

WUPOL Informationssicherheitspolitik

Version 2019-1.0 | Klassifikation: Öffentlich

Inhalt

1.	Zielsetzung.....	2
2.	Geltungsbereich	2
3.	Angestrebte Ziele	2
4.	Umsetzung	3
5.	Pflichten des/der Einzelnen.....	3
6.	Folgen der Nichteinhaltung	3
7.	Qualitätssicherung.....	3
8.	Aufhebung bisheriger Regelungen	3
9.	Dokumentinformationen.....	5

1. Zielsetzung

Die Abhängigkeit von Information und Informationssystemen, deren zunehmende Vernetzung und die damit verbundenen internen und externen Risiken machen es notwendig, Anforderungen an die Informationssicherheit zu regeln.

Die Informationssicherheitspolitik der Wirtschaftsuniversität Wien (WU) drückt die Ziele und die Verantwortungshaltung des Rektorats aus und schafft damit den Rahmen für nachhaltiges Informationssicherheitsmanagement.

Neben den gesetzlichen Verpflichtungen sind es die Ansprüche und Erwartungen der WU, ihrer Angehörigen, Geschäfts- und Kooperationspartner/innen, sowie der Öffentlichkeit, die Informationssicherheit zu einem zentralen Thema machen.

Informationssicherheit ist daher nicht Selbstzweck, sondern ein wesentlicher Aspekt unserer Arbeitsweise.

Von dieser Sicherheitspolitik umfasst sind Informationen in allen Erscheinungsformen, sei es in elektronischer, schriftlicher, mündlicher oder anderer Form.

Nicht umfasst von dieser Informationssicherheitspolitik sind die Funktionen Objektschutz, Brandschutz, Arbeitsplatzsicherheit, Arbeitsmedizin und sonstige, nicht in erster Linie informationsbezogene Themenkreise.

Informationssicherheit dient dem Schutz von Daten und Informationen vor unberechtigtem Zugriff, unbefugter Kenntnisnahme und Preisgabe, vor Verlust, Zerstörung und vor Veränderung, und ermöglicht die Nachvollziehbarkeit von Daten- und Informationsflüssen. Sie stellt somit die Vertraulichkeit, Verfügbarkeit und Integrität unserer und der uns anvertrauten Daten- und Informationsbestände sicher.

2. Geltungsbereich

Die Informationssicherheitspolitik gilt verpflichtend für alle Angehörigen der WU im Sinne des Universitätsgesetzes sowie für Personen, die in WU-nahen Organisationen¹ tätig sind.

Dritte sind in den jeweils relevanten Punkten zu verpflichten.²

Darüber hinaus gilt diese Sicherheitspolitik ohne zeitliche und örtliche Einschränkungen.

3. Angestrebte Ziele

Allgemeine Sicherheitsziele der WU sind:

- Schutz vor Verlust und Zerstörung von Information (Verfügbarkeit)
- Schutz vor unberechtigtem Zugriff, unbefugter Kenntnisnahme und Preisgabe von Information (Vertraulichkeit)
- Schutz vor ungewollter und manipulativer Veränderung von Information (Integrität)
- Schutz vor Verlust der Nachvollziehbarkeit bzw. Nichtabstreitbarkeit von Informationsflüssen

¹ Z.B. WU ZBP Career Center.

² Z.B. mittels Vertraulichkeitsvereinbarungen, Zustimmungserklärungen oder Ähnlichem.

Neben diesen allgemeinen Sicherheitszielen sollen Informationssicherheitsmaßnahmen die folgenden, für uns gleichwertigen Ziele wirksam unterstützen:

- Sicherstellung der Kontinuität des Betriebs
- Schutz aller personenbezogenen und geschäftsbezogenen Daten und Informationen
- Schadensvermeidung und Schadensbegrenzung durch vorbeugende Sicherheitsmaßnahmen
- Entwicklung und Förderung eines umfassenden Sicherheitsbewusstseins und einer Sicherheitskultur
- Einhaltung gesetzlicher Vorgaben und vertraglicher Vereinbarungen
- Gewährleistung eines den Risiken angemessenen Sicherheitsniveaus
- Unterstützung und Förderung der mit sicherheitsrelevanten Aufgaben betrauten Personen
- Positionierung der WU als vertrauensvolle, zuverlässige Partnerin

4. Umsetzung

Die Umsetzung dieser Informationssicherheitspolitik baut auf der Informationssicherheitsstrategie und der darin beschriebenen Informationssicherheitsorganisation der WU auf.

Details dazu finden sich im Dokument „Informationssicherheitsstrategie der WU“.

5. Pflichten des/der Einzelnen

Aus Sicht des Rektorats ist Informationssicherheit ein zentrales Thema. Die Ziele und die abgeleiteten Sicherheitsmaßnahmen werden von ihr daher in jeder Hinsicht getragen und unterstützt.

Aufgrund der großen Bedeutung der Informationssicherheit sind aber auch alle Universitätsangehörigen sowie alle anderen Personen, die mit Daten und Informationen der WU in Berührung kommen, verpflichtet, die entsprechenden Sicherheitsbestimmungen zu beachten und einzuhalten.

Eine besondere Bedeutung kommt dabei der Vorbildfunktion von Führungskräften zu.

6. Folgen der Nichteinhaltung

Die Einhaltung von Regelungen und Sicherheitsmaßnahmen wird regelmäßig, aber auch anlassbezogen überprüft.

Eine Missachtung von Sicherheitsbestimmungen kann neben entsprechenden disziplinären und dienstrechtlichen auch zivil- und strafrechtliche Folgen nach sich ziehen.

7. Qualitätssicherung

Das vorliegende Dokument wird einer jährlichen Evaluierung hinsichtlich Aktualität unterzogen.

8. Aufhebung bisheriger Regelungen

Mit Kundmachung dieses Dokuments wird die „Informationssicherheitspolitik der WU 2015-1.0“ außer Kraft gesetzt und durch das vorliegende Dokument ersetzt.

Wien, am 26.03.2019

Univ.Prof. Mag.Dr. Stefan Pichler
Vizekanzler für Forschung

9. Dokumentinformationen

Pflichtfelder sind mit einem „*“ gekennzeichnet.

Kurztitel^{3*}	WUPOL Informationssicherheitspolitik
Langtitel	Version 2019-1.0 Klassifikation: Öffentlich
Dateiname^{4*}	WUPOL_InfoSec-Politik_2019-1.0.docx
Ersetzt	Informationssicherheitspolitik der WU 2015-1.0 vom [Datum]
Titel englische Version	WUPOL Information Security Policy , [Link]
Version (Nummer, Datum)*	2019-1.0, vom [Versionsdatum]
Inhaltsverantwortlich*	IT-SERVICES / Miksch, Georg [Org.Einheit] / [Nachname, Vorname]
Autor/in*	Riesenfelder, Christoph / [Nachname, Vorname], [Org.Einheit] /
Ansprechperson für inhaltliche Fragen und praktische Umsetzung	IT-SERVICES / Miksch, Georg [Org.Einheit] / [Nachname, Vorname]

Kommunikation* (Mehrfachauswahl möglich)	<input type="checkbox"/> E-Mail <input checked="" type="checkbox"/> Mitteilungsblatt <input checked="" type="checkbox"/> Regelungsdatenbank
Veröffentlicht im Mitteilungsblatt	Studienjahr XXXX/XXXX, XXX. Stück, [Mitteilungsblatt-Nr.] vom [Datum], [Link]
Erstveröffentlichung (optional)	Studienjahr XXXX/XXXX, XXX. Stück, [Nr.] vom [Erstveröffentlichungs-Datum], [Link]

Gültig ab*	01.04.2019
Gültig bis*	31.12.2999
Genehmigt von	Vizekanzler für Forschung, Univ.Prof. Mag.Dr. Stefan Pichler am [Genehmigungsdatum]
Weitere Informationen*	InfoSec, IT-Sicherheit, Datensicherheit, Datenschutz

³ Beispiele für Kurztitel/Langtitel:

- Kurztitel = Kategorie und Schlagwort z.B. WUPOL Software
- Langtitel oder Subtitel = Bezeichnung aus der Abteilung, z.B. Regelung über die Verwendung von WU Software

⁴ Dateinamen max. 60 Zeichen; keine Umlaute, Sonderzeichen oder Leerzeichen verwenden