WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

RL Informationssicherheit

Richtlinie für das WU Informationssicherheitsmanagement

Inhalt

1. Zielsetzung

Die Zielsetzung dieser Richtlinie ist, ein angemessenes Sicherheitsniveau vorzugeben, das einen angemessenen Schutz digitaler und analoger vertraulicher Informationen (nach deren Schutzbedarfsklassifizierung) gewährleistet und Resilienz gegen Cyberattacken erhöht.

2. Geltungsbereich

Die Richtlinie der Informationssicherheit gilt verpflichtend für alle Mitarbeitenden und Studierenden.

Sachlich gilt diese Richtlinie für analoge Informationen und bei Informations- und Kommunikationstechnologie (IKT):

- für bestehende Komponenten und Anwendungen der Informations- und Kommunikationstechnologie (IKT)
- für neue Komponenten und Anwendungen der Informations- und Kommunikationstechnologie (IKT) und
- für die Aktualisierung von Komponenten und Anwendungen der Informations- und Kommunikationstechnologie (IKT)

Partnerinnen und Dienstleister sind in den jeweils relevanten Punkten zu verpflichten.[1]

Darüber hinaus gilt diese Richtlinie bis 30.05.2028 und ohne örtliche Einschränkungen.

3. Glossar

Das Glossar zu dieser Richtlinie findet sich unter https://wiki.wu.ac.at/x/FBoiE

4. Ziele der Informationssicherheit

Die vorliegende Richtlinie für Informationssicherheit unterstützt die Digitalisierungsstrategie der Wirtschaftsuniversität Wien (WU), indem sie die sichere Verarbeitung von vertraulichen Informationen und den ungestörten Universitätsbetrieb gewährleistet.

Ziel ist es, ein Informationssicherheitsniveau zu etablieren, um mögliche Gefährdungen zu erkennen und diese durch entsprechende Maßnahmen auf ein vertretbares Maß zu vermindern sowie die verbleibenden Restrisiken zu ermitteln und nachvollziehbar zu akzeptieren. Diese Ziele sind primär:

- **Risikobetrachtung** - auf Basis einer aktuellen Risikobetrachtung werden aktuelle und zukünftige Cybersecurity-Risiken identifiziert und unter wirtschaftlichen Gesichtspunkten behandelt.
- **Schutz vertraulicher Informationen** - die verarbeiteten vertraulichen Informationen müssen (analog und digital) geschützt werden und dürfen nur Personen zugänglich gemacht werden, die auch über sie verfügen sollen. Das gilt sowohl technisch (z.B.: Schutz vor Cyber-Attacken), als auch organisatorisch (z.B.: Zugriffsberechtigungen).
- **Cybersecurity Resilienz** - die Entwicklung einer Strategie, die im Falle eines Cyberangriffes die Funktion der Basisdienste des Universitätsbetriebes sicherstellt.
- **Compliance** – die Einhaltung des Datenschutzes und anderer geltenden rechtlichen Vorgaben.

[1] Z.B. mittels Vertraulichkeitsvereinbarungen, Zustimmungserklärungen oder Ähnlichem.

Um die dargestellten Ziele zu unterstützen, wird ein Informationssicherheits-Managementsystem (ISMS) in Anlehnung an ISO 27001 eingeführt.

Bei der Implementierung des ISMS setzen wir darauf, das Bewusstsein für Informationssicherheit zu stärken und relevante Fähigkeiten schrittweise zu verbessern. Alle Personen werden entsprechend ihrer Verantwortung, Rolle und Aufgabe sensibilisiert, geschult und trainiert, wobei dabei das Vorwissen der Zielgruppe (Rektorat, Führungskräfte, Leiter*innen der Organisationseinheiten, IT und externe Partnerinnen) berücksichtigt wird und die Inhalte zielgruppengerecht aufbereitet und kommuniziert werden.

Zur Gewährleistung der Informationssicherheit müssen die Infrastrukturen und Prozesse der IT, die für die Verarbeitung von Informationen genutzt werden, ebenso den Sicherheitsanforderungen entsprechen. Die Festlegung der notwendigen IT-Sicherheitsmaßnahmen (zu finden in den WUPOLs, die Teil des ISMS sind: 4.4) erfolgt risikoorientiert und berücksichtigt dabei den aktuellen Stand der Technik.

Das Rektorat betrachtet Informationssicherheit und das resultierende ISMS als Angelegenheit von strategischer Bedeutung und bekennt sich ausdrücklich zur kontinuierlichen Verbesserung und fördert und unterstützt alle notwendigen Aktivitäten und Maßnahmen. Für die Weiterentwicklung der vorliegenden Vorgaben, deren Umsetzung und Etablierung des ISMS sowie die Überprüfung der Einhaltung wird ein Chief Information Security Officer (CISO) (Rollenbeschreibung: 4.2) eingesetzt.

Informationssicherheit ist eine Verantwortung aller und verpflichtet Informationen zu schützen und den nötigen Mehraufwand für die Einhaltung der festgelegten Sicherheitsmaßnahmen zu Gunsten der Gesamtsicht in Kauf zu nehmen.

Führungskräfte haben in ihrem Bereich auf die Einhaltung des ISMS (zu finden in den WUPOLs, die Teil des ISMS sind: 4.4) hinzuwirken.

Dazu gelten neben der Anwendung dieser Richtlinie und den daraus abgeleiteten WUPOLs immer auch folgende Prinzipien:

Die Autorisierung zur Nutzung von Daten und Informationen orientiert sich an der auszuführenden Aufgabe. Das bedeutet, jeder Person sind nur jene Daten und Informationen zugänglich zu machen, die für die Erfüllung ihrer Aufgaben bzw. Ausübung ihrer Rolle notwendig sind (Prinzip des notwendigen Wissens).

und:

*Personen, Benutzer*innen, Systeme, Programme etc. verfügen über so wenig Zutritts- bzw. Zugriffsrechte wie möglich. Das bedeutet, dass Rechte zum Betreten, Lesen bzw. Anlegen, Schreiben, Ändern, Löschen, Ausführen oder zur Übertragung von Berechtigungen, gemessen an der durchzuführenden Aufgabe, im jeweils geringstmöglichen Ausmaß erteilt sind (Prinzip der Vermeidung überschießender Rechte).*

4.1. Angestrebtes Sicherheitsniveau

Die Anwendung von Informationssicherheit ist immer eine Abwägung zwischen Risiko und Kosten.

Beim angestrebten Sicherheitsniveau werden Risiken basierend auf den folgenden Angriffsgruppen bewertet und Informationssicherheitsmaßnahmen zum Schutz vor deren Bedrohungen implementiert:

- **Kriminelle Gruppen:** Organisierte Gruppen von Hackern, die aus wirtschaftlichem Interesse in Computersysteme eindringen. Diese Gruppen nutzen Phishing, Spam, Spyware und Malware für Erpressung, Diebstahl privater Informationen und Online-Betrug.
- **Hacker:** Einzelne Hacker haben es mit einer Vielzahl von Angriffstechniken auf Unternehmen abgesehen. Ihre Motive sind in der Regel persönlicher Gewinn, Rache, finanzieller Gewinn oder politische Aktivitäten. Hacker entwickeln oft neue Angriffsarten, um ihre kriminellen Fähigkeiten zu verbessern und ihr persönliches Ansehen in der Hacker-Community zu steigern.
- **Böswillige Insider:** Eine Person, die rechtmäßig Zugang zu Organisationsressourcen hat und diesen Zugang missbraucht, um Informationen zu stehlen oder Computersysteme zu beschädigen, um daraus wirtschaftlichen oder persönlichen Nutzen zu ziehen. Bei den Insidern kann es sich um Mitarbeitende, Auftragnehmerinnen, Zulieferer oder Partnerinnen der Zielorganisation handeln.

4.2. Rollen, Rechte und Pflichten in der Informationssicherheitsorganisation

In diesem Abschnitt wird der Aufbau der Sicherheitsorganisation festgelegt.

Die folgende Listung definiert die Informationssicherheitsverantwortlichkeiten innerhalb des Informationssicherheitsmanagementsystems (ISMS). Personen mit zugeordneten Verantwortlichkeiten dürfen Aufgaben an andere delegieren, jedoch bleiben sie weiterhin für die Aufgaben verantwortlich und müssen prüfen, ob alle Aufgaben ordnungsgemäß durchgeführt wurden.

Rektorat

Das Rektorat betrachtet Informationssicherheit als Angelegenheit von strategischer Bedeutung und beschließt die Strategie. Diese Strategie und die Umsetzung einzelner Maßnahmen oder eines Maßnahmenpakets schlägt die*der CISO dem Rektorat vor. Das Rektorat kann dann die*den ressortzuständig*en Vizerektor*in mit der Umsetzung des Maßnahmenpakets oder einzelner Maßnahmen beauftragen.

Chief Information Security Officer (CISO)

Die*Der CISO berät und erstellt Vorgaben in allen Belangen der Informationssicherheit und ist in dieser Funktion fachlich direkt der*dem ressortzuständigen Vizerektor*in unterstellt und an diese*n berichtspflichtig. Die Erstattung des Berichts sollte zumindest einmal im Monat an diese*n erfolgen. Zudem muss einmal pro Jahr an das Rektorat berichtet werden (siehe 4.3).

Der*Dem CISO kommt in ihrer*seiner Ausübung insbesondere ein Mitsprache- und Vetorecht gegenüber den umsetzenden Organisationseinheiten in Bezug auf die Informationssicherheit (bspw.: Speicherung von Daten, Übermittlung von Daten) zu. Die*der CISO macht Vorgaben, welches Schutzbedarfsniveau zu erreichen ist, aber nicht, wie das konkret umgesetzt wird. Das Rektorat kann Ausnahmen genehmigen (siehe Abschnitt 6).

Die Agenden der*des CISOs können durch weitere, zentral von ihr*ihm gesteuerte Funktionen unterstützt werden: Information Security Officer (ISO), Information Security Risk Manager (ISRM), Cyber Security Architects (CSA) oder Cyber Defence Center (CDC) Mitarbeitende.

Führungskräfte

Führungskräfte haben in allen Belangen der Informationssicherheit eine besondere Vorbildfunktion. Zudem ist jede Führungskraft verpflichtet in ihrem Verantwortungsbereich auf die Einhaltung des ISMS (zu finden in den WUPOLs, die Teil des ISMS sind: 4.4) hinzuwirken und zu kontrollieren.

Mitarbeitende

Alle Mitarbeitenden der WU sind zur Einhaltung des ISMS (zu finden in den WUPOLs, die Teil des ISMS sind: 4.4) verpflichtet.

Studierende

Alle Studierenden der WU, sind zur Einhaltung dieser Richtlinie verpflichtet.

4.2.1. Unabhängigkeit

Die Funktion der*des CISO ist fachlich und budgetär nur an Anweisungen des*der ressortzuständige*n Vizerektor*in gebunden.

Die*der CISO ist weder für die technische Implementierung von Sicherheitsmaßnahmen zuständig, noch trifft sie*er die Entscheidungen über den Einsatz von technischen Mitteln. Diese Aufgaben sind in der Verantwortung der jeweiligen Leitung der wissenschaftlichen Einrichtung für Lehre und/oder Forschung oder der jeweiligen Leitung der Dienstleistungseinrichtung (laut Organisationsplan der WU). Die*der CISO oder die*der CSA kann unterstützen, wenn dies angefordert wird.

Ebenso ist die*der CISO nicht für die Umsetzung der Informationssicherheitsrichtlinien in der jeweiligen Organisationseinheit zuständig. Diese Aufgaben liegen in der Verantwortung der jeweiligen Führungskräfte.

4.3. Senior Management Review

Das Rektorat betrachtet Informationssicherheit als Angelegenheit von strategischer Bedeutung und muss daher regelmäßig über die Effektivität und den Betrieb des ISMS informiert werden. Aus diesem Grund muss zumindest einmal pro Jahr ein „Senior Management Review"[2] geplant und durchgeführt werden. Dabei müssen folgende Punkte berichtet werden:

- Rückblick auf die definierten Maßnahmen aus dem letzten Review und deren Status
- Lagebild zur Informationssicherheit in- und außerhalb der Organisation
- Relevante Informationssicherheitsvorfälle und Folgemaßnahmen
- Ergebnisse aus den Audits laut Prüfplan (siehe 4.6)
- Ergebnisse der Informationssicherheitsrisikoanalysen
- Verbesserungsvorschläge und Maßnahmen

Sollte es erforderlich sein, kann das Rektorat auch ein häufigeres Intervall festlegen.

4.4. Regelungshierarchie

Die Hierarchie der Dokumente innerhalb des ISMS hält sich an die Vorgabe der WUPOL Regelungsmanagement Prozessbeschreibung (Referenz) im Abschnitt „Kategorisierung von Regelungen und Zuordnung zu Kategorien".

Alle zum ISMS gehörigen **WUPOLs** folgen dem Namensschema „WUPOL Informationssicherheitsvorgaben [Thema der WUPOL]".

[2] Der Begriff „Senior Management" ist definiert in der ISO/IEC 27002:2022. Im Fall der WU entspricht das Senior Management dem Rektorat.

4.5. Schnittstellen

4.5.1. Betrieb von IKT-Systemen

Die für den Betrieb vom jeweiligen IKT-System zuständige Organisationseinheit hat die Compliance zum ISMS zu gewährleisten. Entsprechende Regelungen sind in den WUPOL Informationssicherheitsvorgaben definiert.

4.5.2. IKT-Änderungsmanagement

Änderungen an IKT-Systemen, die einen Einfluss auf die Informationssicherheit haben, sind vor der Änderung zu evaluieren und zu dokumentieren. Dies umfasst die Erstellung eines Betriebshandbuches des Systems, eine Dokumentation der Schnittstellen mit Protokoll, Port und Richtung des Datenverkehrs und die Dokumentation der Verantwortlichkeiten in Bezug auf die Informationssicherheit.

4.5.3. Physische Sicherheit

Die Regelungen zur physischen Sicherheit werden durch die Hausordnung (siehe Link) der WU des Campus Managements geregelt.

4.6. Unabhängige Überprüfung der Informationssicherheit

Um sicherzustellen, dass die Anforderungen aus Richtlinien, Normen, Standards und anderen relevanten Vorgaben erfüllt sind, müssen Überprüfungen durchgeführt werden. Der*die CISO legt dem Rektorat zur Kenntnisnahme einen Jahresprüfplan vor, der sich an den Kapiteln der ISO27001 und einem risikobasierten Ansatz orientiert. Die Prüf-Tätigkeit der*des CISO umfasst neben den Prüfungen laut Jahresprüfplan auch ad hoc-Prüfungen (Audit), das die*der CISO veranlasst oder freiwillig von der (für den Betrieb des jeweiligen IKT-Systems) zuständigen Organisationseinheit in die Wege geleitet wird:

- Die Prüfung kann von einem internen Auditor oder einer externen Organisation durchgeführt werden, nicht jedoch von der (für das zu prüfende IKT-System) zuständigen Organisationseinheit
    - Der für die Prüfung erforderliche Zugriff auf Informationen ist mit der zuständigen Führungskraft zu vereinbaren.
    - Der Umfang und Zeitpunkt der Audittätigkeit ist festzulegen und zu kommunizieren.
- Die Ergebnisse der unabhängigen Überprüfung müssen aufgezeichnet werden und an die jeweilige Leitung der wissenschaftlichen Einrichtung für Lehre und/oder Forschung (laut Organisationsplan der WU) oder der jeweiligen Leitung der Dienstleistungseinrichtung sowie den*die CISO berichtet werden.
- Alle Audittätigkeiten sind von der beauftragenden Person zu überwachen und zu protokollieren.
- Abweichungen sind festzuhalten und gemeinsam mit der jeweiligen Leitung der wissenschaftlichen Einrichtung für Lehre und/oder Forschung (laut Organisationsplan der WU) oder der jeweiligen Leitung der Dienstleistungseinrichtung. Abweichungen sind im zentralen Vulnerability-Tracking zu erfassen. Bei Gefahr in Verzug ist unverzüglich das Rektorat zu informieren.

5. Aufhebung bisheriger Regelungen

- WUPOL Informationssicherheitspolitik vom 01.04.2019
- WUPOL Informationssicherheitsstrategie vom 01.04.2019
- WUPOL InfoSec Regelungshierarchie vom 01.04.2019

- WUPOL Privacy-by-Design vom 01.04.2019

6. Ausnahmen

Alle in dieser Richtlinie angeführten Anforderungen müssen für neue IKT-Systeme erfüllt werden. Für bestehende IKT-Systeme gilt eine Umsetzungsfrist von 6 Monaten ab Veröffentlichung der Richtlinie.

Sollten Anforderungen nicht erfüllt werden können, müssen von der (für den Betrieb des jeweiligen IKT-Systems) zuständigen Organisationseint entsprechende kompensierende Maßnahmen getroffen oder ein Umsetzungsplan erstellt sowie vom CISO freigegeben werden.

Sollte dies nicht zu einer Einigung führen, kann das Rektorat die Ausnahme genehmigen.

7. Qualitätssicherung

Das vorliegende Dokument wird jährlich einer Evaluierung hinsichtlich Aktualität unterzogen.

8. Dokumentinformationen

Kurztitel	RL Informationssicherheit
Langtitel	Richtlinie für das WU Informationssicherheitsmanagement
Dateiname	RLInformationssicherheit.docx
Ersetzt	WUPOL Informationssicherheitspolitik vom 01.04.2019, WU-POL Informationssicherheitsstrategie vom 01.04.2019, WU-POL InfoSec Regelungshierarchie vom 01.04.2019, WUPOL Privacy-by-Design vom 01.04.2019
Titel englische Version	
Version (Nummer, Datum)	2023-1.0 vom 04.07.2023
Inhaltsverantwortlich	Matthias Harrer / CISO
Autor/in	Matthias Harrer / CISO
Ansprechperson für inhaltliche Fragen und praktische Umsetzung	Matthias Harrer / CISO

Kommunikation (Mehrfachauswahl möglich)	☐ E-Mail ☒ Mitteilungsblatt ☒ Regelungsdatenbank
Veröffentlicht im Mitteilungsblatt	Studienjahr 2022/2023; 42. Stück; fortlaufende Nummer: 256; vom 12.07.2023; Link zum Mitteilungsblatt

Gültig ab	12.07.2023
Gültig bis	30.06.2028
Genehmigt von	Rektorat; am 11.07.2023
Weitere Informationen	Informationssicherheit, ISMS, Datenschutz