WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

WUPOL IT End User Devices

Version 2019-1.0 | Classification: Public

Contents

1. Purpose

Information and the related application of information technologies (IT) are indispensable to achieving business objectives and fulfilling the responsibilities of WU (Vienna University of Economics and Business).

To this end, suitable organizational and technical measures must be taken to ensure the economic, secure and legally compliant use of IT. The information and communication systems used, the applications running on them and the data processed must therefore be protected accordingly.

The personal responsibility of the user is particularly important.

The purpose of this regulation is to establish suitable regulations for the use of IT, in particular passwords, so that the achievement of the aforementioned goals of WU is ensured.

A further aim of this regulation is to ensure that information on data carriers (including paper and microfilm) remains protected if it is passed on permanently or reaches the final end of its useful life.

The provisions in this document are intended as a measure to create a reliable framework.

This document does not include explanatory statements on the individual regulations. The regulations are presented and disseminated by means of training courses and awareness-raising activities, where their background is explained in a clear and comprehensible manner.

2. Scope

This regulation applies

- to all WU employees working at administrative/service units or teaching and/or research units who use IT end user devices owned by WU or connect IT end user devices owned by WU to WU's network and access it,1 and
- in cases where these employees use IT end user devices that are not owned by WU to connect to and access WU's network,2
- to persons employed by WU's affiliated organizations who connect their IT end user devices to WU's network and access it, or use IT end user devices owned by WU,3
- to all WU students who connect IT end user devices to WU's network and access it, or use IT end user devices owned by WU,4 and
- to third parties who connect IT end user devices to WU's network and access it, in particular those who have been authorized to access systems, applications and the network operated by IT-SERVICES. These are subject to obligations as specified in the relevant items.[5]

In addition, this regulation applies without any restrictions of time and location.

3. Definitions

In the context of this regulation, relevant terms are defined as follows:

---

1 E.g. employees of service units, departments, research institutes, competence centers, and the WU Executive Academy.
2 E.g. devices financed from sponsors' funds, private devices
3 E.g. affiliated organizations, the Students' Union (ÖH), WU ZBP Career Center.
4 E.g. Internet surf stations, training, and student workplace devices, devices in the Language Resource Center and library, as well as any other publicly available IT end user devices owned by WU.
5 E.g. by means of Confidentiality Agreements, Declarations of Consent, or similar documents.

Information and Communication System

Servers, network components (routers, switches, etc.), desktops, portable devices (notebooks, tablets, etc.), network-compatible small devices (smartphones, cell phones, navigation devices, data acquisition devices, etc.), and multi-function devices (multi-function fax machines, print (fax) stations, etc.).

IT End User Device

Desktops, portable devices (laptops, tablet PCs, tablets, etc.), network-compatible small devices (smartphones, cell phones, navigation devices, data acquisition devices, VoIP telephones, etc.), end devices for device control systems, and multi-function devices (multi-function fax machines, printer (fax) stations, etc.); also workplace printers, scanners, and similar devices holding no user data or other data requiring protection (so-called IT peripheral devices).

Mobile Storage Media

Flash drives (USB flash drives), all types of memory cards (including those in multimedia players, cameras, etc.), mobile hard disk drives (e.g. magnetic and flash memory-based), CDs, DVDs, floppy disks, magnetic tapes, and similar storage media.

Data Separation

Separation of one user's data from data of other users.

Application

Applications are any type of program, including operating systems, databases, hardware protection mechanisms (e.g. for hard disk drives), access control systems, and similar programs.

Account

An account is a combination of a user ID and a password, which combined constitute a user's login data. An account grants the user access rights to an IT system.

The terms user account, access rights, or user credentials are used as synonyms for "account."

User (Account) with Extended Rights

Users (accounts) with extended rights are those who have more comprehensive rights than standard users. As a rule, administrators belong to this user group.

User ID

A user ID is termed as a character string of letters, numbers and/or special characters that are attributed to a specific access profile, and is thus individually assigned.

The term user name is synonymous to "user ID."

Password

A password is termed as a character string of letters, numbers and/or special characters that make it possible to confirm a user's identity.

The terms code word or keyword are used as synonyms for "password."

Function User ID

Contrary to an individually assigned user ID, a function user ID may be used by numerous persons.

Initial Password

An initial password is termed as a password set only once for an account.

Owner

In the context of this document, owners are persons who within the scope of their function are authorized to use storage media or devices with built-in electronic storage media. However, these could for instance also be the heads of organizational units, who, as representatives of their respective units, are understood to be owners (e.g. with regard to backup tape from the tape robot or network-attached storage).

Owners are authorized to exercise legitimate control over the storage media or devices and specify protection requirements for the data stored on them.

User

Users are persons who have been authorized by the owner of a storage medium or device with built-in electronic storage media to use it, and have the de facto power of control over the storage medium or device. The owner, however, can also be a user. If the owner cannot be clearly determined, the possessor of the storage medium or device is taken to be its owner.

Handing Over

Handing over means passing on the power of control over the storage medium or device to another person or entity. Examples are: permanently handing over a USB flash drive, returning a defective storage medium to the manufacturer, returning a notebook for proper disposal, exchanging a smartphone for a new one, throwing away paper, etc. Handing over does not mean temporarily entrusting a storage medium or device to a trustworthy person.

4. Regulations Applying to All Persons Named in the Document Scope Except for Students

4.1. General Regulations

The following regulations apply to all persons named in the document scope **except for students**:

(1) IT end user devices on which WU data is processed must be protected by access protection in the form of a PIN or password or by a biometric measure. If this measure is not or cannot be technically implemented by WU, the password regulations of WU must be implemented analogously by the user.

(2) The password-protected locking screen or the device lock on WU IT end user devices on which WU data is processed must be set so that it is activated after 15 minutes of inactivity at the latest and must be activated manually when leaving the workplace.

(3) Deactivating the preset PIN-protected device lock or the password-protected lock screen on IT end user devices is prohibited.

(4) In the event of loss or theft of an IT end user device or mobile storage media on which WU data is stored, the affected employee must comply with the process for reporting data protection incidents and immediately submit a police report to IT-SERVICES.

(5) IT end user devices owned by WU must always be operated in the standard configuration delivered by IT-SERVICES.

(6) The use of IT end devices which had their predefined authorization settings or their operating system been altered in a way that prevents standardized maintenance and administration by IT-SERVICES is only permissible for scientific employees if the management of the organizational unit agrees to this form of use. The use is at the own risk of the management of the organizational unit in which this device is operated. In such cases, IT-SERVICES does not provide support.

(7) IT end user devices that are not maintained and administered by IT-SERVICES, in particular dual-boot devices, are operated at the user's own risk. The claim for support by IT-SERVICES does not apply in these cases.

(8) An up-to-date and activated real-time malware scanner must be installed, if such a scanner is supported by the operating system.

(9) Current malware signatures must be available immediately after the connection has been established.

(10) An up-to-date local firewall that monitors incoming and outgoing data traffic must be installed and activated if such a firewall is integrated in the operating system by default.

(11) The operating system and the installed applications must be kept up-to-date with regard to security updates.

(12) Mobile storage media installed in IT end user device equipment owned by WU must be encrypted.

(13) Mobile storage media on which data of the WU classified as internal or confidential is stored must be encrypted.

(14) The work with administrator or root rights on IT end user devices with separation of rights is prohibited, except for work related maintenance purposes.

(15) On IT end user devices which are also used by users other than the authorized user, in particular devices which are not the property of WU, suitable measures must be taken for data separation. Otherwise the IT end user device may only be used by the authorized user.

(16) The storage of private data on IT end user devices and mobile data carriers owned by WU is permitted to a limited extent, on desktops, notebooks and Tablet-PCs however only in a directory designated as "private".

(17) Private data on IT end user devices and mobile storage media owned by WU must be deleted by the person who has stored such data there upon request by IT-SERVICES.

(18) Notebooks owned by WU must, if possible, be connected with a cable lock to a fixed object in case of unsafe locations, unless they can otherwise be physically secured against removal (theft protection). Cable locks can be obtained from IT-SERVICES.

(19) The respective user is responsible for backing up data from IT end user devices.

(20) Masquerading one’s own identity, in particular the official identity, while using the Internet is prohibited.

(21) It is forbidden to change any settings that are recognizable as security-relevant.

(22) The installation of programs that pose security risks is prohibited.

(23) The use of software, hardware and other means whose purpose is to spy on information is prohibited.

(24) Deliberately taking IT-related security risks is prohibited. In case of doubt, coordination with IT-SERVICES must be sought.

(25) Copyrights must be adhered to and license terms must be observed.

(26) Upon termination of the employment relationship, IT work equipment owned by WU must be returned to the respective supervisor or to IT-SERVICES.

(27) Upon termination of a contractual relationship, IT work equipment owned by WU must be returned to the respective contact person of WU.

4.2. Use of Passwords

(28) Authorized users are obligated to keep their passwords secret and may not share them with third parties.6 Users must take care that they are unobserved when entering their passwords.

(29) Passwords may not be transmitted unsecured over the network.

(30) Passwords must differ significantly from other personally used passwords.7

(31) If it must be assumed that unauthorized persons are or could be in possession of an authorized user's password, then the authorized user must change his or her password or request a password reset.

(32) Function users' passwords may be shared only by the person responsible for the respective function user ID, and may be shared only with persons who require the password to fulfill their jobs at WU.

(33) Authorized users must be able to change their passwords at any time. This must be ensured by the operator of the access control system.

(34) Passwords for function user IDs may be changed only by the person responsible for the respective ID. Whenever a member leaves the ID group, the password must be changed immediately.

(35) Initial passwords must be changed to passwords compliant with the minimum requirements after the first login.

(36) If a user logs on to a WU network using an external system not operated by WU, then they must log out immediately after using it.

(37) Additional regulations can be stipulated from case to case as deemed necessary due to specific risk factors.

4.3. Use of Extended Rights

(38) Passwords for users with extended rights must be documented securely to ensure that WU can continue to use the account in exceptional cases.

[6] Including persons such as supervisors, deputies, or assistants

[7] Especially Wi-Fi (WLAN) password and WU password must differ significantly

4.4. Assignment of Initial Passwords

(39) Only for SAP: The SAP administrator and the user set the initial password together during the initial login. The initial password is to be used only once.

(40) Initial passwords must meet or exceed the minimum requirements.

(41) Concerning all except SAP: Initial passwords must be randomly generated and individually allocated and must be valid for a limited time only.

(42) Factory-set passwords must be changed immediately in accordance with the minimum requirements.

4.5. Password Structure

The binding regulations detailed below are supplemented by recommendations (guidelines) not included in this Directive to facilitate implementation, e.g. tips on finding secure passwords.

Passwords must meet the following minimum requirements:

Characteristic	**Standard User**	**User with Extended Rights**
Minimum password length	8 characters for SAP 12 characters for IT-SERVICES staff 10 characters for others	8 characters for SAP 16 characters for others
Inadmissible phrases	No restrictions for SAP Password may not include user ID for others	No restrictions for SAP Password may not include user ID for others
Complexity requirements: See below a) and b)	None for SAP Yes for others	None for SAP Yes for others
Device lock/screen lock	After 15 minutes of inactivity	After 15 minutes of inactivity
Password reuse	The last two (SAP: 3) passwords may not be reused	The last two (SAP: 3) passwords may not be reused
Maximum password age	180 days for SAP No requirements for others	180 days for SAP No requirements for others
Minimum password age	1 day for SAP No requirements for others	1 day for SAP No requirements for others
Permissible attempts until account is locked	3 attempts for SAP No requirements for others	3 attempts for SAP No requirements for others

Waiting time until the next attempt	No requirements	No requirements
Counter reset for blocked accounts	No requirements	No requirements

a) **Passwords, except for SAP,** must feature all of the following characteristics:

- At least one capital letter (A to Z)
- At least one lower-case letter (a to z)
- At least one number (0 to 9)
- At least one special character

b) **PINs** must feature all of the following characteristics:

- Digits only (0 to 9)
- Minimum length: four characters

On IT end user devices owned by WU, compliance with security measures can be audited by WU at any time.

4.6. Deletion of Data and Destruction of Storage Media

The owner or the authorized user is responsible[8] for the secure erasure and disposal of data and storage media.

In the event that equipment and thus permanently installed electronic storage media are not the property of WU, but contain data worth protecting (e.g. in the case of equipment leasing for intelligent printing stations), the owner of the respective equipment must be contractually obliged to delete this electronic storage media in accordance with the provisions of WU or to physically destroy and dispose of it. This applies in particular to suppliers of test equipment or of leased or rented multifunction devices (printers).

When electronic storage media have come to the end of their service life, or when electronic storage media are to be passed on or disposed of, the data stored on them must be erased, if technically possible, prior to handing the storage medium in or passing it on.

Disposing of storage media with non-public contents		
Type of storage medium		**Procedure**
Hard disk drives from notebooks, desktop computers, and servers, as well as external hard disk drives and NAS drives	Magnetic hard disk drives	Secure erasure, subsequently return the device or disk drive to IT-SERVICES
	SSD (flash-based solid state drive)-hard disk drives and hybrid hard disk drives (= flash drive & magnetic drive)	Initialize via the manufacturer's program, subsequently return the device or disk drive to IT-SERVICES

[8] Upon request, IT-SERVICES is available to properly dispose of storage media, i.e. to destroy them. A request for the storage medium to be picked up by IT-SERVICES can be sent e.g. via a Helpdesk ticket.

Small devices with built-in storage media	Smartphones, tablets, cell phones	Reset to factory settings, subsequently return to IT-SERVICES for disposal by a specialized disposal company
	PDAs, cameras, multimedia players, etc.	Reset to factory settings, subsequently return to IT-SERVICES
Small storage media, with the exception of CDs and DVDs	USB flash drives, memory cards (SD, MMC, etc.), other small flash drive storage media	Secure erasure, subsequently return to IT-SERVICES
	Floppy disks, ZIP cartridges	Perforate or return to IT-SERVICES
CDs, DVDs, and other optical storage media		Scratch, perforate, or return to IT-SERVICES for shredding
Backup tapes from tape stations and tape robots		Return to IT-SERVICES
Paper, incl. photographic paper, and microfilm		Shredding or cutting into pieces manually
Other storage media, irrespective of whether electronic or physical in nature and of the device they are built into		Securely erase electronic storage media, or reset/initialize the device and destroy it; destroy non-electronic storage media

In case of doubt, storage media must be physically destroyed.

An authorized, designated IT-SERVICES employee must physically destroy electronic storage media within six months after taking them over. If physical destruction is not directly performed at WU, the storage media in question must be disposed of by a qualified waste disposal company.

In cases where IT-SERVICES has to hand over electronic storage media to a qualified waste disposal company for disposal, the following regulations apply: IT-SERVICES is responsible for the disposal, IT-SERVICES must arrange the physical disposal within six months after taking over the storage medium, and the waste disposal company must monitor and document the process.

5. Regulations for Students

The following regulations apply to students:

(1) Malware signatures must be kept up to date and must be updated prior to further use of the network connection to WU.

(2) Copyrights must be adhered to and license terms must be observed.

(3) Upon termination of contractual relationships, IT end user devices owned by WU must be returned to the appropriate WU contact person.

The following activities are strictly prohibited:

(4) Booting publicly accessible IT end user devices from external storage media;

(5) Using software, hardware and other means whose purpose is to spy on information.

6. Reporting Security Incidents and Risks

All persons encompassed within the scope of this regulation are obligated to immediately report security-relevant incidents and risks to it-security@WU.ac.at.

7. Consequences of Non-Compliance

Compliance with regulations and security measures is monitored on a regular basis, but also if and when indicated by specific circumstances.

Non-compliance may lead not only to disciplinary action and consequences under employment law, but also to civil and criminal proceedings.

8. Exceptions

As a rule, standard procedures that are in accordance with this regulation remain the first choice. Exceptions shall only be considered if standard procedures are found to be inadequate or impractical for technical or organizational reasons, or for reasons of economy.

Exceptions must be:

- Limited in duration,
- Limited to a specific purpose and group of users,
- Fully documented regarding the application, the decision to approve or reject the application, any changes made, and expiry of the exception granted,
- Reviewed and phased out after an appropriate period of time, if the exception expires and no reapplication is submitted, and
- Immediately canceled in the case of non-compliance with any of WU's regulations.

Applications for exceptions shall be submitted in advance and in writing.

All exceptions currently in place shall be listed separately from this regulation in a supplementary document entitled "Ausnahmen von Sicherheitsregelungen der WU," administered by the InfoSec Security Coordinator. This list of exceptions shall not be made publicly available[9].

9. Quality Assurance

This document is subject to an annual review.

In the event of discrepancies between the German original and the English translation, the German version shall prevail.

10. Invalidation of Previous Regulations

This document replaces the following previous regulations, which cease to be effective upon official publication of this document.

- „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"

[9] Only the members of the Rector's Council, the InfoSec Service Team, and IT-SERVICES shall have access to this document. If circumstances warrant, access can be granted to additional parties by the InfoSec Security Coordinator as needed.

Vienna, March 26, 2019

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

11. Document Details

All fields marked with an asterisk (*) are required.

Short title[10]*	WUPOL IT End User Devices
Long title	Version 2019-1.0 | Classification: Public
File name[11]*	WUPOL_EN_IT_End_User_Devices_2019-1.0.docx
Replaces	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 dated [date]
Title of German version	WUPOL IT-Endgeräte, [link]
Version (number, date)*	2019-1.0, dated [version dated
Responsible for content*	IT-SERVICES / Schöpf, Oskar IT-SERVICES / Langenberger, Willi
Author*	Christoph Riesenfelder / [last name, first name], [Organizational unit] / [last name, first name]
Contact for content-related questions and practical implementation	IT-SERVICES / Schöpf, Oskar [last name, first name]

Communication* (multiple selection is possible)	☐ email ☐ WU Bulletin ☒ WU regulations database
Publication in the WU Bulletin (*Mitteilungsblatt*)	WU Bulletin Academic year XXXX/XXXX, Issue XX, [WU Bulletin no.] dated [date], [link]
First publication (optional)	WU Bulletin Academic year XXXX/XXXX, Issue XX, [WU Bulletin no.] WU Bulletin [no.] dated [date of first publication]

Valid as of*	April 1, 2019
Valid until*	December 31, 2999
Approved by	Vizerektor für Forschung, Univ.Prof. Mag.Dr. Stefan Pichler on [approval date]
Further information*	Data Protection, Privacy, Security

[10] Examples of short/long titles:
- Short title = category and keyword, e.g. WUPOL Software
- Long title or subtitle = designation provided by the organizational unit, e.g. "Regulation on the use of WU Software"

[11] No more than 60 characters; do not use any diacritics, special characters, and spaces