Leitlinie zur Informationssicherheit der Universität Hohenheim

Vom Rektorat in seiner Sitzung vom 21.11.2023 beschlossen,
mit Gültigkeit ab dem 22.11.2023.

Inhalt

1. Einleitung 3
2. Ziel und Zweck der Leitlinie zur Informationssicherheit 3
3. Geltungsbereich 3
   3.1. Informationssicherheitsziele und -grundsätze 4
   3.2. Grundlegende und erweiterte Schutzziele der Informationssicherheit 4
   3.3. Aufgaben und Ziele der Informationssicherheit 5
   3.4. Technische Sicherheitsmaßnahmen 6
   3.5. Organisatorische Sicherheitsmaßnahmen 8
4. Verantwortlichkeiten 10
   4.1. Universitätsleitung 10
   4.2. Stabsstelle Informationssicherheit (CISO/ISB) 10
   4.3. Leitung der Organisationseinheit 10
   4.4. Systembetreuer:innen 11
   4.5. Datenschutzbeauftragte:r 11
   4.6. Nutzer:innen 11
5. Überprüfung, Audit und Verbesserung 12
6. Inkraftreten 12

1. Einleitung

Die Informationssicherheit hat in der heutigen, hochgradig vernetzten Welt eine signifikante Bedeutung erlangt. Die Hauptziele der Informationssicherheit bestehen darin, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und IT-Infrastruktursystemen zu schützen und zu gewährleisten. Die vorliegende Leitlinie zur Informationssicherheit legt die Grundsätze und Anforderungen für die Informationssicherheit an der Universität Hohenheim fest und bietet Verhaltens- und Handlungsgrundsätze für die Umsetzung von Sicherheitsmaßnahmen. Um die Informationssicherheitsziele zu erreichen und ein ausreichendes und angemessenes Sicherheitsniveau zu etablieren, werden die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zugrunde gelegt und an die Gegebenheiten der Universität Hohenheim angepasst.

2. Ziel und Zweck der Leitlinie zur Informationssicherheit

Die Leitlinie zur Informationssicherheit ist ein zentrales Referenzdokument für die Informationssicherheitsarchitektur der Universität Hohenheim. Sie beschreibt verbindliche Prinzipien und das anzustrebende Niveau für IT- und Informationssicherheit an der Universität Hohenheim zur Stärkung der Cyber-Resilienz. Sie bildet die Grundlage für die Erstellung weiterer, auch fachspezifischer Richtlinien, Informationssicherheitskonzepte, detaillierter Regelungen und Dienstanweisungen zur Sicherstellung der Ziele der Informationssicherheit.

3. Geltungsbereich

Der Geltungsbereich dieser Leitlinie zur Informationssicherheit umfasst alle Systeme, Netzwerke, Anwendungen, Daten und Informationen, die von der Universität Hohenheim verwaltet, verarbeitet oder gespeichert werden. Sie richtet sich an alle Mitglieder und Angehörige der Universität Hohenheim, einschließlich der Studierenden, Dozierenden und Beschäftigten, sowie an externe Auftragnehmer und Dritte, welche Zugriff auf diese Ressourcen haben (im folgenden Nutzer:innen).

3.1. Informationssicherheitsziele und -grundsätze

Informationssicherheit bezieht sich auf den Schutz von Informationen vor unbefugtem Zugriff, Offenlegung, Veränderung, Zerstörung oder sonstigen Bedrohungen. Sie soll die Vertraulichkeit, Integrität und Verfügbarkeit dieser Informationen gewährleisten. Dazu ist ein multidisziplinärer Ansatz, der technische, organisatorische und personelle Maßnahmen bzw. Verantwortungen umfasst, erforderlich. Im Folgenden werden die grundlegenden Informationssicherheitsziele (Vertraulichkeit, Integrität, Verfügbarkeit), die erweiterten Informationssicherheitsziele und -grundsätze (Authentizität, Nicht-Abstreitbarkeit, Verbindlichkeit) sowie die Aufgaben und Ziele der Informationssicherheit (Zuverlässigkeit, Risikomanagement, Bewusstsein der Beschäftigten, Kontinuierliche Verbesserung) dargestellt:

3.2. Grundlegende und erweiterte Schutzziele der Informationssicherheit

Vertraulichkeit

Informationen sind vor unbefugtem Zugriff, Offenlegung oder unbefugter Nutzung zu schützen. Der Grundsatz der Vertraulichkeit stellt sicher, dass nur autorisierte Personen Zugriff auf bestimmte Informationen haben.

Integrität

Informationen müssen vollständig, korrekt und unverfälscht sein. Der Grundsatz der Integrität bezieht sich darauf, dass Informationen vor unbefugter Änderung oder Manipulation geschützt werden, um sicherzustellen, dass sie zuverlässig und vertrauenswürdig sind.

Verfügbarkeit

Informationen sollten jederzeit für autorisierte Nutzer:innen zugänglich sein, wenn sie benötigt werden. Der Grundsatz der Verfügbarkeit stellt sicher, dass Systeme, Netzwerke und Datenverarbeitungsdienste zuverlässig und kontinuierlich verfügbar sind, um die Geschäftsprozesse der Universität zu unterstützen.

Authentizität

Die Identität von Nutzer:innen, Systemen und Netzwerken müssen verifiziert werden, um sicherzustellen, dass nur legitime und autorisierte Personen und Systeme Zugriff erhalten. Der Grundsatz der Authentizität bezieht sich darauf, dass die Identität einer Person oder eines Systems überprüft und bestätigt wird.

Nicht-Abstreitbarkeit

Handlungen und/oder (Trans-)Aktionen müssen zum Schutz der beteiligten Parteien nachvollziehbar sein. Bei der Nicht-Abstreitbarkeit liegt der Fokus auf der Nachweisbarkeit gegenüber Dritten. Das kann durch den Einsatz von kryptografischen Signaturen, digitalen Zertifikaten, Protokollierung und anderen Sicherheitsmechanismen erreicht werden, um sicherzustellen, dass die Integrität und Authentizität von Handlungen und/oder (Trans-)Aktionen überprüfbar sind und keine der beteiligten Parteien diese später bestreiten oder leugnen können, sofern ein Nachweis gegenüber Dritten erforderlich ist.

Verbindlichkeit

Das Informationssicherheitsschutzziel der Verbindlichkeit vereint die beiden erweiterten Schutzziele der Authentizität und Nicht-Abstreitbarkeit. Der Grundsatz der Verbindlichkeit bezieht sich auf die Notwendigkeit, dass Handlungen, Entscheidungen und Vereinbarungen (in Bezug auf die Informationssicherheit) eindeutigen Identitäten zugeordnet werden können, um die an der Universität Hohenheim geltenden Sicherheitsregeln und -maßnahmen rechtsverbindlich durchzusetzen.

3.3. Aufgaben und Ziele der Informationssicherheit

Zuverlässigkeit

Zuverlässigkeit stellt ein grundlegendes Prinzip der Informationssicherheit dar und bezieht sich auf die Fähigkeit eines Systems, seine beabsichtigten Aufgaben und (Sicherheits-)Funktionen unter den vorgegebenen Bedingungen und innerhalb eines vorhersehbaren Zeitrahmens verlässlich zu erfüllen ohne unerwartete Ausfälle oder Störungen.

Risikomanagement

Der Grundsatz des Risikomanagements bezieht sich darauf, dass Sicherheitsrisiken identifiziert, bewertet und angemessen behandelt werden. Für alle Informationsverbünde (Dienste und Systeme) sollten angemessene Risikobewertungen durchgeführt und geeignete Sicherheitsmaßnahmen ergriffen werden, um Risiken zu minimieren.

Bewusstsein der Nutzer:innen

Nutzer:innen sollten über ihre Verantwortlichkeiten (spezifische Aufgaben, Rollen und/oder Pflichten) im Hinblick auf Informationssicherheit geschult und sensibilisiert werden. Der Grundsatz des Bewusstseins der Nutzer:innen bezieht sich darauf, dass

diese über Sicherheitsrichtlinien, -verfahren und Vorgehensweisen informiert und sich ihrer Rolle bzw. Verantwortung zum Schutz von Informationen bewusst sind.

Kontinuierliche Verbesserung

Die Informationssicherheit sollte als ein partizipativer, wiederkehrender Prozess gesehen und verstanden werden, um mit den sich ständig ändernden Bedrohungsszenarien und Technologien Schritt zu halten. Der Grundsatz der kontinuierlichen Verbesserung erfordert, dass Sicherheitsmaßnahmen regelmäßig überprüft, aktualisiert und an neue Bedrohungen und Technologien angepasst werden.

3.4. Technische Sicherheitsmaßnahmen

Technische Sicherheitsmaßnahmen und Mechanismen sind essenziell, um die Sicherheit von IT-Systemen, Netzwerken, Daten und Informationen zu gewährleisten. Sie ergänzen die organisatorischen Sicherheitsmaßnahmen und helfen auf technischer Ebene dabei, Bedrohungen zu minimieren, Angriffe sowie Manipulationsversuche zu erkennen und die Informationssicherheit infrastrukturell zu gewährleisten.

Im Folgenden werden die technischen Sicherheitsmaßnahmen dargestellt:

Zugriffskontrolle

An der Universität Hohenheim sind Mechanismen zur Authentifizierung und Autorisierung implementiert, um sicherzustellen, dass nur autorisierte Nutzer:innen Zugriff auf Informationen und Systeme haben. Die Zugriffskontrolle wird durch die Verwendung von Zugangsprofilen, starken Passwörtern, Zwei-Faktor-Authentifizierung, biometrischer Identifikation und Zugangsberechtigungen realisiert.

Verschlüsselung

Um Informationen während der Übertragung, Speicherung oder Verarbeitung zu schützen, kommen dem aktuellen Stand der Technik entsprechende soft- oder hardwarebasierte Verschlüsselungstechnologien zum Einsatz. Dies gewährleistet, dass Informationen nur von autorisierten Nutzer:innen gelesen oder verstanden werden können.

Firewalls und Intrusion Detection/Prevention System (IDS/IPS)

Der Einsatz von Firewall-Systemen und Intrusion Detection/Prevention-Systemen (IDS/IPS) sowie weiteren Protokollen und Sicherheitsmechanismen dienen der Identifizierung von Angriffen und ungewöhnlichen Aktivitäten in der Netzwerkinfrastruktur. Der ein- und ausgehende Netzwerkverkehr wird dadurch vor unbefugtem Zugriff und Sicherheitsverletzungen geschützt. Durch die Kontrolle des

Datenverkehrs auf bekannte Angriffsmuster wird eine proaktive und automatisierte Reaktion auf potenzielle Bedrohungen realisiert.

Malware-Schutz

Der Einsatz von Antivirus- und Anti-Malware-Software und weiteren Client-/Server-Sicherheitslösungen minimiert das Risiko von Malware-Infektionen und den damit einhergehenden Schäden. Der flächendeckende Einsatz einer Antivieren-Lösung wird daher dringend empfohlen.

Sicherheitspatches und Updates

Um bekannte Schwachstellen zu beheben und Sicherheitslücken zu schließen, werden durch die System- und Anwendungsverantwortlichen regelmäßig Aktualisierungen an den Infrastruktursystemen durchgeführt. Updateverfahren, die zu einer Unterbrechung des Regelbetriebs führen, werden - soweit es die Sicherheitslage zu lässt - in Form eines Wartungsfensters angekündigt und kommuniziert. Spürbare Unterbrechungen in der Verfügbarkeit der Systeme für den Zeitraum der Aktualisierung sind bei einem kontinuierlichen Dienstangebot unvermeidbar.

Dezentral betriebene Geräte, dazu gehören insbesondere auch die Geräte der Nutzer:innen wie Desktop-PCs und Laptops sowie andere mobile Geräte, sollten nach den gleichen Prinzipien gepflegt werden. Empfohlen wird, regelmäßig Sicherheitspatches und Updates durchzuführen bzw. die Ausführung der Installation zu überprüfen. Sofern möglich, sollten die automatischen Aktualisierungsfunktionen verwendet werden. Zur Behebung besonders (zeit-)kritischer Schwachstellen erforderliche Sicherheitspatches und Updates werden von der Informationssicherheit u.a. über kurz gemeldet mitgeteilt. Es wird dringend empfohlen, diese Sicherheitspatches und Updates zeitnah einzuspielen.

Datensicherung

Durch den Einsatz von speziellen Backup-Systemen und -Verfahren stellt die Universität den Nutzer:innen eine hausinterne Möglichkeit zur Verfügung, wichtige Daten vor Verlust oder Beschädigung zu schützen und im Bedarfsfall wiederherstellen zu können. Den Nutzer:innen wird daher empfohlen, wichtige Daten (Dateien) auf den von der Universität Hohenheim zentral zur Verfügung gestellten Netzlaufwerken zu speichern.

Monitoring und Protokollierung

In der IT-infrastruktur (Gebäude, Kommunikationsdienste, Maschinen und Programme) der Universität Hohenheim werden an neuralgischen Knotenpunkten Monitoring- und Protokollierungssysteme zur frühzeitigen Erkennung von Sicherheitsverletzungen eingesetzt, um Sicherheitsvorfälle zu erkennen, Aktivitäten zu beobachten, Angriffe zu verfolgen und Sicherheits-Audits durchzuführen. Die Protokollierung stellt außerdem eine wichtige Grundlage für forensische Untersuchungen nach einem Sicherheitsvorfall dar.

Physische Sicherheit

Die Universität realisiert durch die Implementierung von Sicherheitsmaßnahmen den Schutz ihrer physischen Ressourcen wie Serverräumen, Rechenzentren, Datenzentren. Entsprechende Zugangskontrollen zu sensiblen Bereichen stellen sicher, dass nur autorisierte Personen Zugang haben.

3.5. Organisatorische Sicherheitsmaßnahmen

Die organisatorischen Sicherheitsmaßnahmen sind entscheidend dafür, ein robustes Sicherheitsumfeld zu schaffen. Sie ergänzen die technischen Sicherheitsmaßnahmen und ermöglichen es, eine homogene Sicherheitskultur an der Universität Hohenheim zu etablieren, in der personelle und technische Organisationskapazitäten wirksam geschützt sind.

Im Folgenden werden die organisatorischen Sicherheitsmaßnahmen dargestellt:

Informationssicherheitsrichtlinien

Die Universität Hohenheim erstellt, als Komplement zu der vorliegenden Leitlinie für Informationssicherheit, weitere Richtlinien, die klare Anweisungen und Regeln für den Schutz von Informationen und Systemen festlegen (z. B. Passwortrichtlinie). Diese Richtlinien legen Standards, Verantwortlichkeiten und Verfahren fest, die von allen Nutzer:innen der Universität befolgt werden müssen.

Sicherheitsbewusstsein und Schulungen

Die Stabsstelle Informationssicherheit informiert regelmäßig durch das Angebot von Schulungen, Trainings, Sensibilisierungskampagnen und interne Kommunikationsmittel (E-Mails, Newsletter, Intranet-Beiträge etc.) die Nutzer:innen der Universität über die aktuelle IT-Sicherheitslage. Dies umfasst auch die Vermittlung von Kenntnissen über Bedrohungen, Sicherheitsrisiken, Phishing-Angriffe, Passwortsicherheit, sicheres Verhalten im Internet und die Identifizierung von Sicherheitsbedrohungen. Um die Erfüllung ihrer Informationsbedürfnisse zu unterstützen, sind die Nutzer:innen der Universität dazu angehalten, ein

Sicherheitsbewusstsein zu entwickeln und sich an einschlägigen Sicherheitsschulungen zu beteiligen. Dies schließt die Bereitschaft ein, die Bedeutung der Informationssicherheit in der Arbeitsumgebung zu verstehen und sicherheitsrelevante Informationen und Schulungen aktiv zu suchen.

Zugriffskontrollen und Identitätsmanagement

Die Universität Hohenheim implementiert Mechanismen zur Kontrolle des Zugriffs auf Informationen und Systeme. Dies umfasst die Vergabe von Berechtigungen und Zugriffsrechten auf der Grundlage der Funktionen und Verantwortlichkeiten der Nutzer:innen sowie die Verwendung von Authentifizierungs- und Autorisierungssystemen.

Incident-Response-Plan

Die Universität Hohenheim hält einen Plan zur Bewältigung von Sicherheitsvorfällen und Störfällen (Incidents) vor. Dieser Plan definiert die Verfahren und Zuständigkeiten für die Erkennung, Reaktion, Untersuchung und Behebung von Sicherheitsvorfällen, um deren Auswirkungen zu minimieren oder zu verhindern.

Notfallwiederherstellungsplan (Business-Continuity-Plan)

Die Universität Hohenheim hält Pläne und Verfahren vor, um die Geschäftsprozesse und den Geschäftsbetrieb in Stör-, Not- oder Katastrophenfällen aufrechtzuerhalten. Dies umfasst unter anderem die Sicherung von Daten durch die Einrichtung von Backup-Systemen, die Verfügbarkeit und Einsatz von Alternativlösungen und die Durchführung von regelmäßigen Notfalltests und Übungen.

Risikomanagement

Die Stabsstelle Informationssicherheit führt gemeinsam mit den Systembetreuer:innen turnusmäßig Risikobewertungen ihrer IT-Verfahren und Infrastruktursysteme durch, um potenzielle Bedrohungen und Schwachstellen zu identifizieren. Aufgrund dieser Bewertungen werden geeignete Maßnahmen geplant und durchgeführt, um Sicherheitsrisiken auf ein akzeptables Niveau zu reduzieren oder gänzlich zu vermeiden.

Lieferanten und Dienstleister

Die Universität Hohenheim stellt sicher, dass Sicherheitsaspekte in Verträgen und Vereinbarungen mit externen Lieferanten und Dienstleistern berücksichtigt werden. Dies umfasst die Einbeziehung von Sicherheitsklauseln, die Überprüfung der Sicherheitspraktiken und -standards der Geschäftspartner sowie die Festlegung von Sicherheitsanforderungen und -kontrollen für die Zusammenarbeit.

4. Verantwortlichkeiten

4.1. Universitätsleitung

- Die Universitätsleitung ist für die Festlegung der Sicherheitsstrategie und -ziele verantwortlich.
- Sie initiiert, steuert und überwacht den Sicherheitsprozess.
- Sie entscheidet über den Umgang mit Risiken und den Einsatz von finanziellen, personellen und zeitlichen Ressourcen.
- Sie übernimmt im Bereich der Informationssicherheit eine Vorbildfunktion und beachtet alle vorgegebenen Sicherheitsregeln.
- Sie unterstützt andere Führungskräfte bei der Ausübung ihrer Vorbildfunktion.

4.2. Stabsstelle Informationssicherheit (CISO/ISB)

- Die Stabsstelle Informationssicherheit vertritt die Interessen der Universitätsleitung gegenüber den Nutzer:innen der Universität und ist für die Wahrnehmung aller Belange der Informationssicherheit der Universität zuständig.
- Sie erstellt auf der strategischen und taktischen Ebene Empfehlungen und prüft deren Einhaltung.
- Sie unterstützt und berät die Universitätsleitung hinsichtlich der Erreichung des angestrebten Sicherheitsniveaus.
- Sie koordiniert und unterstützt bei der Erstellung von Sicherheitskonzepten.
- Sie prüft das IT-Sicherheitsniveau und berichtet an die Universitätsleitung.
- Sie erstellt und prüft Realisierungspläne für geplante Sicherheitsmaßnahmen.

4.3. Leitung der Organisationseinheit

- Die Leitungen der Organisationseinheiten verantworten die Umsetzung der Sicherheitsmaßnahmen im eigenen Bereich.
- Sie ermöglichen, dass Nutzer:innen in ihrem Bereich an Maßnahmen zur Sensibilisierung hinsichtlich der Informationssicherheit teilnehmen können.
- In ihrer Vorbildfunktion unterstützen und motivieren sie ihre Nutzer:innen für Informationssicherheit.
- Sie bewerten Optionen zur Behandlung von identifizierten Risiken.
- Sie melden identifizierte Sicherheitsrisiken und -vorfälle an die Stabsstelle für Informationssicherheit.
- Sie arbeiten eng mit der Stabsstelle Informationssicherheit der Universität Hohenheim zusammen, um die gewählte Sicherheitsstrategie und den Sicherheitsprozess in ihrem Bereich zu etablieren.

4.4. Systembetreuer:innen

- Die Systembetreuer:innen verantworten für ihren Zuständigkeitsbereich die Konfiguration und Verwaltung der Sicherheitseinstellungen und -funktionen in den Anwendungen und IT-Systemen.
- Sie sind verantwortlich für die Umsetzung und Überprüfung der Sicherheits-richtlinien und -standards.
- Sie werten Protokolldaten/Berichte der IT-Systeme aus, um Systemfehler und/oder Sicherheitsvorfälle frühzeitig zu erkennen.
- Sie leiten im Rahmen des Incident-Managements angemessene Maßnahmen zur Begrenzung von Schäden durch Sicherheitsvorfälle ein.
- Sie unterstützen bei der Erstellung von Incident-Response-Plänen.
- Sie melden identifizierte Sicherheitsrisiken und -vorfälle an die Leitung ihrer Organisationseinheit.
- Sie unterstützen bei der kontinuierlichen Verbesserung der Sicherheit der IT-Systeme und IT-Verfahren.

4.5. Datenschutzbeauftragte:r

- Die Datenschutzbeauftragen sind in Übereinstimmung mit den geltenden Datenschutzgesetzen für den Schutz personenbezogener Daten an der Universität Hohenheim verantwortlich.
- Sie überwachen die Einhaltung der Datenschutzbestimmungen.
- Sie unterstützen bei der Erstellung von Datenschutzrichtlinien.
- Sie beraten bei Datenschutzfragen.
- Sie schulen und sensibilisieren die Nutzer:innen der Universität in Bezug auf den Datenschutz.

4.6. Nutzer:innen

- Die Nutzer:innen informieren sich über relevante Sicherheitsrichtlinien und Sicherheitsverfahren (s. Sicherheitsbewusstsein und Schulungen).
- Sie informieren sich über geltende Datenschutzrichtlinien und -gesetze.
- Sie setzen sich für die Einhaltung der Datenschutz- und Sicherheitsrichtlinien und -verfahren ein.
- Sie tragen durch den verantwortungsvollen Umgang mit Informationen und IT-Infrastruktursystemen zur Informationssicherheit bei.
- Sie fördern durch einen bewussten Umgang mit Informationen und IT-Infrastruktursystemen die Informationssicherheit.
- Sie tragen durch die verantwortungsvolle Auswahl und Einsatz von Software und Anwendungen zur Informationssicherheit bei.

- Sie melden verdächtige Aktivitäten oder Sicherheitsvorfälle umgehend ihren Vorgesetzten und der Stabsstelle Informationssicherheit.

5. Überprüfung, Audit und Verbesserung

Die Informationssicherheit ist ein fortlaufender Prozess, welcher ständige Aufmerksamkeit von allen Nutzer:innen der Universität erfordert. Das angestrebte Sicherheitsniveau kann nur erreicht werden, wenn der Informationssicherheitsprozess für den gesamten Geltungsbereich (s. Pkt 3.) umgesetzt wird. Die aus den organisatorischen und technischen Sicherheitsmaßnahmen gewonnen Erkenntnisse dienen dazu, die IT-Sicherheit und Resilienz der Universität Hohenheim in Bezug auf die Cybersicherheitsbedrohungen zu stärken und Informationssicherheitsrisiken zu minimieren. Darüber hinaus werden regelmäßige Überprüfungen, Audits und Aktualisierungen durchgeführt, um sicherzustellen, dass die integrierten Sicherheitsmaßnahmen den aktuellen Bedrohungen und Risiken gerecht werden. Durch die Behebung von Schwachstellen und die Integration neuer Sicherheitslösungen oder -technologien sowie durch ein konsequentes Schulungs- und Weiterbildungsangebot für die Nutzer:innen der Universität wird die Informationssicherheit kontinuierlich verbessert.

6. Inkraftreten

Die Leitlinie für Informationssicherheit wurde verabschiedet, tritt am 22.11.2023 in Kraft und wird mindestens alle zwei Jahre durch den Informationssicherheitsbeauftragten (ISB) der Universität Hohenheim überprüft und aktualisiert.