WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

WUPOL IT-Endgeräte

Version 2019-1.0 | Klassifikation: Öffentlich

Inhalt

1. Zielsetzung

Zur Erreichung der Geschäftsziele und zur Erfüllung der Aufgaben der Wirtschaftsuniversität Wien (WU) ist Information, und damit verbunden der Einsatz von Informationstechnologien (IT), unerlässlich.

Dazu muss auch durch geeignete organisatorische und technische Maßnahmen die wirtschaftliche, sichere und gesetzeskonforme Verwendung der IT gewährleistet werden. Die verwendeten Informations- und Kommunikationssysteme, die darauf laufenden Anwendungen und die verarbeiteten Daten sind somit entsprechend zu schützen.

Dabei kommt die Eigenverantwortung der Benutzer/innen in besonderem Maße zum Tragen.

Zweck dieser Regelung ist es, geeignete Regelungen für den Einsatz von IT, insbesondere Passwörtern, zu treffen, sodass die Erreichung der oben genannten Ziele der WU sichergestellt wird.

Ein weiteres Ziel dieser Regelung ist es, sicherzustellen, dass Informationen auf Datenträgern (inkl. Papier und Mikrofilm) geschützt bleiben, wenn diese dauerhaft weitergegeben werden oder das endgültige Ende ihrer Nutzungsdauer erreichen.

Die Regelungen in diesem Dokument verstehen sich als Maßnahme zur Schaffung eines verlässlichen Rahmens.

Nicht in diesem Dokument enthalten sind Begründungen zu den einzelnen Regelungen. Die Regelungen werden im Rahmen von Schulungen und Sensibilisierungsaktivitäten kommuniziert und dabei so aufbereitet, dass ihre Hintergründe verständlich und nachvollziehbar sind.

2. Geltungsbereich

Diese Regelung gilt verpflichtend

- für alle Mitarbeiter/innen im Dienstleistungsbereich, in Einrichtungen für Lehre und/oder Forschung, sofern sie im Eigentum der WU befindliche IT-Endgeräte nutzen oder an das Netzwerk der WU anschließen bzw. sich damit verbinden[1], bzw.
- sofern diese Mitarbeiter/innen IT-Endgeräte, die nicht im Eigentum der WU stehen[2], an das Netzwerk der WU anschließen bzw. sich damit verbinden,
- für Personen, die in WU-nahen Organisationen tätig sind und IT-Endgeräte an das Netzwerk der WU anschließen bzw. sich damit verbinden oder im Eigentum der WU befindliche IT-Endgeräte nutzen[3],
- für alle Studierenden der WU, die IT-Endgeräte an das Netzwerk der WU anschließen bzw. sich damit verbinden oder im Eigentum der WU befindliche IT-Endgeräte[4] nutzen, sowie
- für Dritte, die IT-Endgeräte an das Netzwerk der WU anschließen bzw. sich damit verbinden, insbesondere jene, die berechtigt wurden, auf von IT-SERVICES betriebene Systeme, Anwendungen und das Netzwerk zuzugreifen. Diese sind in den jeweils relevanten Punkten zu verpflichten.[5]

Darüber hinaus gilt diese Regelung ohne zeitliche und örtliche Einschränkungen.

---

1 Z.B. Mitarbeiter/innen der Service-Einrichtungen, Mitarbeiter der Departments, Forschungsinstitute, Kompetenzzentren und WU-Executive Academy.

2 Z.B. aus Sponsorgeldern finanzierte Geräte, Privatgeräte.

3 Z.B. assoziierte Vereine, ÖH, WU ZBP Career Center.

4 Z.B. Surfstation-, Schulungs- und Studierendenarbeitplatzgeräte, Geräte im Sprachlernzentrum und in der Bibliothek sowie sonstige öffentlich zugängliche IT-Endgeräte im Eigentum der WU.

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

3. Definitionen

Im Kontext dieses Dokuments werden Begriffe wie folgt definiert:

Informations- und Kommunikationssystem

Server, Netzwerkkomponenten (Router, Switches etc.), Standgeräte (Desktops), tragbare Geräte (Notebooks, Tablets etc.), netzwerkfähige Kleingeräte (Smartphones, Mobiltelefone, Navigationsgeräte, Datenerfassungsgeräte etc.), sowie Multifunktionsgeräte (Kombifaxe, Druck(Fax)stationen etc.).

IT-Endgerät

Standgeräte (Desktops), tragbare Geräte (Notebooks, Tablet PCs, Tablets etc.), netzwerkfähige Kleingeräte (Smartphones, Mobiltelefone, Navigationsgeräte, Datenerfassungsgeräte, VoIP-Telefone etc.), Endgeräte bei Gerätesteuerungen sowie Multifunktionsgeräte (Kombifaxe, Druck(Fax)stationen etc.); außerdem Arbeitsplatzdrucker, Scanner und ähnliche Geräte, die keine Benutzerdaten oder sonstige schutzbedürftige Daten halten (so genannte IT-Peripheriegeräte).

Mobiler Datenträger

Speichersticks (USB-Sticks), Speicherkarten aller Art (auch in Multimedia-Abspielgeräten, in Kameras etc.), mobile Festplatten (z.B. magnetisch und flashspeicher-basiert), CDs, DVDs, Disketten, Magnetbänder und ähnliche Speichermedien.

Datentrennung

Trennung der Daten eines Benutzers/einer Benutzerin von Daten anderer Benutzer/innen.

Anwendung

Programme jeglicher Art, inklusive Betriebssystemen, Datenbanken, Hardware-Schutzmechanismen (z.B. für Festplatten), Zutrittskontrollsystemen und Ähnlichem.

Account

Eine Kombination aus einer Benutzer-ID und einem Passwort. Diese beiden Elemente bilden die sogenannten Zugangsdaten. Ein Account stellt eine Zugriffsberechtigung zu einem IT-System dar.

Die Begriffe Konto, Benutzerkonto, Zugriffsberechtigung oder User Credentials werden als Synonyme für Account verwendet.

Benutzer/in (Account) mit erweiterten Rechten

Jene Benutzer/innen (Accounts), die umfassendere Rechte als Standardbenutzer/innen besitzen. In der Regel gehören Administrator/inn/en zu dieser Benutzer/innen/gruppe.

Benutzer-ID

Eine Zeichenfolge aus Buchstaben, Ziffern und/oder Sonderzeichen, die eine eindeutige Zuordnung zu einem Berechtigungsprofil darstellt und somit personenbezogen ist.

Die Begriffe Username, Benutzername oder User-ID werden als Synonyme für Benutzer-ID verwendet.

Passwort

Eine Zeichenfolge aus Buchstaben, Ziffern und/oder Sonderzeichen bezeichnet, die die Überprüfung einer Identität möglich macht.

Die Begriffe Kennwort, Schlüsselwort oder Password werden als Synonyme für Passwort verwendet.

Funktionsbenutzer-ID

Eine Funktionsbenutzer-ID, darf im Gegensatz zu personenbezogenen Benutzer-IDs von mehreren Personen verwendet werden. Im Kontext von SAP verfügen diese über keinen GUI-Zugriff und sind auf bestimmte IP-Adressen eingeschränkt.

Initial-Passwort

Ein Passwort, das einmalig (erstmalig) für einen Account gesetzt wird.

Eigentümer/in (Owner)

Eigentümer/innen, im Folgenden als „Owner" bezeichnet, sind im Kontext dieses Dokuments Personen, die im Rahmen ihrer Funktion autorisiert sind, Datenträger bzw. Geräte, in denen elektronische Speichermedien verbaut sind, zu verwenden. Dies können jedoch z.B. auch die Leitung von Organisationseinheiten sein, die stellvertretend für ihre Organisationseinheit als Owner verstanden werden (z.B. bei Sicherungsbändern aus dem Bandroboter oder Network Attached Storage). Owner besitzen die legitimierte Verfügungsberechtigung über die Datenträger bzw. Geräte und legen den Schutzbedarf der darauf befindlichen Daten fest.

Nutzer/in

Nutzer/innen sind Personen, die vom Owner eines Datenträgers bzw. Geräts, in dem elektronische Speichermedien verbaut sind, zu dessen Nutzung berechtigt wurden und die tatsächliche Verfügungsgewalt darüber innehaben. Nutzer/in kann allerdings auch der Owner selbst sein. Ist der Owner nicht eindeutig feststellbar, ist damit der/die Besitzer/in des Datenträgers bzw. Geräts gemeint.

Abgabe

Unter Abgabe wird die Aufgabe der tatsächlichen Verfügungsgewalt, d.h. der Kontrolle über den Datenträger bzw. das Gerät verstanden. Beispiele sind die dauerhafte Weitergabe eines USB-Sticks; die Übergabe eines defekten Speichermediums an den Hersteller; die Rückgabe eines Notebooks/PCs zur Vernichtung und Entsorgung; der Tausch eines Smartphones gegen ein neues; das Wegwerfen von Papier etc. Nicht gemeint ist die kurzfristige Überlassung des Datenträgers bzw. Geräts an eine vertrauenswürdige Person.

4. Regelungen für alle im Geltungsbereich genannte Personen ausgenommen Studierende

4.1. Allgemeine Regelungen

Die untenstehenden Regelungen gelten für alle im Geltungsbereich genannten Personen **außer für Studierende**:

(1) IT-Endgeräte, auf denen Daten der WU verarbeitet werden, müssen über einen Zugriffsschutz in Form eines PIN oder Passworts oder über eine biometrische Maßnahme abgesichert sein. Sofern diese Maßnahme nicht durch die WU technisch erzwungen wird oder werden kann, sind die Passwortregelungen der WU benutzer/innen/seitig sinngemäß umzusetzen.

(2) Der passwortgeschützte Sperrbildschirm bzw. die Gerätesperre auf IT-Endgeräten der WU, auf denen Daten der WU verarbeitet werden, ist so einzustellen, dass er spätestens nach 15 Minuten Inaktivität aktiviert wird und ist bei Verlassen des Arbeitsplatzes manuell zu aktivieren.

(3) Das Deaktivieren der voreingestellten PIN-geschützten Gerätesperre bzw. des passwortgeschützten Sperrbildschirms auf IT-Endgeräten ist untersagt.

(4) Im Falle eines Verlustes oder Diebstahls eines IT-Endgeräts oder eines mobilen Datenträgers, auf dem sich Daten der WU befinden, ist vom betroffenen Mitarbeiter/von der betroffenen Mitarbeiterin der Prozess zur Meldung von Datenschutzvorfällen einzuhalten und umgehend eine polizeiliche Anzeigebestätigung bei IT-SERVICES abzugeben.

(5) Im Eigentum der WU stehende IT-Endgeräte sind grundsätzlich in der von IT-SERVICES ausgelieferten Standardkonfiguration zu betreiben.

(6) Die Nutzung von IT-Endgeräten, deren vordefinierte Berechtigungseinstellungen oder deren Betriebssystem in einer Form verändert wurden, die die standardmäßige Wartung und Administration durch IT-SERVICES verhindert, ist nur für wissenschaftliche Mitarbeiter/innen zulässig, wenn die Leitung der Organisationseinheit dieser Nutzungsform zustimmt. Die Nutzung erfolgt auf eigenes Risiko der Leitung der Organisationeinheit, in der dieses Gerät betrieben wird. Der Anspruch auf Unterstützung durch IT-SERVICES entfällt in diesen Fällen.

(7) IT-Endgeräte, die nicht von IT-SERVICES gewartet und administriert werden, insbesondere auch Dual-Boot-Geräte, werden auf eigenes Risiko des Benutzers/der Benutzerin betrieben. Der Anspruch auf Unterstützung durch IT-SERVICES entfällt in diesen Fällen.

(8) Ein aktueller und aktivierter Echtzeit-Schadsoftwarescanner muss installiert sein, sofern ein solcher vom Betriebssystem unterstützt wird.

(9) Aktuelle Schadsoftwaresignaturen müssen unmittelbar nach dem Verbindungsaufbau vorhanden sein.

(10) Eine aktuelle lokale Firewall, die ein- und ausgehenden Datenverkehr überwacht, muss installiert und aktiviert sein, sofern eine solche standardmäßig im Betriebssystem integriert ist.

(11) Das Betriebssystem und die installierten Anwendungen sind in Bezug auf Sicherheitsupdates aktuell zu halten.

(12) Datenträger, die in IT-Endgeräten verbaut sind, die im Eigentum der WU stehen, sind zu verschlüsseln.

(13) Mobile Datenträger, auf denen sich als intern oder vertraulich klassifizierte Daten der WU befinden, sind zu verschlüsseln.

(14) Die Arbeit mit Administrator- oder Root-Rechten auf IT-Endgeräten mit Rechtetrennung ist, außer zu dienstlich notwendigen Wartungszwecken, untersagt.

(15) Auf IT-Endgeräten, die auch von anderen als dem/der berechtigten Benutzer/in verwendet werden, insbesondere Geräte, die nicht im Eigentum der WU stehen, müssen zur Datentrennung geeignete Maßnahmen ergriffen werden, andernfalls das IT-Endgerät nur durch den/die berechtigte/n Benutzer/in verwendet werden darf.

(16) Die Speicherung privater Daten auf im Eigentum der WU stehenden IT-Endgeräten und mobilen Datenträgern ist in beschränktem Umfang zulässig, auf Desktops, Notebooks und Tablet-PCs jedoch nur in einem als "privat" benannten Verzeichnis.

(17) Private Daten auf im Eigentum der WU stehenden IT-Endgeräten und mobilen Datenträgern sind auf Aufforderung durch IT-SERVICES von der Person, die diese Daten dort gespeichert hat, zu löschen.

(18) Im Eigentum der WU stehende Notebooks sind, wenn möglich, an unsicheren Orten mit einem Kabelschloss an einem festen Gegenstand anzuschließen, wenn diese nicht anders physisch gegen Wegnahme gesichert werden können (Diebstahlschutz). Kabelschlösser können über IT-SERVICES bezogen werden.

(19) Für die Sicherung von Daten auf IT-Endgeräten ist der jeweilige Benutzer/die jeweilige Benutzerin verantwortlich.

(20) Das Verschleiern der eigenen, insbesondere der dienstlichen Identität im Rahmen der Internet-Nutzung ist untersagt.

(21) Das Verändern von erkennbar sicherheitsrelevanten Einstellungen ist untersagt.

(22) Die Installation sicherheitsgefährdender Programme ist untersagt.

(23) Der Einsatz von Soft- und Hardware und sonstigen Mitteln, deren Zweck es ist, Informationen auszuspähen, ist untersagt.

(24) Die bewusste Inkaufnahme IT-bezogener Sicherheitsrisiken ist untersagt. Im Zweifelfall ist eine Abstimmung mit IT-SERVICES zu suchen.

(25) Urheberrechte sind zu wahren und Lizenzbestimmungen sind einzuhalten.

(26) Bei Beendigung des Dienstverhältnisses sind im Eigentum der WU stehende IT-Arbeitsmittel an den jeweiligen Vorgesetzten/die jeweilige Vorgesetzte oder an IT-SERVICES zu retournieren.

(27) Bei Beendigung eines Vertragsverhältnisses sind im Eigentum der WU stehende IT-Arbeitsmittel an die jeweilige Ansprechperson der WU zu retournieren.

4.2. Gebrauch von Passwörtern

(28) Passwörter sind vom berechtigten Benutzer/der berechtigten Benutzerin geheim zu halten und dürfen nicht weitergegeben werden.[6] Auf eine unbeobachtete Eingabe des Passworts ist zu achten.

(29) Passwörter dürfen nicht ungesichert über das Netzwerk übertragen werden.

(30) Passwörter müssen so gewählt werden, dass sie sich signifikant von anderen eigenen Passwörtern unterscheiden.[7]

(31) Passwörter, von denen angenommen werden muss, dass sie Unberechtigten bekannt geworden sein könnten oder sind, müssen vom berechtigten Benutzer/der berechtigten

[6] Auch nicht z.B. an Dienstvorgesetzte, Vertretungen oder Assistent/inn/en.

[7] Insbesondere müssen sich WLAN-Passwort und WU-Passwort deutlich unterscheiden.

Benutzerin geändert werden bzw. muss von diesem/dieser eine Passwortrücksetzung veranlasst werden.

(32) Die Weitergabe von Passwörtern von Funktionsbenutzer-IDs darf nur durch die für die jeweilige Funktionsbenutzer-ID verantwortliche Person erfolgen und nur an Personen, die das Passwort für die Erfüllung ihrer Aufgaben an der WU benötigen.

(33) Passwörter müssen vom berechtigten Benutzer/der berechtigten Benutzerin jederzeit geändert werden können. Dies ist durch den Betreiber des Berechtigungssystems sicherzustellen.

(34) Passwörter für Funktionsuser-IDs dürfen nur von der für die jeweilige ID verantwortlichen Person geändert werden. Bei Ausscheiden einer Person aus der von der ID umfassten Gruppe ist das Passwort umgehend zu ändern, ausgenommen bei SAP.

(35) Initial-Passwörter sind bei der ersten Anmeldung entsprechend den Minimalanforderungen zu ändern.

(36) Meldet sich ein Benutzer/eine Benutzerin über ein externes, nicht von der WU betriebenes System an einem System der WU an, so muss er/sie sich unmittelbar nach Benützung wieder abmelden.

(37) Zusätzliche Regelungen können, abhängig von der jeweiligen Situation, dann getroffen werden, wenn dies aus Risikogesichtspunkten notwendig erscheint.

4.3. Nutzung erweiterter Rechte

(38) Passwörter von Benutzer/inne/n mit erweiterten Rechten müssen gesichert hinterlegt werden, sodass im Ausnahmefall die Weiternutzung des Accounts durch die WU sichergestellt ist.

4.4. Vergabe von Initial-Passwörtern

(39) Nur betreffend SAP: Initial-Passwörter werden von dem/der SAP-Benutzerverantwortlichen gemeinsam mit dem/der Benutzer/in beim Erst-Login zur einmaligen Verwendung festgelegt.

(40) Die Struktur von Initial-Passwörtern muss zumindest den Minimalanforderungen entsprechen.

(41) Alle, außer SAP, betreffend: Initial-Passwörter müssen nach dem Zufallsprinzip individuell vergeben werden und müssen eine begrenzte Gültigkeitsdauer haben.

(42) Werkseitig voreingestellte Passwörter sind umgehend entsprechend den Minimalanforderungen zu ändern.

4.5. Struktur von Passwörtern

Die untenstehenden, verbindlichen Regelungen werden durch entsprechende Empfehlungen (Leitlinien) außerhalb dieses Dokuments ergänzt, um die Umsetzung der Vorgaben zu erleichtern, z.B. mittels Tipps zur Findung sicherer Passwörter.

Passwörter müssen zumindest den folgenden Anforderungen (im Folgenden „Minimalanforderungen" genannt) entsprechen:

Merkmal	**Standardbenutzer/in**	**Benutzer/in mit erweiterten Rechten**
Minimale Passwortlänge	SAP: 8 Zeichen Mitarbeiter/innen von IT-SERVICES: 12 Zeichen Sonst: 10 Zeichen	SAP: 8 Zeichen Sonst: 16 Zeichen
Unzulässige Phrasen	SAP: Keine Einschränkungen Sonst: Die Benutzer-ID darf nicht Teil des Passworts sein	SAP: Keine Einschränkungen Sonst: Die Benutzer-ID darf nicht Teil des Passworts sein
Komplexitätserfordernisse: Siehe unten unter a) und b)	SAP: Keine Sonst: Ja	SAP: Keine Sonst: Ja
Gerätesperre / Bildschirmsperre	Nach 15 Minuten Inaktivität	Nach 15 Minuten Inaktivität
Passwortwiederverwendung	Die letzten zwei (SAP: drei) Passwörter dürfen nicht nochmals verwendet werden	Die letzten zwei (SAP: drei) Passwörter dürfen nicht nochmals verwendet werden
Maximales Passwortalter	SAP: 180 Tage Sonst: Keine Anforderung	SAP: 180 Sonst: Keine Anforderung
Minimales Passwortalter	SAP: 1 Tag Sonst: Keine Anforderung	SAP: 1 Tag Sonst: Keine Anforderung
Erlaubte Versuche bis Kontosperre	SAP: 3 Versuche Sonst: Keine Anforderung	SAP: 3 Versuche Sonst: Keine Anforderung
Wartezeit bis zu einem neuen Versuch	Keine Anforderung	Keine Anforderung
Rücksetzung des Zählers für die Kontosperre	Keine Anforderung	Keine Anforderung

a) Vergebene **Passwörter, außer für SAP,** müssen alle der folgenden Merkmale aufweisen:

- Mindestens ein Großbuchstabe (A to Z)
- Mindestens ein Kleinbuchstabe (a to z)
- Mindestens eine Ziffer (0 bis 9)
- Mindestens ein Sonderzeichen

b) Vergebene **PINs** müssen alle der folgenden Eigenschaften aufweisen:

- Nur Ziffern (0 bis 9)
- Minimale Länge: Vier Zeichen

Auf im Eigentum der WU stehenden IT-Endgeräten kann die Einhaltung der Sicherheitsmaßnahmen von der WU jederzeit auditiert werden.

4.6. Löschung von Daten und Vernichtung von Datenträgern

Für die sichere Löschung bzw. sichere Entsorgung von Daten(trägern) ist der Owner bzw. der/die berechtigte Nutzer/in des Datenträgers bzw. Geräts verantwortlich.[8]

Für den Fall, dass Geräte und damit fix verbaute elektronische Datenträger zwar nicht im Eigentum der WU stehen, jedoch schützenswerte Daten enthalten (z.B. im Fall von Geräteleasing bei intelligenten Druckstationen) ist der Owner des jeweiligen Geräts vertraglich zu verpflichten, diesen elektronischen Datenträger im Sinne der Regelungen der WU zu löschen bzw. physisch zu zerstören und zu entsorgen. Dies betrifft insbesondere Lieferanten von Testgeräten oder von geleasten oder gemieteten Multifunktionsgeräten (Druckern).

Erreichen elektronische Datenträger das Ende ihrer Nutzungsdauer oder sollen elektronische Datenträger weitergegeben oder entsorgt werden, müssen die darauf enthaltenen Daten, sofern technisch möglich, vor der Ab- oder Weitergabe des Speichermediums gelöscht werden:

Entsorgung von Datenträgern mit Inhalten, die nicht-öffentlich sind		
Datenträgerart		**Vorgehen**
Festplatten aus Notebooks, Desktops und Servern sowie externe Festplatten und NAS-Platten	Magnetische Festplatten	Sicheres Löschen, danach Abgeben des Geräts bzw. der Platte bei IT-SERVICES
	SSD (Flash)-Festplatten und Hybrid-Festplatten (= flash & magnetisch)	Initialisieren mittels Herstellerprogramm, danach Abgeben des Geräts bzw. der Platte bei IT-SERVICES
Kleingeräte mit eingebauten Speichermedien	Smartphones, Tablets, Mobiltelefone	Rücksetzen auf Werkseinstellungen, danach Abgeben bei IT-SERVICES zwecks Entsorgung über einen Entsorgungsbetrieb
	PDAs, Kameras, Multimedia Player etc.	Rücksetzen auf Werkseinstellungen, danach Abgeben bei IT-SERVICES
Klein-Speichermedien, ausgenommen CDs und DVDs	USB-Sticks, Speicherkarten (SD, MMC etc.), andere Klein-Flash-Speichermedien	Sicheres Löschen, danach Abgeben bei IT-SERVICES
	Disketten, ZIP-Cartridges	Lochen oder Abgeben bei IT-SERVICES
CDs, DVDs und andere optische Speichermedien		Zerkratzen, Lochen oder Abgeben bei IT-SERVICES
Sicherungsbänder aus Bandstationen und Bandrobotern		Abgeben bei IT-SERVICES
Papier inkl. Fotopapier sowie Mikrofilm		Shredden oder manuelles Zerschneiden
Sonstige Datenträger, unabhängig davon, ob elektronischer oder physischer Natur und in welchen Geräten eingebaut		Bei elektronischen Datenträgern sicheres Löschen bzw. Rücksetzen/Initialisieren des Geräts und Zerstören; bei nicht-elektronischen Datenträgern Zerstören

[8] IT-SERVICES bietet an, Datenträger auf Wunsch zu vernichten und zu entsorgen. Dazu ist es möglich, z.B. über ein Helpdesk-Ticket eine Abholung zu veranlassen.

In Zweifelsfällen müssen Datenträger physisch zerstört (d.h. vernichtet) werden.

Die physische Zerstörung elektronischer Datenträger ist von einer dazu beauftragten und dafür zuständigen Person im Bereich IT-SERVICES binnen sechs Monaten ab Übernahme durchzuführen. Erfolgt die physische Zerstörung nicht direkt an der WU, muss diese über einen qualifizierten Entsorgungsbetrieb durchgeführt werden.

Wenn die Entsorgung eines elektronischen Datenträgers über IT-SERVICES durch einen qualifizierten Entsorgungsbetrieb stattfinden muss gilt: Zuständig dafür ist der Bereich IT-SERVICES, wobei die physische Zerstörung von IT-SERVICES binnen sechs Monaten ab Übernahme veranlasst und vom Entsorgungsbetrieb überwacht und protokolliert werden muss.

5. Regelungen für Studierende

Die untenstehenden Regelungen gelten für Studierende:

(1) Schadsoftwaresignaturen sind aktuell zu halten und bei Aufbau einer Netzwerkverbindung zur WU vor deren weiterer Nutzung zu aktualisieren.

(2) Urheberrechte sind zu wahren und Lizenzbestimmungen sind einzuhalten.

(3) Bei Beendigung eines Vertragsverhältnisses sind im Eigentum der WU stehende IT-Endgeräte an die jeweilige Ansprechperson der WU zu retournieren.

Ausdrücklich untersagt ist Folgendes:

(4) Das Neustarten (Booten) von öffentlich zugänglichen IT-Endgeräten über externe Datenträger.

(5) Der Einsatz von Soft- und Hardware und sonstigen Mitteln, deren Zweck es ist, Informationen auszuspähen.

6. Meldung von Sicherheitsvorfällen und -mängeln

Alle Personen, die vom Geltungsbereich dieser Regelung umfasst sind, haben ihnen bekannt gewordene sicherheitsrelevante Vorfälle und Sicherheitsmängel umgehend an it-security@wu.ac.at zu melden.

7. Regelungswidriges Vorgehen

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

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

8. Ausnahmen

Es ist generell zunächst eine Vorgehensweise zu wählen, die den geltenden Regelungen entspricht. Erst wenn dies technisch oder organisatorisch nicht möglich oder wirtschaftlich nicht zu vertreten ist, kann über eine Ausnahmeregelung entschieden werden.

Ausnahmen müssen

- zeitlich begrenzt,
- auf Zweck und Benutzer/innen/kreis eingeschränkt,
- hinsichtlich Antrag, Genehmigung/Ablehnung, Änderungen und Auslaufen dokumentiert,
- kontrolliert und im Falle des Auslaufens ohne Neuantrag nach entsprechender Frist aufgehoben und
- im Falle der Nichtbeachtung einschlägiger Regelungen der WU umgehend aufgehoben werden.

Der Antrag zur Erteilung einer Ausnahme ist schriftlich und vorab zu stellen.

Die aktuell gewährten Ausnahmen sind getrennt von dieser Regelung im Dokument „Ausnahmen von Sicherheitsregelungen der WU" vom InfoSec-Sicherheitskoordinator/von der InfoSec-Sicherheitskoordinatorin zu verwalten. Das Ausnahmenregister ist nicht öffentlich einsehbar zu machen.[9]

9. Qualitätssicherung

Das vorliegende Dokument wird einer jährlichen Evaluierung hinsichtlich Aktualität unterzogen.

10. Aufhebung bisheriger Regelungen

Mit Kundmachung dieses Dokuments werden die folgenden Regelungen außer Kraft gesetzt und durch das vorliegende Dokument ersetzt:

- „Benutzungsrichtlinie für IT-Endgeräte an der WU 2017-1.0"
- „Richtlinie für den Einsatz von Passwörtern an der WU durch MitarbeiterInnen 2017-1.0"
- „Richtlinie für den Einsatz von SAP-Passwörtern an der WU durch Mitarbeiter/innen 2017-1.0"
- „Löschungs- und Entsorgungsrichtlinie der WU 2017-1.0"

Wien, am 26.03.2019

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

[9] Einsichtsberechtigt sind das Rektorat, das Serviceteam InfoSec und IT-SERVICES. Im Anlassfall kann dieser Kreis vom InfoSec-Sicherheitskoordinator/von der InfoSec-Sicherheitskoordinatorin entsprechend erweitert werden.

11. Dokumentinformationen

Pflichtfelder sind mit einem „*" gekennzeichnet.

Kurztitel[10]*	WUPOL IT-Endgeräte
Langtitel	Version 2019-1.0 | Klassifikation: Öffentlich
Dateiname[11]*	WUPOL_IT-Endgeraete_2019-1.0.docx
Ersetzt	Benutzungsrichtlinie für IT-Endgeräte an der WU 2017-1.0, Richtlinie für den Einsatz von Passwörtern an der WU durch MitarbeiterInnen 2017-1.0; Richtlinie für den Einsatz von SAP-Passwörtern an der WU durch Mitarbeiter/innen 2017-1.0; Löschungs- und Entsorgungsrichtlinie der WU 2017-1.0 vom [Datum]
Titel englische Version	WUPOL IT End User Devices, [Link]
Version (Nummer, Datum)*	2019-1.0, vom [Versionsdatum]
Inhaltsverantwortlich*	IT-SERVICES / Schöpf, Oskar IT-SERVICES / Langenberger, Willi
Autor/in*	Riesenfelder, Christoph / [Nachname, Vorname], [Org.Einheit] /
Ansprechperson für inhaltliche Fragen und praktische Umsetzung	IT-SERVICES / Schöpf, Oskar [Org.Einheit] / [Nachname, Vorname]

Kommunikation* (Mehrfachauswahl möglich)	☐ E-Mail ☐ Mitteilungsblatt ☒ 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	Vizerektor für Forschung, Univ.Prof. Mag.Dr. Stefan Pichler am [Genehmigungsdatum]
Weitere Informationen*	InfoSec, IT-Sicherheit, Datensicherheit, Datenschutz

[10] 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

[11] Dateinamen max. 60 Zeichen; keine Umlaute, Sonderzeichen oder Leerzeichen verwenden