänge sind zu deaktivieren, um einen unbefugten Zugang zum Netz der Universität zu erschweren.

M 2.44 Kommunikation zwischen unterschiedlichen Sicherheitsniveaus

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal, IT-Dienstleistende**

Die gesamte Kommunikation zwischen Bereichen mit unterschiedlichem Schutzbedarf oder mit externen Personen und Einrichtungen darf ausschließlich über kontrollierte und abgesicherte Kanäle erfolgen. Die Installation und der Betrieb anderer Kommunikationsverbindungen neben den Netzverbindungen der Universität Bielefeld sind nicht gestattet. Sollte die Installation anderer Kommunikationswege auf Grund besonderer Umstände unumgänglich sein (z. B. zu Fernwartungszwecken), muss diese zuvor durch die IT-Beauftragten genehmigt und mit dem HRZ abgestimmt werden. Alle Zugriffe externer Personen sind zu protokollieren.

1.9 Datensicherung

M 2.45 Organisation der Datensicherung

Verantwortlich für Initiierung	→	**IT-Beauftragte, IT-Verfahrensverantwortliche**
Verantwortlich für Umsetzung	→	**IT-Personal**

Die Datensicherung muss auf Basis eines dokumentierten, dem Schutzbedarf der Daten angemessenen Datensicherungskonzepts erfolgen. Im Falle personenbezogener Daten sind in Abstimmung mit der oder dem Datenschutzbeauftraten die geforderten Mindest- bzw. Höchstzeiträume laut den gesetzlichen Regelungen des DSG NRW für eine Speicherung zu beachten.

Das Datensicherungskonzept enthält alle notwendigen Details der Datensicherung (was wird aus welchem Grund, von wem, nach welcher Methode, wann, wie oft und wo gesichert). Alle Maßnahmen sind entsprechend zu dokumentieren.
Alle Personen, die Datensicherungssysteme nutzen können, sollten über die Möglichkeiten zur Datensicherung informiert werden.

M 2.46 Durchführung von Datensicherungen

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal**

Daten sollten turnusgemäß auf zentralen Fileservern gesichert werden. Sollte ein zentraler Sicherungsserver nicht zur Verfügung stehen oder der Zugriff derzeit noch nicht möglich sein, sind die Daten lokal zu sichern. Die Sicherungen sind an einem sicheren Ort und nicht in unmittelbarer Nähe oder in dem gleichen Brandabschnitt des gesicherten IT-Systems zu lagern.
Die Sicherung der Daten sollten in einem angemessen Rhythmus erfolgen. Auch System- und Programmdaten sind nach Veränderungen zu sichern. Zur Datensicherung sind geeignete Backup-Werkzeuge zu verwenden, die eine Datensicherung nach dem Generationenprinzip unterstützen. Die Konfigurationen aller aktiven Netzkomponenten sind in eine regelmäßige Datensicherung einzubeziehen.
Für Daten, deren Wiederherstellung mehr als einige Tage Zeit erfordert, sollten mindestens 3 Sicherungsgenerationen vorgehalten werden. Es ist empfehlenswert eine Sicherung für mindestens 3 bis 6 Monate aufzubewahren. Es ist technisch oder organisatorisch sicher zu stellen, dass eine weitere Nutzung personenbezogener Daten in den Sicherungsdaten verhindert wird.

M 2.47 Verifizierung der Datensicherung

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal**

Die Konsistenz der Datensicherungsläufe ist sicher zu stellen, d. h. die Lesbarkeit der Datensicherung ist regelmäßig zu überprüfen. Darüber hinaus sollte mindestens einmal jährlich das testweise Wiedereinspielen von Datensicherungen geprüft und geübt werden.

1.10 Umgang mit Datenträgern und schützenswerten Daten

M 2.48 Handhabung von Datenträgern

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal**

Sicherungsdatenträger sind getrennt von dem jeweilis gesicherten IT-System in einem anderen Gebäude, einer anderen Brandschutzzone oder in einem für Datenträger geeigneten feuersicheren Tresor aufzubewahren.
Bei der Lagerung der Datenträger sind die Angaben der Hersteller, insbesondere zu Temperatur und Luftfeuchtigkeit zu beachten. Bei längerer Lagerung sind Vorkehrungen zu treffen, die eine alterungsbedingte Zerstörung der Datenträger verhindern. In angemessenen Zeitabständen ist ein Umkopieren der Daten auf neuere Datensicherungsträger vorzusehen. Die Fortentwicklung der Sicherungssysteme ist zu beachten. Bei einer Langzeitarchivierung muss ggf. die Bereitstellung eines Lesegeräts eingeplant werden, das für die verwendeten Datenformate geeignet ist.

M 2.49 Entsorgung von Daten, Datenträgern und Dokumenten

Verantwortlich für Initiierung	→	**IT-Beauftragte, Bereichsleitung**
Verantwortlich für Umsetzung	→	**IT-Personal, IT-Anwendende, Dezernat FM**

Datenträger (Festplatten, CDs, DVDs etc.), auch in IT-Geräten (Handys, Smartphones, USB-Sticks etc.) und vertrauliche Dokumente müssen sicher entsorgt werden. Bei unsachgemäßer Entsorgung können vertrauliche Daten in falsche Hände gelangen. Das kann erhebliche negative Folgen für die Universität und ihre Beschäftigten nach sich ziehen.
Bei der Entsorgung von personenbezogenen Informationen sind die Regelungen des Datenschutzgesetzes NRW (DSG NRW) zu beachten.

Beachten Sie bei der Entsorgung folgende Hinweise und sprechen Sie ggf. die genannten Ansprechpersonen an:

- Entsorgung von Festplatten, Laptops und IT-Kleingeräten mit Datenträgern
  Einzelne Festplatten, Laptops und IT-Geräte wie Handys, PDAs, USB-Sticks etc. können während der Dienststunden im Dispatching des HRZ (V0-215) über Sicherheitsbehälter entsorgt werden. Die Vernichtung wird unter Beachtung des Datenschutzgesetzes NRW durchgeführt. Größere Mengen sind mit der Sachbearbeitung Abfallwirtschaft (abfallwirtschaft@uni-bielefeld.de) abzustimmen. Geräte, die aufgrund ihrer Größe nicht auf diesem Weg entsorgt werden können, sind über den im nächsten Punkt beschriebenen Entsorgungsweg einer geregelten Vernichtung zuzuführen.

- Entsorgung von Arbeitsplatzrechnern
  Sollte es nicht möglich sein die Festplatten auszubauen, können Arbeitsplatzrechner auch komplett einer Vernichtung zugeführt werden. Die Anmeldung erfolgt über ein Webformular: http://www.uni-bielefeld.de/abfallservice. Die Rechner werden nach einer Terminvereinbarung abgeholt und einer sicheren Entsorgung zugeführt.

- Entsorgung von CDs, DVDs und Disketten
  CDs, DVDs, Disketten etc. können während der Dienststunden beim Dispatching des HRZ (V0-215) über Sicherheitsbehälter geregelt entsorgt werden.

- Entsorgung von Magnet-, Videobändern etc.

Magnet- oder Videobänder müssen gesondert entsorgt werden. Bei Bedarf nehmen Sie bitte Kontakt mit der Sachbearbeitung Abfallwirtschaft (abfallwirtschaft@uni-bielefeld.de) auf.

- Akten- und Papiervernichtung
  Ausdrucke und Akten können ebenso wie Datenträger vertrauliche Daten enthalten. Diese sind so zu vernichten, dass die ursprünglichen Informationen nicht wiederhergestellt werden können. Beachten Sie vor der Vernichtung von Akten der Universität unbedingt die „Richtlinien über Aufbewahrung, Aussonderung, Archivierung und Vernichtung von Akten“.[3]
  Für größere Mengen wird mehrfach jährlich nach Bedarf eine Aktenvernichtung durch die Sachbearbeitung Abfallwirtschaft (abfallwirtschaft@uni-bielefeld.de) organisiert. Für kleine Aktenmengen steht in den Dienstzeiten in der Zentralverwaltung ein Aktenvernichter zur Verfügung, der eine ausreichend hohe Sicherheitsstufe besitzt. Nähere Hinweise zur Aktenvernichtung finden sich auf den Internetseiten der Abfallwirtschaft (http://www.uni-bielefeld.de/abfall). Bei der Beschaffung eines eigenen Aktenvernichters sind die DIN 32757 bzw. mindestens die Sicherheitsstufe 3 zu beachten.

M 2.50 Physisches Löschen von Datenträgern

Verantwortlich für Initiierung	→	**IT-Beauftragte**
Verantwortlich für Umsetzung	→	**IT-Personal**

Wenn Datenträger, auf denen schützenswerte Daten gespeichert sind, zur weiteren Verwendung an Dritte gehen, müssen alle Daten vor der Weitergabe physisch so gelöscht werden, dass Sie nicht wiederhergestellt werden können. Das kann mit geeigneter Software erfolgen. Die vom Betriebssystem dafür vorgesehenen Mechanismen genügen in der Regel nicht für eine sichere Löschung.
Die Reparatur beschädigter Datenträger, auf denen schützenswerte Daten gespeichert sind, ist nur in besonderen Ausnahmenfällen erlaubt. Sollten Datenträger durch externe Dienstleistende repariert werden, sind die Auftragnehmenden in Abstimmung mit der oder dem Datenschutzbeauftragten auf die Wahrung der Vertraulichkeit der Daten zu verpflichten. Die Verpflichtung muss vertraglich vereinbart werden.

[3] Bekannt gegeben am 9.12.2003 durch ein Rundschreiben des Kanzlers an die Leiterinnen und Leiter der Fakultäten und Einrichtungen. Die Regelungen können über das Universitätsarchiv bezogen werden.

Glossar

Begriff	Erläuterung
Applikationsbetreuende	Die Applikationsbetreuerin oder der Applikationsbetreuer sind die für den technischen Betrieb einer Software-Anwendung verantwortlichen Ansprechpersonen. Sie oder er ist mit der Konfiguration der Applikation vertraut und in der Lage, Änderungen an ihr vorzunehmen.
Audit	Ein Audit („Anhörung“) ist ein systematisches Untersuchungs-verfahren, das sicherstellen soll, dass Anforderungen und Richtlinien, beispielsweise bei einem IT-System, entsprechend umgesetzt worden sind und eingehalten werden.
Bereichs-IT-Sicherheits-beauftragte (BITS)	Die Bereichs-IT-Sicherheitsbeauftragten (BITS) sind in ihrer Organisationseinheit Ansprechpersonen für die IT-Sicherheit und tragen Sorge für die Umsetzung der im IT-Sicherheitsprozess erarbeiteten Vorgaben. Sie arbeiten eng mit der oder dem zentralen IT-Sicherheitsbeauftragten zusammen.
Datenschutzbeauftragte	Die oder der Datenschutzbeauftragte überwacht die Einhaltung datenschutzrechtlicher Bestimmungen. Sie oder er ist der Leitung der Universität unterstellt, nicht weisungsgebunden, wird von der Landesbeauftragten für den Datenschutz kontrolliert und kann sich in Zweifelsfällen an diese wenden.
Filesharing	Unter dem Begriff Filesharing wird ein Datenaustausch zwischen Nutzerinnen und Nutzern über das Internet verstanden. Dies geschieht meist unter zuhilfenahme von sogenannten „Peer-to-Peer“-Diensten wie beispielsweise Bittorrent, die Daten der Nutzenden verteilen und gleichzeitig von anderen herunterladen.
Integrität	Integrität ist gewährleistet, wenn IT-Systeme und die durch sie verarbeiteten Informationen nicht unbefugt bzw. unzulässig verändert werden können.
IT	Informationstechnik
IT-Verfahrensverantwortliche	IT-Verfahrensverantwortliche sind Personen, die für den Betrieb eines IT-Verfahrens Verantwortung tragen und Auskunft über die technische und organisatorische Umsetzung geben können.
IT-Anwenderinnen und Anwender	IT-Anwenderinnen und Anwender sind Personen, die IT für ihre Aufgabenerfüllung nutzen, jedoch keine administrativen Berechtigungen haben wie beispielsweise das mit besonderen Berechtigungen ausgestattete IT-Personal.
IT-Beauftragte	Der oder die IT-Beauftragte ist für die inhaltliche und strategische Planung einer Fakultät bzw. Einrichtung verantwortlich. Er oder sie stellt sicher, dass eine permanente bedarfsorientierte Versorgung der Fakultät bzw. Einrichtung mit IT-Dienstleistungen erreicht wird.

IT-Betreuung	Die IT-Betreuung steht den Beschäftigen der Fakultäten und Einrichtung als primäre Ansprechperson bei allen Fragen zur Informationstechnik und Datenverarbeitung zur Verfügung. Dies beinhaltet insbesondere die Hard- und Softwarebetreuung, die Ersteinrichtung, Wartung und Entsorgung von Arbeitsplatzrechnern.
IT-Dienstleistende	IT-Dienstleistende wird als Oberbegriff für die IT-Betreuung und die Systemadministration verwendet. Dienstleistende an der Universität Bielefeld sind beispielsweise das Computerlabor der Mathematik, die Rechnerbetriebsgruppe (RBG) der Technischen Fakultät oder das Hochschulrechenzentrum (HRZ).
IT-Geräte	Elektronische Geräte wie Arbeitsplatzrechner, Notebooks, Server etc., die für die Verarbeitung von Daten genutzt werden.
IT-Kleingeräte	Elektronische Kleingeräte, die Daten verarbeiten und speichern können. Zu diesen zählen beispielsweise Handys, Smartphones oder USB-Sticks.
IT-Personal	Zum IT-Personal zählen Beschäftigte der Universität, die im Rahmen ihrer Tätigkeiten insbesondere mit der Installation, Konfiguration und Pflege von IT-Geräten und -Systemen betraut sind (siehe auch **Systemadministration**).
IT-Sicherheitsbeauftragter	Die oder der IT-Sicherheitsbeauftragte ist unter Anderem verantwortlich für die Entwicklung des Regelwerks der IT-Sicherheit, dessen Veröffentlichung und Fortschreibung und die Sicherstellung, dass dieses in den Fakultäten und Einrichtungen umgesetzt wird. Des Weiteren berät er oder sie die Fakultäten und Einrichtungen und führt Schulungs- und Sensibilisierungsmaßnahmen durch.
IT-Sicherheitsmanagement-Team (SMT)	Das Sicherheitsmanagement-Team (SMT) berät und unterstützt den IT-Sicherheitsbeauftragten oder die IT-Sicherheitsbeauftragte bei der Umsetzung und Steuerung des IT-Sicherheitsprozesses. Dem SMT fällt keine operative Kompetenz zu. Das SMT besteht aus 11 Mitgliedern der Universität Bielefeld. Den Vorsitz führt der oder die IT-Sicherheitsbeauftragte.
IT-Sicherheitsprozess	Um ein angemessenes Sicherheitsniveau für den Betrieb von Informationstechnik und die in diesem Zusammenhang verarbeiteten Daten herzustellen, ist ein organisiertes Vorgehen notwendig. Dies wird als IT-Sicherheitsprozess bezeichnet. In diesem Zusammenhang werden strategische Leitaussagen zur IT-Sicherheit formuliert, konzeptionelle Vorgaben erarbeitet und die organisatorischen Rahmenbedingungen geschaffen, welche die Risiken für die Integrität, Verfügbarkeit und Vertraulichkeit auf ein angemessenes Maß reduzieren. Eine regelmäßige Prüfung und Fortschreibung der Regelungen und Maßnahmen stellt sicher, dass auf neue Bedrohungen adäquat reagiert werden kann.
IT-Verfahren	Unter IT-Verfahren werden alle Arbeitsabläufe (Prozesse) verstanden, die auf Informationstechnik basieren. Ein IT-Verfahren bildet aus

	arbeitsorganisatorischer Sicht eine abgeschlossene Einheit. Hierzu zählen Beispielsweise der Betrieb eines E-Mail-, Content-Management- oder Backup-Systems. Ein einzelner Arbeitsplatz-rechner stellt kein IT-Verfahren dar.
Netzlaufwerk	Ein Netzlaufwerk ist ein reservierter Speicherbereich auf einem zentralen Speichersystem, der wie ein echtes Laufwerk (z. B. Laufwerk C: oder D:) auf dem Arbeitsplatzrechner eingebunden wird. Solche Netzlaufwerke bietet beispielsweise das HRZ als zentrale IT-Dienstleistung an. Diese bieten durch eine Reihe von Maßnahmen (Spiegelung und regelmäßiges Backup der Daten) einen hohen Schutz gegen Ausfall und Datenverlust.
Notfall	Einen „Notfall“ bezeichnet eine Situation, in der beispielsweise durch eine Betriebsstörung die Verfügbarkeit, Integrität oder Vertraulichkeit von Daten nicht mehr gegeben ist und ein verhältnismäßig hoher Schaden doht.
Personenbezogene Daten	Der Begriff wird im Datenschutzrecht (Bundesdatenschutz- und Landesdatenschutz-Gesetze) definiert und bezieht sich auf alle Daten bzw. Informationen, die einer natürlichen Person zugeordnet werden können.
Revision	Eine Revision ist ähnlich wie ein **Audit** eine regelmäßige Überprüfung von Maßnahmen auf ihre Angemessenheit und Wirksamkeit, die beispielsweise zur Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit umgesetzt worden sind.
Schutzbedarf	Grundsätzlich sind alle Daten schützenswert. Der tatsächliche Schutzbedarf von Daten wird durch eine Schutzbedarfsanalyse ermittelt. Abhängig von dem Ergebnis müssen entsprechende Maßnahmen ergriffen werden, um die Daten angemessen zu schützen. Die Vorlage zur Durchführung einer Schutzbedarfsanalyse ist bei dem oder der IT-Sicherheitsbeauftragten erhältlich.
Schutzbedarfsanalyse	Eine Schutzbedarfsanalyse wird im Rahmen des IT-Sicherheitsprozesses durchgeführt, um anhand von sechs vorgegebenen Kategorien den **Schutzbedarf** von Daten oder Systemen zu ermitteln. Im Ergebnis werden die Schutzbedarfsstufen Normal, Hoch und sehr Hoch unterschieden. Abhängig von dem Ergebnis werden entsprechende Maßnahmen ergriffen, um die Daten angemessen zu schützen. Bei einem hohen oder sehr hohen Schutzbedarf wird ergänzend eine Risikoanalyse durchgeführt.
Schützenswerte Daten	Grundsätzlich sind alle Daten schützenswert. Der tatsächliche Schutzbedarf von Daten wird durch eine Schutzbedarfsanalyse ermittelt. Abhängig von dem Ergebnis werden Maßnahmen ergriffen, um die Daten angemessen zu schützen.
Smartphones	Smartphones vereinen den Leistungsumfang eines Mobiltelefons mit einer elektronischen Terminplanung, E-Mail-, Internet-Zugang und ähnlichen Diensten. Sie gehören zu der Kategorie **IT-Kleingeräte**.

Systemadministration	Die Systemadministration ist für die Verwaltung von IT-Systemen verantwortlich. Zu ihren Aufgaben zählen insbesondere die Installation, Konfiguration und Pflege der betreuten Systeme. Für diesen Zweck sind diese mit entsprechenden Zugriffsberechtigungen ausgestattet.
Verfahrensverzeichnis	Der Begriff Verfahrensverzeichnis stammt aus dem Datenschutz und beschreibt unter anderem die Dokumentation der im Rahmen eines IT-Verfahrens verarbeitenden Daten. Im IT-Sicherheitsprozess werden alle **IT-Verfahren** der Universität dokumentiert unabhängig davon, ob Sie personenbezogene Daten enthalten oder nicht.
Verfügbarkeit	Verfügbarkeit ist gewährleistet, wenn IT-Systeme, ihre Komponenten und die auf ihnen gespeicherte Informationen zu jedem Zeitpunkt, an welchem diese gebraucht werden, zur Verfügung stehen.
Vertrauliche Daten	Vertrauliche Daten sind Informationen, die nicht für die Öffentlichkeit, sondern ausschließlich für einen eingeschränkten Personenkreis bestimmt sind. Beispiele sind Personaldaten, Finanzdaten, allgemein Daten mit Personenbezug (**personenbezogene Daten**) und Forschungsdaten die nicht bzw. noch nicht publiziert worden sind (siehe auch **Schutzbedarf**).
Vertraulichkeit	Vertraulichkeit ist gewährleistet, wenn Informationen ausschließlich durch die dafür autorisierten Personen eingesehen bzw. abgerufen werden können.

IT-Sicherheitsbeauftragter

Universität Bielefeld
Universitätsstr. 25
33615 Bielefeld

Telefon: 0521. 106-30 32
E-Mail: it-sicherheit@uni-bielefeld.de

www.uni-bielefeld.de/it-sicherheit