UNIVERSITÄT
BERN

Weisungen ICT-Grundschutz 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

Der ICT-Grundschutz legt die minimalen Anforderungen bezüglich Informationssicherheit an der Universität Bern fest und unterstützt die Umsetzung der Sicherheitsziele, die in den Weisungen Governance Informationssicherheit der Universität Bern definiert sind.

Es sind systematische Prozesse und Abläufe aufzubauen und zu etablieren, die sicherstellen, dass die in den vorliegenden Weisungen enthaltenen Vorgaben wirksam und nachhaltig umgesetzt werden. Die Einhaltung der Vorgaben ist von den Verantwortlichen regelmässig zu überprüfen.

2. Geltungsbereich

Diese Weisungen gelten für alle Mitarbeitenden der Universität Bern, die ICT-Systeme On-Premise oder in der Cloud für die Universität Bern betreiben und bereitstellen. Studierende und ihre Informatikmittel sind davon ausgenommen.

Externe Dritte sind vertraglich zu verpflichten, den ICT-Grundschutz sinngemäss umzusetzen.

3. Grundsätze

- **Virtualisierung** – Der ICT-Grundschutz gilt unabhängig davon, ob ein Schutzobjekt auf dedizierter Hardware oder einer Virtualisierungslösung betrieben wird.
- **Stand der Technik** – Die eingesetzten Schutzmassnahmen entsprechen dem aktuellen Stand der Technik.
- **Need to Know/Least Privilege** – Berechtigungen werden nur erteilt, wenn diese zur geschäftlichen Aufgabenerfüllung notwendig sind. Das heisst, es werden keine Berechtigungen auf Vorrat vergeben. Das Prinzip bezieht sich auf ICT-Systeme [3], Netzwerkzonen und Informationen.
- **Security by Default** – Alle ICT-Systeme [3] müssen so entwickelt, konfiguriert und betrieben werden, dass alle sinnvollen Sicherheits- und Schutzmechanismen (z.B. Verschlüsselung) standardmässig aktiviert sind und ihre Wirkung entfalten können, ohne dass sich die Nutzenden darum kümmern müssen.
- **Attack Surface Reduction** – ICT-Systeme [3] bieten nur Funktionen und Dienste an, welche für die Leistungserbringung zwingend notwendig sind. Um die Angriffsfläche von ICT-Systemen zu verringern, sind unnötige Dienste und Funktionen zu deaktivieren oder zu entfernen.

4. Organisation und Zuständigkeiten

In diesem Kapitel werden die Rollen und Aufgaben im Kontext dieser Weisungen beschrieben.

In Ziffer 6 werden den jeweiligen Rollen die einzelnen Vorgaben zugeordnet. Diese Zuordnung ist in der Tabelle in der Spalte «zuständig» ersichtlich. Wenn eine Vorgabe nicht eindeutig einer Rolle zugeordnet werden kann, wird sie der geschäftsführenden Direktorin oder dem geschäftsführenden Direktoren zugewiesen. Diese oder dieser kann die Umsetzung der Vorgaben innerhalb ihrer oder seiner Organisation an andere Stellen delegieren.

4.1 Geschäftsführende Direktoren/innen

- Die geschäftsführenden Direktorinnen oder Direktoren (**GD)** sorgen dafür, dass die Vorgaben zur Informationssicherheit (Weisungen und Richtlinien) bekannt sind und in den operativen Prozessen ihrer Organisationseinheit integriert und umgesetzt werden. Sie stellen sicher, dass relevante Vorgaben (Weisungen, spezifische Gesetze und Regelungen z.B. Humanforschungsgesetz) in ihrem Wirkungsbereich bekannt sind und umgesetzt werden.
- Sie sind dafür verantwortlich, dass die vorliegenden Weisungen in ihrer Organisation umgesetzt werden.
- Sie 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 delegiert werden. Die Verantwortung bleibt bei den GD.

4.2 Chief Information Security Officer (CISO)

Die oder d CISO ist für das Management der Informationssicherheit verantwortlich. Sie oder er schafft Voraussetzungen, um Informationssicherheitsrisiken an der Universität Bern angemessen zu begegnen. Sie oder er ist das Bindeglied zwischen der Universitätsleitung, den Fakultäten und Instituten, den Informatikdiensten und den Mitarbeitenden. Ihre oder seine wesentlichsten Aufgaben im Rahmen dieser Weisungen sind:

- Erarbeiten von Sicherheitsmassnahmen (ICT-Grundschutz).
- Regelmässige Aktualisierung des ICT-Grundschutzes aufgrund neuer Bedrohungen oder neuer Vorgaben, z.B. neue Gesetze und Verordnungen.
- Bericht erstatten an die Universitätsleitung – Reporting Informationssicherheit.

4.3 Informationseigner/innen

Die Informationseigerinnen oder Informationseigner (IE) 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 Informationseignerinnen oder Informationseigner werden von den geschäftsführenden Direktorinnen oder Direktoren ernannt.

Die wichtigsten Aufgaben der Informationseignerinnen oder Informationseigner im Kontext dieser Weisungen sind in der Spalte «zuständig» in Ziffer 6 geregelt.

4.4 Information Security Officer

Die oder der Information Security Officer (ISO) ist jeweils der verlängerte Arm der oder des CISO und vertreten ihre oder seine Interessen in der jeweiligen Organisationseinheit. Die wichtigsten Aufgaben im Kontext dieser Weisungen sind:

- Anlaufstelle für Fragen zur Informationssicherheit.
- Identifizieren und dokumentieren von Informationssicherheitsrisiken und Abweichungen zum ICT-Grundschutz.
- Erarbeitet in ihrem Verantwortungsbereich, wo nötig und sinnvoll, ergänzende Sicherheitsmassnahmen zum ICT-Grundschutz.
- Unterstützten bei der Umsetzung des ICT-Grundschutz.
- Melden identifizierte Abweichungen zum ICT-Grundschutz der CISO.

Die ISO werden von den geschäftsführenden Direktorinnen oder Direktoren ernannt.

Die Aufgaben der ISO im Kontext dieser Weisungen sind in der Spalte «zuständig» in Ziffer 6 festgehalten.

4.5 Technikverantwortliche

Die Technikverantwortlichen (TV) sind für die technische Umsetzung der Informationssicherheitsanforderungen gemäss der Spalte «zuständig» in Ziffer 6 in den Fakultäten und Instituten zuständig.

4.6 Informatikdienste

In den Informatikdiensten (ID) gibt es keine Technikverantwortlichen. Sinngemäss wird in der Spalte «zuständig» in Ziffer 6 zusätzlich die ID aufgeführt, wenn sie zuständig sind.

5. Schutzkonzept

Der ICT-Grundschutz garantiert einen Basisschutz (basierend auf den *CIS Controls* in der Version 8) gegenüber bekannten Bedrohungen und Schwachstellen in der ICT. Informationen und *ICT-Systeme* mit erhöhtem Schutzbedarf können mittels zusätzlicher Schutzmassnahmen geschützt werden. Der Schutzbedarf kann mittels einer *Schutzbedarfsanalyse* oder einer *Risikoanalyse* ermittelt werden.

Hilfsmittel	Schutzbedarf	Schutzlevels
Weisungen ICT-Grundschutz	Normaler Schutzbedarf	ICT-Grundschutz
Schutzbedarfsanalyse/Risikoanalyse	Erhöhter Schutzbedarf	Wird individuell festgelegt

Die CIS Controls können als Hilfsmittel zur Identifikation von pragmatischen Massnahmen herangezogen werden. Die Umsetzung der CIS Controls als Ergänzung zum ICT-Grundschutz wird empfohlen. Als Hilfsmittel zur Standortbestimmung kann das Dokument *CIS Controls UniBE* genutzt werden.

6. Vorgaben

Die nachfolgenden Vorgaben gelten für ICT-Systeme On-Premise und in der Cloud (IaaS, PaaS), die von Mitarbeitenden der Universität Bern aufgebaut und betrieben werden.

6.1 Schulung und Sensibilisierung

Nr.	Vorgabe	Zuständig
1	Personen, die *sensitive Daten/Informationen* der Universität Bern bearbeiten, müssen über den korrekten Umgang mit Sicherheits- und Schutzmassnahmen geschult und angeleitet werden, (z.B. Datenschutzschulung, Anleitungen) sowie über mögliche Sanktionen aufgeklärt werden.	ISO

6.2 Inventar

Nr.	Vorgabe	Zuständig
	Ein Inventarisierungsprozess, welcher sicherstellt, dass zu jedem Zeitpunkt ein vollständiges Inventar der ICT-Systeme (physische und virtuelle Instanzen) inkl. Software und Lizenzen vorhanden ist, soll etabliert werden. Das Inventar sollte mindestens die nachfolgenden Objekte enthalten: • Bezeichnung des Objekts • Standort • Verantwortliche Personen (Owner) • Kritikalität, Recovery Time Objective (RTO), Recovery Point Objective (RPO) • Vertraulichkeitslevel, wird abgeleitet von den klassifizieren Daten • HW-Typ • Softwarebezeichnung • Software-Version	ISO

6.3 Dokumentation und ISDS-Dokumente

Nr.	Vorgabe	Zuständig
1	Für alle ICT-Systeme ist eine Dokumentation zu erstellen und über den gesamten Life Cycle aktuell zu halten. Die Dokumentation muss folgende Aspekte beinhalten: • Verwendungszweck • Zuständigkeiten • Kritikalität (Vertraulichkeitslevel, RTO, RPO, Integritätslevel) • Datenschutzspezifische Massnahmen • Sicherheitsrelevante Komponenten, Funktionen und Konfigurationen • Service Level Agreement (SLA), welches zur Anwendung kommt • Lieferkette • Vertragliche Vereinbarungen	TV/ID
2	Bei Projektbeginn (Vorphase) oder bei grösseren Veränderungen von ICT-Systemen muss eine Schutzbedarfsanalyse erstellt oder aktualisiert werden. Ergibt die Schutzbedarfsanalyse, dass die Daten/Informationen einen erhöhten Schutzbedarf haben, muss ein ISDS-Konzept erstellt werden. Sind die Voraussetzungen für eine Vorabkontrolle (Art. 17a KDSG) erfüllt (bspw. bei der Bearbeitung von besonders schützenswerte Personendaten), muss das ISDS-Konzept zudem der Datenschutzaufsichtsstelle des Kanton Bern (DSA) unterbreitet werden. In einem solchen Fall sind der/die CISO und der Rechtsdienst (Fachstelle Datenschutz) zu involvieren.	TV/ID

6.4 Identitäts- und Account-Management

Alle (internen und externen) Mitarbeitenden der Universität Bern und technischen Ressourcen müssen vor der Ausübung einer Tätigkeit oder Funktion eindeutig identifiziert und autorisiert werden.

Nr.	Vorgabe	Zuständig
1	Vor der Vergabe eines persönlichen Accounts muss jede Person identifiziert werden. In der Regel im Rahmen des Anstellungsprozesses. Die Identitäten sind eindeutig und zentral zu erfassen.	GD
2	Ein Account, muss wenn immer möglich mit einer Multifaktor Authentifizierung (MFA) identifiziert werden. MFA ist für die folgenden Fälle **zwingend**: • Nutzung von privilegierten Accounts z.B. Administratoren. • Zugriffe aus nicht vertrauenswürdigen Netzen (z.B. Internet, Remote Access, Support Zugänge) auf nicht öffentliche Daten und Informationen der Uni Bern. • Zugriffe von unbekannten Geräten (z.B. BYOD) auf Daten und Informationen der Universität Bern.	TV/ID
3	Passwörter müssen mindestens 12 Zeichen (Für Admin-Accounts 14 Zeichen) enthalten und eine Kombination von, drei der nachfolgenden vier Elemente, enthalten. (Grossbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen) und sind technisch zu erzwingen.	TV/ID
4	Nach 10 ungültigen Anmeldeversuchen muss ein Account für eine gewisse Zeit blockiert werden.	TV/ID

5	Für die Erstanmeldung neuer Benutzerinnen oder Benutzer müssen zufällig generierte Initial-Passwörter vergeben werden, die nach einmaligem Gebrauch gewechselt werden müssen. Die Anforderung ist, wenn möglich, technisch zu erzwingen.	TV/ID
6	Passwörter dürfen nicht im Klartext übertragen oder gespeichert werden. Für die Speicherung von Passwörtern muss ein sicherer Passwort-Hashing Algorithmus mit Salt (zufällig gewählte Zeichenfolge) verwendet werden. Die Anforderung ist, wenn möglich, technisch zu erzwingen.	TV/ID
7	Passwörter sind persönlich und dürfen nicht weitergegeben werden. Geschäftliche Passwörter dürfen nicht für private Zwecke genutzt werden.	Benutzer
8	Wenn immer möglich ist auf die Nutzung von lokalen Accounts zu verzichten und ein zentrales Directory zu verwenden. Lokale Accounts sind zu dokumentieren und einer verantwortlichen Person zuzuweisen.	TV/ID
9	Es sind Abläufe zu etablieren (wenn möglich automatisiert), die sicherstellen, dass Benutzer-Accounts (lokale und zentrale): • bei einem Austritt (Kündigung) auf das Austrittsdatum deaktiviert oder gelöscht werden. • bei einem Express Austritt (fristlose Kündigung, Freistellung) die Deaktivierung der Identität/Account) unmittelbar erfolgt.	TV/ID
10	Nicht genutzte Benutzer-Accounts sind zu löschen oder, wenn dies zwecks Nachvollziehbarkeit nicht möglich ist, zu deaktivieren.	TV/ID
11	Privilegierte Aktivitäten müssen mittels spezifischen Administratoren-Accounts oder dokumentierten, bestellbaren, zeitlich begrenzten, protokollierten und MFA geschützten, privilegierten Rollen ausgeführt werden. Allgemeine Aktivitäten wie Surfen im Internet, Bearbeiten von E-Mails oder die Nutzung von Office Applikationen, sind mit dem persönlichen, nicht privilegierten, Benutzer-Account auszuführen.	TV/ID
12	Unpersönliche Accounts z.B. Service Accounts sind nach Möglichkeit zu vermeiden. Wenn doch nötig, sind die Accounts zu dokumentieren (Begründung, Datum, Laufzeit, verantwortliche Person) und einer technikverantwortlichen Person zuzuweisen.	TV/ID
13	Für unterschiedliche Systemservices sind dedizierte Service Accounts mit den jeweilig notwendigen Privilegien zu verwenden. Derselbe Account darf nicht mehrere Systemdienste und Programme ausführen.	TV/ID

6.5 Rollen und Berechtigungen

Nr.	Vorgabe	Zuständig
1	Es bedarf eines transparenten Antrags- und Genehmigungsverfahrens für die Vergabe von Berechtigungen und Rollen auf vertraulich/streng vertraulich klassifizierte Informationen. Die Vergabe von Berechtigungen und Rollen muss geplant und in einem Berechtigungskonzept pro Applikation dokumentiert und aktuell gehalten werden.	IE
2	Es ist sicherzustellen, dass bei Eintritt, Übertritt und Austritt von Mitarbeitenden (inkl. externer Mitarbeitenden) die Berechtigungen überprüft und wenn nötig entzogen werden.	IE
3	Die Vergabe von Berechtigungen erfolgt gemäss dem Need-to-Know Prinzip und hat über etablierte und dokumentierte Prozesse zu erfolgen.	IE

	Bei der Vergabe der Berechtigungen ist die Klassifizierung der Daten und Informationen zu berücksichtigen.	
4	Die Berechtigungen sind periodisch oder bei Änderungen, jedoch mindestens jährlich zu überprüfen und nachvollziehbar zu dokumentieren.	IE

6.6 Technisches Schwachstellenmanagement

Nr.	Vorgabe	Zuständig
1	Es ist ein Prozess inkl. Rollen zu etablieren, der sicherstellt, dass technische Schwachstellen in ICT-Systemen erkannt und in angemessener Zeit behoben werden. Massgebend für die Reaktionszeit und Priorisierung von Schwachstellen sind folgende Faktoren: • Schweregrad der Schwachstelle basierend auf CVSS-Score; • Exposition des betroffenen ICT- Betriebsmittels • Kritikalität des betroffenen ICT-Systems	TV[1]/ID
2	Ein Schwachstellen-Scan muss regelmässig, jedoch mindestens vier Mal pro Jahr erfolgen.	TV/ID
3	Es müssen Patching-Verfahren etabliert sein, die sicherstellen, dass: • Notfall-Patches (0-Day) innerhalb von 24h, • Hochkritische Schwachstellen (CVSS 7-10) innerhalb von 30 Tagen, • kritische (CVSS 4.1-6.9) innerhalb von 60 Tagen • und allen übrigen innerhalb von 180 Tagen geschlossen oder alternative Schutzmassnahmen implementiert werden.	TV/ID

6.7 ICT-Infrastruktur

Nr.	Vorgabe	Zuständig
1	Die Software der ICT-Systeme (z.B. Applikationen, Middleware. Endgeräte, Netzwerkkomponenten) ist aktuell zu halten (vom Hersteller empfohlener stabiler Release einer unter Wartung stehenden Major Version).	TV/ID
2	Es darf nur vom Hersteller unterstützte Software und Hardware eingesetzt werden.	TV/ID
3	Softwarefehler und Schwachstellen müssen von den Herstellern in angemessener Frist behoben beziehungsweise geschlossen werden. Es müssen entsprechende Vereinbarungen mit den Herstellern getroffen und gegebenenfalls erneuert werden.	TV/ID
4	Defekte Hardware muss in nützlicher Frist, abhängig von den Verfügbarkeitsanforderungen, ersetzt werden. Es müssen entsprechende Vereinbarungen mit den Herstellern getroffen oder genügend Ersatzmaterial beschafft werden.	TV/ID
5	ICT-Systeme müssen sicher konfiguriert werden (Hardening), bspw. gemäss Empfehlung der Hersteller oder gemäss Hardening Guidelines	TV/ID

[1] Die Gruppe NETSEC der Informatikdienste betreibt eine Infrastruktur für das Scannen technischer Schwachstellen und steht für Unterstützung zur Verfügung.

	z.B.ID-Hardening Guidelines oder CIS-Benchmarks. Mindestanforderungen sind: • Best Practice vom Hersteller ist zu berücksichtigen. • Es dürfen nur Dienste (Software) installiert respektive aktiviert sein, die für den vorgesehenen Betrieb des Systems notwendig sind. Keine Installation/Aktivierung auf Vorrat. • Vorkonfigurierte Accounts (z.B. Gast) sind zu löschen oder zu deaktivieren. • Services dürfen nur die Berechtigungen haben, die sie benötigen (keine Root/Admin Rechte). • Initial-Passwörter müssen gewechselt werden. • Fehler- und Debug-Meldungen für Endbenutzer ausschalten und nur bei Bedarf aktivieren.	
6	Entwicklungs-, Integrations- und Produktionsumgebungen sind voneinander zu trennen.	TV/ID
7	Eine Trennung zu Systemen, welche von anderen Kunden oder Mandanten benutzt werden, ist sicherzustellen.	TV/ID
8	ICT-Systeme sind entsprechend den in der *Schutzbedarfsanalyse* festgelegten Verfügbarkeitskriterien auszulegen. D.h. kritische ICT-Systeme sind hochverfügbar und/oder standortredundant aufzubauen.	TV/ID
9	Es dürfen nur Softwarebibliotheken (z.B. dll, ocx, so Dateien) aus vertrauenswürdigen Quellen genutzt werden.	TV/ID
10	Datenträger müssen sicher entsorgt bzw. vernichtet werden. Es sind geeignete Abläufe zu etablieren.	TV/ID

6.8 Applikationssicherheit/Softwareentwicklung

Nr.	Vorgabe	Zuständig
1	Die Anforderungen an die Sicherheit von Anwendungen richten sich nach den jeweils aktuellen Empfehlungen (De-Facto-Standards) gemäss *O-WASP*. Diese Grundlagen sind im gesamten Entwicklungs- und Betriebsprozess unter Berücksichtigung von Risiko und Wirtschaftlichkeit angemessen zu berücksichtigen.	TV/ID
2	Der Zugriff auf Repositorien ist klar zu regeln und auf ein Minimum zu beschränken.	TV/ID
3	Software muss vor der Einführung und nach jedem grösseren Release systematisch getestet werden.	TV/ID
4	Applikationen, die Zugriff auf zentrale Systeme nehmen, sind vor einer Anschaffung, Inbetriebnahme oder Nutzung durch die Informatikdienste zu genehmigen. Bei datenschutzrechtlichen Risiken sind der/die CISO und der Rechtsdienst zu involvieren.	TV

6.9 Malware Defense

Nr.	Vorgabe	Zuständig
1	ICT-Systeme müssen Massnahmen zur Erkennung und Abwehr von Malware implementieren.	TV/ID

	• Signatur und verhaltensbasierte Erkennung sollten unterstützt werden. • Die Programme sind regelmässig zu aktualisieren. Bei der Nutzung von austauschbaren Medien (z.B. USB-Stick) ist immer vorgängig ein Malware-Scan durchzuführen.	
2	E-Mails inkl. Anhänge sind vor der Zustellung in die Mailbox auf Malware zu untersuchen.	TV/ID
3	Es sind Massnahmen zu implementieren, die Fälschen oder Verändern von E-Mails verhindern.	TV/ID
4	Es muss sichergestellt werden, dass nur aktuelle und vom Hersteller unterstützte E-Mail-Clients und Webbrowser genutzt werden.	TV/ID
5	Zur DNS-Auflösung müssen die zentralen DNS-Server der Informatikdienste verwendet werden. So wird sichergestellt, dass die DNS-Firewall von Switch verwendet wird. Interne DNS-Server in Institutionen müssen rekursive Anfragen an die zentralen DNS-Server der Informatikdienste weiterleiten. (DNS Forwarding)	TV/ID
6	Unnötige Filetypen sind auf dem Mailserver zu blockieren.	TV/ID

6.10 Datensicherheit

Nr.	Vorgabe	Zuständig
1	Informationen und *Informationssammlungen* müssen bezüglich Vertraulichkeit, Verfügbarkeit und Integrität klassifiziert werden. Mittels der Schutzbedarfsanalyse wird der Schutzbedarf von Informationen/Informationssammlungen ermittelt.	IE
2	*Sensitive Daten* müssen während der Übertragung verschlüsselt werden.	TV/ID
3	Datenträger müssen verschlüsselt werden.	TV/ID
4	Sensitive Daten im Ruhezustand (at Rest) auf Servern, Anwendungen und Datenbanken müssen auf Client oder Applikationsebene verschlüsselt werden.	TV/ID
5	Auf Endgeräten (Notebook, PC, Mobiltelefon, usw.) sollen keine sensitiven Daten gespeichert werden. Falls doch, muss das Endgerät verschlüsselt werden z.B. mit, (Windows BitLocker®, Apple FileVault® oder Linux® dm-crypt).	TV/ID
6	Basierend auf den geltenden gesetzlichen und betrieblichen Anforderungen soll ein Datenverwaltungsprozess etabliert werden. Der Prozess soll sicherstellen, dass ein Dateneigentümer/Informationseigner bestimmt ist und dass Aufbewahrungs- und Löschvorschriften bekannt sind und eingehalten werden.	GD
7	Die Verarbeitung und Speicherung von sensitiven Daten soll von nicht sensitiven Daten (technisch oder organisatorisch) getrennt werden.	TV/ID
8	Alle Informationssammlungen mit hohem Schutzbedarf müssen inventarisiert und dem CISO gemeldet werden.	ISO
9	Personendaten gemäss *DSG/KDSG*, auf Entwicklungs- und Test-Systemen, müssen anonymisiert oder synthetisiert werden.	TV/ID
10	Können Test- oder Entwicklungsdaten nicht anonymisiert oder synthetisiert werden, müssen dieselben Sicherheitsmassnahmen eingehalten	TV/ID

	werden wie im Produktions-Umfeld (Kompletter Grundschutz inkl. Berechtigungen).	

6.11 Netzwerksicherheit

Nr.	Vorgabe	Zuständig
1	Der Zugriff auf sensitive Daten im Netzwerk, muss mittels Firewalls auf das nötigste eingeschränkt werden (Ausgehender und eingehender Datenverkehr).	TV/ID
2	Wenn möglich und unterstützt, sind «lokale» Firewalls auf Servern zu aktivieren und zu verwalten.	TV/ID
3	Firewalls auf Endgeräten der Benutzerin oder des Benutzers müssen aktiviert und verwaltet werden.	TV/ID
4	Netzwerkverkehr zu kritischen Systemen und sensitiven Daten muss authentifiziert und autorisiert werden.	TV/ID
5	Das Netzwerk muss in verschiedene Netzwerkzonen (Segmentierung) aufgeteilt werden.	ID
6	Jede Netzwerkzonentyp muss über eine Policy verfügen. Die Policy sollte mindestens folgendes regeln: - Name der Zone - Eingehender und ausgehender Datenverkehr - Authentifizierung von Netzwerkverkehr - Aufzeichnungslevel (Was wird geloggt) - Monitoring (Was wird überwacht)	ID
7	Der Netzwerkverkehr in und aus Netzwerkzonen mit kritischen ICT-Systemen ist zu überwachen und zu protokollieren.	TV/ID
8	Es muss eine Netzwerkdokumentation vorhanden sein und aktuell gehalten werden.	ID
9	Remote Zugriffe ins Netzwerk der Universität Bern müssen über einem zentralen Gateway geführt, verschlüsselt, authentifiziert und aufgezeichnet (Logfiles) werden. Zudem sollte ein Zugriff nur auf die benötigten Systeme erlaubt werden.	ID
10	Wo immer möglich ist eine Transportverschlüsselung zu implementieren und sichere Protokolle zu nutzen. (z.B. SFTP anstelle von FTP).	TV/ID

6.12 Backup, Restore

Nr.	Vorgabe	Zuständig
1	Betrieblich notwendige Daten und Konfigurationsdateien von Applikationen und Systemen sind gemäss den geschäftlichen Verfügbarkeitsanforderungen (Siehe RPO in Schutzbedarfsanalyse regelmässig (automatisiert) zu sichern.	TV/ID
2	Der Restore von Backup-Daten ist regelmässig zu testen.	TV/ID
3	Backupdaten sind vor Malware/Ransomware zu schützen. Es ist mittels Offline-Lagerung oder sonstigen Massnahmen (z.B. Air-Gap, dedizierte Netzwerkzone) sicherzustellen, dass Backup-Daten nicht durch Malware/Ransomware gefährdet sind.	TV/ID

6.13 Protokollierung und Monitoring

Nr.	Vorgabe	Zuständig
1	Logs von am Internet exponierten Systemen sind an eine Security Log/Monitoring Infrastruktur anzubinden.	TV/ID
2	Logs von Systemen mit sensitiven Daten sind an eine Security Log/Monitoring Infrastruktur anzubinden.	TV/ID
3	Veränderungen an Systemkonfigurationen (in Applikationen und IT-Systemen) sind durch die Systeme zu protokollieren.	TV/ID
4	Logfiles von kritischen ICT-Systemen oder ICT-Systeme mit sensitiven Daten sind 180 Tage aufzubewahren.	TV/ID
5	Der Zugriff auf sensitive Daten muss nachvollziehbar sein (Logs).	TV/ID

6.14 Notfallplanung

Nr.	Vorgabe	Zuständig
1	Für alle Schutzobjekte, die einen relevanten Geschäftsprozess unterstützen, ist ein Notfallplan zu erstellen. Der Notfallplan beschreibt die Planung und Katastrophenvorsorge des Schutzobjekts, um die Aufrechterhaltung und Wiederherstellung der Geschäftsfähigkeit in ausserordentlichen Situationen zu gewährleisten. Die Relevanz eines Geschäftsprozess kann mittels einer Schutzbedarfsanalyse, einer Business Impact Analyse oder einer Risikoanalyse ermittelt werden.	IE/TV/ID

6.15 Physische Sicherheit

Nr.	Vorgabe	Zuständig
1	ICT-Systeme (Userendgeräte bilden eine Ausnahme) müssen in dafür vorgesehenen Räumen betrieben werden. Folgende Sicherheitsmassnahmen müssen berücksichtigt werden: • Zutritte nur für Berechtigte – Es werden nur identifizierte Personen berechtigt, die im Rahmen ihrer geschäftlichen Tätigkeit den Zutritt auch tatsächlich benötigen. • Regelmässige Kontrolle der Zutrittsberechtigungen • Zutritte sollen nachvollziehbar sein (z.B. mittels Badge System) und protokolliert werden. Die Logs sind mind. 180 Tage aufzubewahren • Raumsichernde Massnahmen bei Fenstern und Türen • Brandmeldeanlage • Brandabschottungen/Brandabschnitte • (Hoch-)Wasserschutz • Überspannungsschutz • Klimakontrolle	GD

6.16 Outsourcing/Cloud

Nr.	Vorgabe	Zuständig
1	Mit jedem ICT-Dienstleister muss ein Vertrag abgeschlossen werden, der, abhängig von der bezogenen Dienstleistung, «mindestens» die nachfolgenden Aspekte regelt: • Wartung und Support • Lizenz-Management • Informationssicherheits- und Datenschutzvorgaben (AGB/ISDS) • Meldung von Sicherheits- und Datenschutzvorfällen • Katastrophen- und Notfallvorsorge (bei kritischen Dienstleistungen) • Audit und Prüfrecht • Vertraulichkeitsvereinbarung • Regelung Auftragsdatenbearbeitung (bei Bearbeitung von Personendaten)	GD
2	Es muss ein Inventar aller externen Service-Dienstleistern und Services erstellt und aktuell gehalten werden. Das Inventar muss mindestens die folgenden Angaben enthalten: • Dienstleister • Ansprechpersonen • Kritikalität der Dienstleistung und ausgelagerten Daten	ISO
3	Bei der Auslagerung von kritischen Dienstleistungen oder von sensitiven Daten/Informationen muss im Vorfeld zusätzlich eine Risikoanalyse durchgeführt werden, in der insbesondere die wesentlichen Aspekte von Datenschutz und Informationssicherheit überprüft werden. Weiter muss eine Exitstrategie erstellt werden, die aufzeigt, wie die Dienstleistungen/Daten im Notfall zurückgenommen oder an einen anderen Partner ausgelagert werden können.	GD

7. Glossar/Referenzierte Dokumente

Begriffe/Abkürzungen	Beschreibung
AGB/ISDS	Allgemeine Geschäftsbedingungen (AGB) in Bezug auf ISDS bei der Erbringung von Informatikdienstleistungen für die Informatikdienste der Universität Bern.
CIS Controls	Die CIS Controls (ehemals CIS Critical Security Controls) sind eine Sammlung empfohlener Sicherheitsmassnahmen zur Abwehr der verbreitetsten und gefährlichsten Cyber-Angriffe.
CIS Controls UniBE	Sheet zur Durchführung einer Gap-Analyse und zur Ermittlung von Risiken.
ICT-Systeme	Informations- und Kommunikationstechnologie ICT oder IKT auf Deutsch: Alle Geräte (Hardware) und Anwendungen (Software) zur Speicherung, Verarbeitung und Übermittlung von Daten, Informationen und Sprache.
Informationssammlungen	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.
ISDS-Konzept	Im ISDS-Konzept wird dokumentiert, wie die Sicherheits- und Datenschutzmassnahmen (z.B. der Grundschutz) für ein bestimmtes Schutzobjekt/Informationssammlung umgesetzt werden.
OWASP	Das Open Worldwide Application Security Project (OWASP) ist eine offene Gemeinschaft, die sich dafür einsetzt, dass Unternehmen vertrauenswürdige Anwendungen und APIs entwickeln, erwerben und pflegen können.
Risikoanalyse	Dokument zur Einschätzung und Dokumentation von ICT-Risiken
RPO	Recovery Point Objective = Maximaler Datenverlust
RTO	Recovery Time Objective = Wiederanlaufzeit
Schutzbedarfsanalyse	SchuBAn - Ein Hilfsmittel zur Identifikation von kritischen, sensitiven Daten und Informationen.
Sensitive Daten/Informationen	Sind Daten/Informationen, die gemäss Schutzbedarfsanalyse einen erhöhten Schutzbedarf aufweisen.
Technische Ressourcen	Sind ICT-Systeme, Funktionen oder Dienste eines ICT-Systems.
Weisungen Governance Informationssicherheit	Die Weisungen Governance Informationssicherheit legen die elementaren Ziele, Grundsätze, Zuständigkeiten und Prozesse der Informationssicherheit an der Universität Bern fest.
Kritische Systeme/Dienstleistungen	Sind Anlagen, Systeme oder Teile davon, die für die Aufrechterhaltung wichtiger Funktionen und Dienstleistungen an der Universität Bern von wesentlicher Bedeutung sind.
Besonders schützenswerten Personendaten	Um besonders schützenswerte Personendaten handelt es sich bei: Angaben über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, über die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, über Massnahmen der sozialen Hilfe und über administrative oder strafrechtliche Verfolgungen und Sanktionen. Persönlichkeitsprofile: Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt. Profiling: automatisierte Bearbeitung von Personendaten, um bestimmte

	persönliche Aspekte zu bewerten, zu analysieren oder vorherzusagen. Genetische Daten und biometrische Daten, die eine natürliche Person eindeutig identifizieren.
DSG/ KDSG	Das DSG, ist das eidgenössische Datenschutzgesetz und gilt für Private und Bundesorgane. Das KDSG ist das kantonale Datenschutzgesetz und gilt für kantonale Behörden wie z.B. die Universität Bern.
Hardening Guidelines	Mindestanforderungen, die zu berücksichtigen sind.

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, 5. Dezember 2023

Namens der Universitätsleitung:

Prof. Dr. Christian Leumann

Rektor