UNIVERSITÄT BERN

Weisungen Governance Informationssicherheit der Universität Bern

Die Universitätsleitung

gestützt auf Artikel 39 Abs. 1 Bst. k des Gesetzes vom 5. September 1996 über die Universität (UniG)

beschliesst:

1. Ziel und Zweck der Weisungen

Die Weisungen Governance Informationssicherheit legen die elementaren Ziele, Grundsätze, Zuständigkeiten und Prozesse der Informationssicherheit an der Universität Bern fest. Die Governance hat das Ziel, die Informationssicherheit zu steuern und zu optimieren. Die Weisungen legen zudem die Grundlage, um das Handlungsfeld «*Sicherheitsbezogenen Herausforderungen begegnen»* aus der Digitalisierungsstrategie 2030 der Universität Bern zu erfüllen.

2. Geltungsbereich

Die vorliegenden Weisungen sind für die gesamte Universität Bern anwendbar und für alle Mitarbeitenden verbindlich. Die Studierenden bilden eine Ausnahme und sind von diesen Weisungen nicht betroffen.

3. Grundsätze

- **Risikoorientierung**
  Informationssicherheit ist kein Selbstzweck. Die Umsetzung von Massnahmen und Initiativen zur Erreichung der Sicherheitsziele erfolgt risikobasiert, verhältnismässig und unter Berücksichtigung von Kosten und Nutzen.
- **Best Practice**
  Die Universität Bern nutzt anerkannte Standards. Zur Umsetzung der Cybersecurity / Informationssicherheit werden die folgenden Standards eingesetzt.
  - CIS (Center for Internet Security) Critical Security Controls in der Version 8
  - NIST (National Institute of Standards and Technology) Cybersecurity Framework.
  - DMP (Data Management Plan des Schweizerischen Nationalfonds, basierend auf den FAIR Data Principles)

- **Security/Privacy by Design**
  Informationssicherheit und Persönlichkeitsschutz sind Grundbestandteil unseres täglichen Handelns und werden in Geschäftsabläufe integriert und bei Projekten von Anfang an berücksichtigt.
- **Eigenverantwortung**
  Alle Mitarbeitenden sind in ihrem Verantwortungsbereich für die Umsetzung der Sicherheit verantwortlich.
- **Zuständigkeit**
  Für alle Informationen, ICT-Systeme und Geschäftsprozesse (Schutzobjekte) ist eine verantwortliche Person definiert.
- **ISMS**
  Die Universität Bern unterhält ein Informationssicherheits-Managementsystem. Dieses dient dazu, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

4. Informationssicherheitsziele/-Strategie

4.1 Zielbild

Die Universität Bern hat ein Bewusstsein für die Handhabung von Informationssicherheitsrisiken in Bezug auf Systeme, Mensch, Vermögenswerte, Daten und Fähigkeiten entwickelt. Es werden geeignete organisatorische und technische Schutzmassnahmen angewandt, um den Aufbau und den Betrieb der kritischen Dienste der Universität zu gewährleisten. Zudem sind wir als Organisation fähig, Cyber-Security-Ereignisse frühzeitig zu erkennen, in angemessener Zeit darauf zu reagieren und bei einem Ausfall von Diensten diese in der vordefinierten Zeit wiederherzustellen.

4.2 Ziele

- **Resilienz**
  Die Informationssicherheit für Lehre, Forschung, Verwaltung und Dienstleistungen wird bedarfsgerecht, risikoorientiert und systematisch sichergestellt und somit die Widerstandsfähigkeit gegenüber Cyber-Attacken erhöht.
- **Sensibilisierung**
  Die Informationssicherheit an der Universität Bern wird aktiv gelebt, als essenzieller Aspekt der Arbeit verstanden und nicht als behindernd empfunden.
- **Vertraulichkeit von Informationen**
  Daten und Informationen stehen ausschliesslich Berechtigten, in der zulässigen Weise, zur Verfügung.
- **Verfügbarkeit von Informationen**
  Daten und Informationen, die die Universität zur Erfüllung ihrer Geschäftstätigkeit benötigt, stehen im dafür vorgesehenen Zeitraum zur Verfügung.
- **Integrität von Informationen**
  Daten und Informationen sind vollständig, aktuell, unverändert und werden in der geforderten Qualität verarbeitet und übermittelt

Intern

5. Organisation und Zuständigkeiten

5.1 Universitätsleitung (UL)

Die Leitung der Universität Bern (in letzter Instanz die Rektorin / der Rektor) verantwortet die Informationssicherheit. Sie ist oberstes Kontrollorgan und hat folgende Aufgaben. Die Universitätsleitung

- verabschiedet die Informationssicherheitsziele und -strategie;
- erlässt Weisungen im Bereich der Informationssicherheit;
- entscheidet bezüglich Risikobewältigung, gemäss ihrer Kompetenz (siehe Kapitel 6.2.1 Risikobewältigung);
- stellt die nötigen finanziellen und personellen Ressourcen für die Etablierung und Aufrechterhaltung der Informationssicherheit und der definierten Informationssicherheitsziele zur Verfügung.

5.2 Geschäftsführende Direktor/innen (GD)

Die **GD** sorgen dafür, dass die Vorgaben zur Informationssicherheit (Weisungen und Richtlinien) bekannt sind und in den operativen Prozessen ihrer Organisationseinheit integriert und umgesetzt werden.

- stellen sicher, dass die relevanten Vorgaben (wie Weisungen, spezifische Gesetze und Regelungen [z.B. Humanforschungsgesetz] oder Vorgaben des SNF für Forschungsprojekte) in ihrem Wirkungsbereich bekannt sind und umgesetzt werden;
- sind dafür verantwortlich, dass der ICT-Grundschutz in ihrer Organisation umgesetzt wird;
- ernennen nach Bedarf entscheidungsbefugte Personen im Bereich Informationssicherheit in ihrer Organisationseinheit, jedoch mindestens Informationseigner/innen (IE), Information Security Officer (ISO) und Technikverantwortliche (TV) (siehe Kapitel 5.3 - 5.5);
- entscheiden bezüglich Risikobewältigung gemäss ihrer Kompetenz in ihrer Organisationseinheit (siehe Kapitel 6.2.1 Risikobewältigung);
- stellen im Rahmen ihrer Möglichkeiten die nötigen personellen und finanziellen Ressourcen zur Verfügung, um die definierten Aufgaben zu bewältigen.

Die Aufgaben können innerhalb der eigenen Organisation auch delegiert werden. Die Verantwortung bleibt bei den GD.

5.3 Informationseigner/innen (IE)

Die Informationseigner/innen sind verantwortlich für eine Informationssammlung. Eine Informationssammlung ist eine Ansammlung von Informationen, die unabhängig von der Art ihrer Speicherung in einem bestimmten Kontext verwendet wird. In der Regel wird eine Informationssammlung mithilfe einer Anwendung bearbeitet.

Beispiele: Applikationen (inkl. Datenbanken), Geschäftsablagen, Forschungsdaten, Archiv (physisch oder digital).

Die Informationseigner/innen werden von den Geschäftsführenden Direktor/innen ernannt.

Die wichtigsten Aufgaben der Informationseigner/innen im Kontext dieser Weisungen umfassen die nachfolgenden Punkte: Die Informationseigner/innen

- legen mittels Klassifizierung den Schutzbedarf einer Informationssammlung fest (Vertraulichkeit, Verfügbarkeit und Integrität);
- bewilligen Berechtigungen und überprüfen diese regelmässig;

Intern

- bewilligen die Weitergabe von Informationen;
- stellen sicher, dass die Aufbewahrung und Archivierung von Informationssammlungen den geschäftlichen und gesetzlichen Anforderungen entsprechen;
- legen fest, zu welchem Zweck die Informationssammlungen verwendet werden;
- stellen die Datenqualität sicher;
- sind zuständig für die Umsetzung des ICT-Grundschutzes in seinem Wirkungsbereich;
- stellen sicher, dass bei der Auslagerung von Dienstleistungen die Informationssicherheitsanforderungen und deren Überprüfung vertraglich festgehalten werden;
- sind in Forschungsprojekten für den Lebenszyklus von Forschungsdaten verantwortlich, insbesondere in Bezug auf folgende Bereiche:
    - *Datenerhebung und -dokumentation*
    - *Ethische, rechtliche und Sicherheitsfragen*
    - *Datenspeicherung und -erhalt*
    - *Austausch und Weiterverwendung der Daten*

Aufgaben können an weitere Stellen delegiert werden. Die Verantwortung bleibt den Informationseigner/innen.

5.4 Information Security Officer (ISO)

Die ISO sind jeweils der verlängerte Arm der CISO und vertreten deren Interessen in der jeweiligen Organisationseinheit. Die wichtigsten Aufgaben im Kontext dieser Weisungen sind:

- Enge Abstimmung mit den CISO;
- Erste Anlaufstelle für Fragen zur Informationssicherheit;
- Führen eines aktuellen Inventars von Informationssammlungen mit hohem Schutzbedarf;
- Identifizieren und Dokumentieren von Informationssicherheitsrisiken und Abweichungen zum ICT-Grundschutz;
- Erarbeitung, wenn nötig, von ergänzenden Sicherheitsmassnahmen zum ICT-Grundschutz, in ihren Verantwortungsbereichen z.B. für Forschungsprojekte;
- Unterstützung bei der Umsetzung des ICT-Grundschutzes;
- Regelmässige Berichterstattung an die CISO, insbesondere in Bezug auf folgende Bereiche:
    - Abweichungen vom ICT-Grundschutz.
    - Rapportieren von identifizierten Informationssicherheitsrisiken.
    - Rapportieren von relevanten Security Incidents.
    - Melden von Informationssammlungen mit hohem Schutzbedarf
- Mitgliedschaft im Fachgremium Informationssicherheit.

Die ISO werden von den Geschäftsführenden Direktor/innen ernannt.

5.5 Technikverantwortliche (TV)

Die Technikverantwortlichen sind für den sicheren Betrieb der ICT-Infrastruktur verantwortlich. Ihre Aufgaben im Kontext dieser Weisungen sind:

- Umsetzung und Aufrechterhaltung des ICT-Grundschutzes in ihrem Verantwortungsbereich;
- Umsetzung von technischen Vorgaben des in Forschungsprojekten;
- Zusammenarbeit mit den ISO.

Intern

5.6 Chief Information Security Officer (CISO)

Die/der CISO ist für das Management der Informationssicherheit verantwortlich. Sie/er schafft Voraussetzungen, um Informationssicherheitsrisiken an der Universität Bern angemessen zu begegnen. Sie/er ist das Bindeglied zwischen der Universitätsleitung, den Fakultäten und Instituten, der IT und den Mitarbeitenden. Ihre/seine wesentlichen Aufgaben sind:

- Erarbeiten, Abstimmen, Vernehmlassen und Pflegen der Informationssicherheitsstrategie der Universität Bern;
- Definieren und Koordinieren der Informationssicherheitsprozesse;
- Erarbeiten von Sicherheitsmassnahmen (ICT-Grundschutz);
- Aufbauen der Sicherheitsorganisation an der Universität Bern;
- Initiieren, Durchführen und Koordinieren von Sensibilisierungsmassnahmen;
- Aufbauen und Pflegen des Inventars für Informationssicherheitsrisiken der Universität Bern;
- Aufbauen, Pflegen und Weiterentwickeln des universitätsweiten Informationsmanagement Systems (ISMS);
- Berichterstattung an die Universitätsleitung – Reporting Informationssicherheit;
- Abstimmung mit der Fachstelle Datenschutz des Rechtsdienstes und dem Risikomanagement der Uni Bern.

5.7 Projektleitende (PL)

Projektleitende sind verantwortlich, dass der ICT-Grundschutz in Projekten umgesetzt wird. Abweichungen vom ICT-Grundschutz und allfällig identifizierte Risiken sind dem ISO/CISO zu melden. Projektleitende

- stellen sicher, dass die notwendigen ISDS-Dokumente (Schutzbedarfsanalyse und wenn nötig ISDS-Konzept und Risikoanalyse) in den entsprechenden Projektphasen vorliegen;
- stellen in Forschungsprojekten Qualität, Sicherheit und ethische Standards sicher.

5.8 Security Operation Center (SOC) / Computer Security Incident Response Team (CSIRT)

Das Security Operation Center (SOC) ist zuständig für Entdeckung und Abwehr von Cyberangriffen auf die zentrale ICT-Infrastruktur der Universität Bern. Die SOC- sowie die CSIRT-Aufgaben werden von der Gruppe NETSEC der Informatikdienste wahrgenommen. Die wesentlichen Aufgaben sind:

- Aufdecken von technischen Schwachstellen;
- Erkennen und Vermeiden von Informationssicherheitsvorfällen (Monitoring);
- Eindämmen und Bearbeiten von Informationssicherheitsvorfällen (Incident Response);
- Rapportieren an die/den CISO und die betroffenen Benutzungsgruppen;
- Präventive Erkennung von potenziellen Gefahren für ICT-Infrastruktur der Universität (Threat Hunting);
- Analysieren von Informationssicherheitsvorfällen und ableiten von Verbesserungen.

Intern

5.9 Gremien

5.9.1 Fachgruppe Informationssicherheit Zentralbereich (FGIS ZB)

Die Fachgruppe Informationssicherheit dient dem regelmässigen Austausch und der Weiterentwicklung der Informationssicherheit im Zentralbereich. Das Gremium besteht aus den Information Security Officers (ISOs) des Zentralbereichs und wird von der/dem CISO geleitet. Das Gremium trifft sich mindestens vier Mal pro Jahr oder bei Bedarf. Die wesentlichen Aufgaben des Gremiums sind:

- Informations- und Wissensaustausch;
- Sounding Board für Massnahmen im Bereich der Informationssicherheit;
- Analyse der Bedrohungslage;
- Verbessern der Informationssicherheitsprozesse und -Organisation (KVP).

5.9.2 Fachgruppe Informationssicherheit Fakultäten & Institute (FGIS F&I)

Die FGIS F&I dient dem regelmässigen Austausch und der Weiterentwicklung der Informationssicherheit in den Fakultäten, Instituten und weiteren dezentralen Stellen der Universität. Das Gremium besteht aus den dezentralen Information Security Officers (ISOs) und wird von der/dem CISO geleitet. Das Gremium trifft sich mindestens vier Mal pro Jahr oder bei Bedarf. Die wesentlichen Aufgaben des Gremiums sind:

- Informations- und Wissensaustausch;
- Sounding Board für Massnahmen im Bereich der Informationssicherheit;
- Analyse der Bedrohungslage;
- Verbessern der Informationssicherheitsprozesse und Organisation (KVP).

6. ISMS & Informationssicherheitsprozesse

In den nachfolgenden Abschnitten wird beschrieben, mit welchen Praktiken die Erreichung der definierten Informationssicherheitsziele sichergestellt wird. Die Praktiken sind Bestandteil des Informationssicherheitsmanagementsystems (ISMS).

Das ISMS dient dazu, die Informationssicherheit nachhaltig zu steuern. Externe Anforderungen, wie Gesetze, Regulatorien und Verträge, sowie das Risikomanagement bilden die Grundlage für die Definition von Sicherheitszielen, Sicherheitsprozessen und Vorgaben. Mittels Kennzahlen, Management-Reviews und Audits wird sichergestellt, dass das ISMS wirksam und effizient ist.

Kernelemente des ISMS sind eine etablierte Sicherheitsorganisation, ein Securityframework und ein Risikomanagementprozess, der spezifischen Bedrohungen angemessen entgegenwirkt und das ISMS kontinuierlich verbessert.

Intern

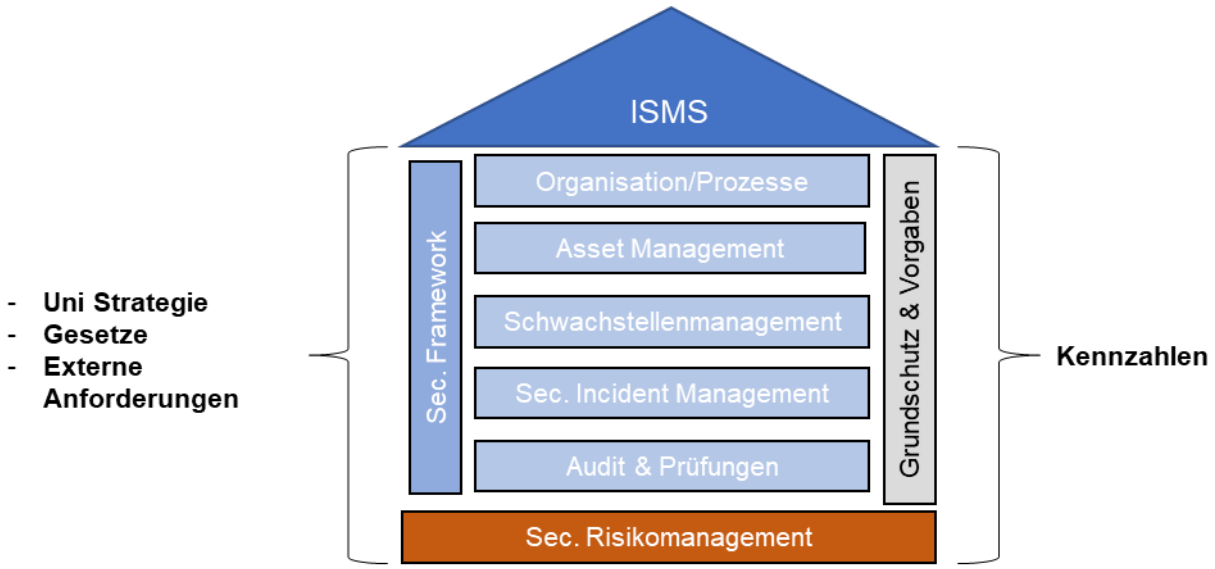

Abbildung 1

6.1 Grundschutz und Vorgaben

Die Universität Bern verwendet anerkannte Frameworks und Standards, um die Informationssicherheit sicherzustellen. Der auf den CIS Controls basierende ICT-Grundschutz enthält eine grosse Anzahl an international anerkannten Schutzmassnamen, die bekannte Bedrohungen entgegenwirken. Die ICT-Grundschutz-Massnahmen inklusive Verantwortlichkeiten und Prozesse werden in den Weisungen ICT-Grundschutz ausführlich beschrieben.

Zusätzlich zum ICT-Grundschutz werden weitere themenspezifische Vorgaben im Kontext der Informationssicherheit erlassen. Gemeinsam mit den themenspezifischen Weisungen bildet der ICT-Grundschutz das Securityframework der Universität Bern.

6.2 Projekte und Vorhaben

Damit die Informationssicherheit und der Datenschutz in Projekten rechtzeitig berücksichtigt werden, müssen die Dokumente gemäss Tabelle 1 in Projekten und Vorhaben genutzt werden. Die Dokumente basieren auf der Projektmethodik HERMES.

ISDS-Dokument	Beschreibung
Schutzbedarfsanalyse	Die Schutzbedarfsanalyse dient der Ermittlung des Schutzbedarfs für Informationssammlungen.
ISDS-Konzept	Im ISDS-Konzept wird dokumentiert, wie die Sicherheits- und Datenschutzmassnahmen (z.B. der Grundschutz) für ein bestimmtes Schutzobjekt/Informationssammlung umgesetzt werden.
Risikoanalyse	Können ICT-Grundschutzmassnahmen nicht oder nur teilweise umgesetzt werden, muss eine Risikoanalyse erstellt werden.

Tabelle 1

Allfällige Risiken sowie die fertiggestellten Dokumente sind dem zuständigen ISO und dem CISO zuzustellen.

Intern

6.3 Risikomanagement im ISMS

Risikomanagement ist ein wesentlicher Teil des ISMS. Es stellt sicher, dass die Informationssicherheit als Ganzes fortwährend analysiert und bei Bedarf optimiert wird.

Schwachstellen (technische und organisatorische), Bedrohungen und Risiken sollen regelmässig identifiziert, bewertet und dokumentiert werden. Die Information Security Officers sind verpflichtet, relevante Informationssicherheits-Risiken dem CISO zu melden. Die/der CISO ist für die zentrale Dokumentation der Risiken und die Berichterstattung an die Universitätsleitung verantwortlich.

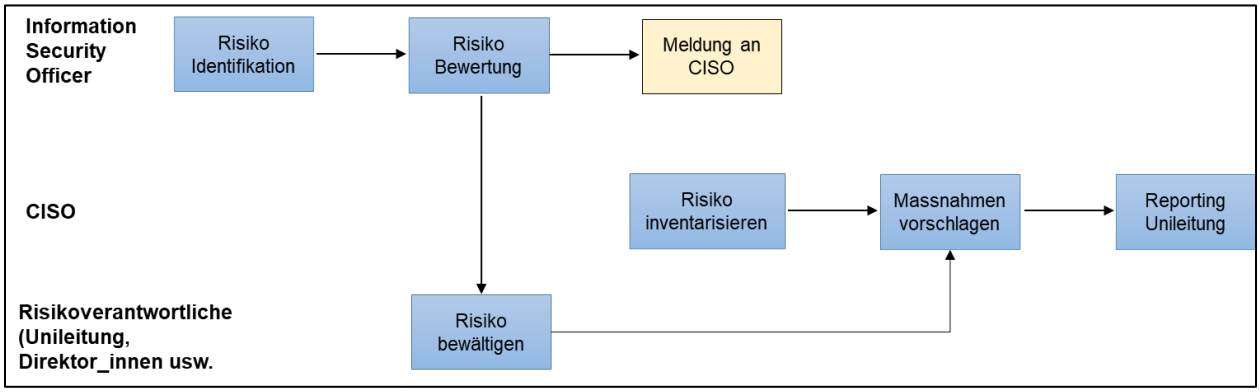

Abbildung 2

6.3.1 Risikomatrix

Gemäss Definition ist ein Risiko ein Mass für die Grösse einer Gefährdung und beinhaltet die Häufigkeit bzw. Wahrscheinlichkeit und das Schadensausmass eines unerwünschten Ereignisses.

Risiko = Schaden x Eintretenswahrscheinlichkeit

Die Bewertung von Risikoszenarien erfolgt gemäss der Risikomatrix in Abbildung 4 durch die jeweiligen Informationseigner/innen. Die Fachgruppe (FGIS) kann bei Bedarf unterstützen.

Eintrittswahrscheinlichkeit				
sehr häufig (4)	moderat	hoch	sehr hoch	sehr hoch
häufig (3)	moderat	moderat	hoch	sehr hoch
selten (2)	gering	moderat	moderat	hoch
unwahrscheinlich (1)	gering	gering	moderat	hoch
	Auswirkung			
	vernachlässigbar (1)	spürbar (2)	kritisch (3)	hoch kritisch (4)

Abbildung 3 Risikomatrix

Intern

Eintrittswahrscheinlichkeit

Sehr häufig	Häufig	Selten	Unwahrscheinlich
Mehrmals im Monat	Einmal im Monat – einmal pro Jahr	Alle 1 – 5 Jahre	Alle 5 Jahre oder weniger häufig

Tabelle 2

Auswirkungen/Schaden

	Vernachlässig-bar	Spürbar	Kritisch	Hoch kritisch
Vertraulichkeit	Einzelne Informationen sind für unberechtigte einsehbar.	Sensitive Informationen in begrenztem Umfang sind für Unberechtigte einsehbar.	Sensitive Informationen sind in umfangreichem Ausmass für Unberechtigte einsehbar.	Sensitive Informationen sind in fast vollumfänglichem Ausmass für unberechtigte einsehbar.
Verfügbarkeit	Ausfall/Unterbruch von einzelnen Services oder Funktionen.	Ausfall/Unterbruch mehrerer Services oder einer Applikation.	Mehrere Applikationen oder ein Geschäftsprozess sind beeinträchtigt oder nicht mehr verfügbar.	Ein oder mehrere Geschäftsprozesse sind beeinträchtigt oder nicht mehr verfügbar.
Integrität	Einzelne Informationen sind nicht mehr integer.	Sensitive Informationen in begrenztem Umfang sind nicht mehr integer.	Sensitive Informationen in umfangreichem Ausmass sind nicht mehr integer	Sensitive Informationen in fast vollumfänglichem Ausmass sind nicht mehr integer.
Reputation	Einmalige negative Berichterstattung oder einzelne unzufriedene Mitarbeitende, Studierende oder Forschende.	1-2 Tage negative Berichterstattung oder grössere Gruppen von unzufriedenen Mitarbeitenden/Studierende oder Forschenden.	Mindestens 3 Tage negative Berichterstattung oder viele unzufriedene Mitarbeitende, Studierende, Forschenden und Vorgesetzte.	Umfassende, mehrtägige bis mehrwöchige negative Berichterstattung oder grösstenteils unzufriedene Mitarbeitende, Studierende, Forschende und Vorgesetzte.
Rechtliche Konsequenzen	Minimale Verstösse. Keine Gefahr eines Rechtstreits oder einer Strafe.	Verstösse, durch welche ein Rechtsstreit oder eine Strafe droht.	Verstösse, durch welche ein Rechtsstreit oder eine Strafe wahrscheinlich ist.	Verstösse, welche zu einem Rechtsstreit oder einer Strafe führen.

Tabelle 3

Intern

6.3.2 Risikobewältigung und -Einschätzung

In Tabelle 3 ist ersichtlich, welche Stelle/Rolle im Grundsatz über die Kompetenz verfügt, den Umgang mit Risiken (Risikobewältigung) festzulegen. Die Geschäftsführenden Direktor/innen können die Kompetenz für moderate und geringe Risiken in ihrer Organisation delegieren.

Mögliche Bewältigungsstrategien:

- Risiko vermeiden – Das Geschäft/Vorhaben wird eingestellt
- Risiko minimieren – Es werden Massnahmen umgesetzt, um ein Risiko zu senken
- Risko akzeptieren – Das Risiko wird akzeptiert
- Risiko transferieren – Mittels Vertrag oder Versicherung

Risiko	Risikoeigner/in	Meldepflicht	Beschreibung
Gering	Geschäftsführende Direktor/innen oder gemäss Delegation	Nein	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmassnahmen bieten einen ausreichenden Schutz. In der Praxis ist es üblich, geringe Risiken zu akzeptieren und die Gefährdung dennoch zu beobachten.
Moderat	Geschäftsführende Direktor/innen oder gemäss Delegation (Siehe Kapitel 5.2)	Nein	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmassnahmen reichen möglicherweise nicht aus, um den Eintritt eines Ereignisses zu verhindern und den Schaden vollumfänglich abzuwenden. In der Praxis wird, unter Berücksichtigung von Kosten und Nutzen, versucht, moderate Risiken zu senken.
Hoch	Geschäftsführende Direktor/innen (Siehe Kapitel 5.2)	Ja	Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmassnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung. In der Praxis werden hohe Risiken selten akzeptiert.
Sehr hoch	Universitätsleitung (Siehe Kapitel 5.1)	Ja	Die bereits oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmassnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung. In der Praxis werden sehr hohe Risiken nicht akzeptiert.

Tabelle 4

Intern

7. Begriffsdefinitionen

Begriff	Beschreibung
Auswirkung/Schadensausmass	Auswirkungen (im Kontext des Risikomanagements) beschreiben die Gesamtheit aller Folgen aus einem oder mehreren Ereignissen. Auswirkungen können sowohl negativ (Schaden) als auch positiv (Nutzen) sein.
Bedrohung/Gefahr	Zustand oder Vorgang, aus dem ein Schaden an einem Schutzobjekt entstehen kann.
CIS Controls	Die CIS Controls (ehemals CIS Critical Security Controls) sind eine Sammlung empfohlener Sicherheitsmassnahmen zur Abwehr der verbreitetsten und gefährlichsten Cyber-Angriffe.
Eintrittswahrscheinlichkeit	Auf eine bestimmte Situation (Risiko-Szenario) oder Zeitdauer bezogene Möglichkeit, dass ein konkretes Ereignis eintritt.
Informationssammlung	Eine Informationssammlung ist eine Ansammlung von meist strukturierten Informationen, die unabhängig von der Art ihrer Speicherung in einem bestimmten Kontext verwendet wird. In der Regel wird eine Informationssammlung mithilfe einer Anwendung bearbeitet. Beispiele: Applikationen (inkl. Datenbanken), Geschäftsablagen, Forschungsdaten, Archiv (physisch oder digital).
Informationen	Information, wird mit Bedeutung oder Wissen gleichgesetzt. Eine Information kann z.B. die Form von Text, Bild oder Tonaufnahmen annehmen. Im Unterschied zu Informationssammlungen sind Informationen in der Regel unstrukturierte Dokumente z.B. Verträge, Protokolle, Vorgaben, Konzepte, Wiki, Intranet oder E-Mails.
ISMS	Information Security Management System. Dies sind alle Aktivitäten wie, Organisation, Prozesse, Vorgaben und technische Hilfsmittel, die sicherstellen, dass Informationssicherheitsrisiken einer Organisation erkannt werden und dauerhaft auf ein akzeptables Level gesenkt werden können.
NIST	National Institute of Standards and Technology aus den USA
Privacy	Ist der englische Begriff für Datenschutz, das heisst für den Schutz der Persönlichkeit und Privatsphäre.
Projekt	Ein Projekt ist ein einmaliges Vorhaben mit einem bestimmten Ziel. Um das Ziel zu erreichen, müssen Handlungen geplant und umgesetzt werden. Das Vorhaben hat einen Beginn und ein Ende.
Risiko	Das Risiko ist ein Mass für die Grösse einer Gefährdung und beinhaltet die Häufigkeit bzw. Wahrscheinlichkeit und das Schadensausmass eines unerwünschten Ereignisses.
Risikoeigner/in	Rolle, die darüber entscheidet, wie mit Risiken umgegangen wird. Die/der Risikoeigner/in entscheidet, ob Risiken reduziert, akzeptiert, transferiert oder vermieden werden. Die Rolle muss über die nötigen Kompetenzen in der Organisation verfügen. Die Rolle wird von der Universitätsleitung/Rektor/in oder einer/einem Geschäftsführenden Direktor/in wahrgenommen.
Risiko Szenario	Allgemeine Beschreibung eines möglichen Ereignisses oder einer Entwicklung und die daraus entstehenden Auswirkungen auf Schutzgüter

Intern

8. Schlussbestimmungen

8.1 Widersprechende Bestimmungen

Bestehende, diesen Weisungen widersprechende Bestimmungen werden hiermit aufgehoben.

8.2 Inkrafttreten

Diese Weisungen treten per sofort in Kraft.

Abweichungen von diesen Weisungen gilt es zu identifizieren und innert nützlicher Frist zu beheben oder als Risiko festzuhalten und durch die Risikoeigner/innen zu akzeptieren.

Bern, 7. November 2023

Namens der Universitätsleitung:

Prof. Dr. Christian Leumann
Rektor

Intern