WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

DIR Information Security

Directive on Information Security Management at WU

Contents

Please note: This is a partly machine-translated document provided **for your information only**. In case of discrepancy, the German original shall prevail.

1. Purpose

The objective of this directive is to specify an appropriate level of security to ensure adequate protection of digital and analog confidential information (in accordance with the corresponding sensitivity classification) and to increase resilience against cyberattacks.

2. Scope

Compliance with the Directive on Information Security Management at WU is mandatory for all employees and students.

As far as its material scope is concerned, this directive applies to analog information and to information and communication technologies (ICT):

- Existing information and communication technology (ICT) components and applications
- New information and communication technology (ICT) components and applications
- Updates of information and communication technology (ICT) components and applications

Appropriate agreements are to be concluded with partners and service providers requiring them to comply with the relevant provisions that apply in each case.[1]

This directive is valid until May 30, 2028, and it applies regardless of location.

3. Glossary

The glossary for this directive is available at https://wiki.wu.ac.at/x/FBoiE (in German).

4. Information security objectives

This information security directive supports the digitalization strategy of WU (Vienna University of Economics and Business) by ensuring the secure processing of confidential information and preventing disruptions of the university's operations.

The goal is to establish an appropriate level of information security that makes it possible to identify potential threats and mitigate them to acceptable levels through appropriate measures, as well as to identify the remaining residual risks and accept them based on transparent criteria. This includes the following primary objectives:

- **Risk assessment** – Based on an up-to-date risk assessment, current and future cybersecurity risks are identified and addressed using economical approaches.
- **Protection of confidential information** – Any confidential information (analog and digital) that is processed must be protected and may only be made accessible to persons authorized to access it. This applies to technical measures (e.g. protection against cyberattacks) as well as to organizational measures (e.g. access authorization).
- **Cybersecurity resilience** – Development of a strategy to ensure that the basic services essential to the university's operations remain functional in the event of a cyberattack
- **Compliance** – Adherence to data protection regulations and other applicable legal requirements

To support the objectives outlined above, an information security management system (ISMS) based on the ISO 27001 framework is established.

[1] E.g. in the form of confidentiality agreements, declarations of consent, or similar instruments.

In implementing the ISMS, we focus on raising awareness of information security and gradually improving the pertinent skills. All relevant people are informed, briefed, and trained according to their specific responsibilities, roles, and tasks, while taking into account the prior knowledge of the target groups (Rector's Council, management personnel, heads of organizational units, IT staff, and external partners) and preparing and communicating the relevant content in a way that is appropriate for the target group.

To ensure information security, the IT infrastructures and procedures used to process information must also comply with the relevant security requirements. The necessary IT security measures (specified in the WUPOL documents that form part of the ISMS, see section 4.4.) are defined in a way that is risk-oriented and takes into account the current state of the art.

The Rector's Council regards information security and the resulting ISMS as a matter of strategic importance, and it is expressly committed to continuously improving, promoting, and supporting all necessary activities and measures in this connection. A Chief Information Security Officer (CISO) (for a description of the CISO's role, see section 4.2) is appointed to further develop the present regulations, implement them, establish an ISMS, and monitor compliance.

Information security is a collective responsibility that requires everyone to protect information and accept the necessary extra effort needed to ensure compliance with the specified security measures for the benefit of the organization as a whole.

Management personnel are required to ensure compliance with the ISMS (as specified in the WUPOL documents that form part of the ISMS, see section 4.4.) in their areas of responsibility.

In addition to the provisions of this directive and the WUPOL documents derived from it, the following principles always apply:

Authorizations to access data and information have to be granted based on the tasks to be performed. This means that people should only be given access to those data and information that are necessary for fulfilling their respective tasks and roles (need-to-know principle).

And:

Persons, users, systems, applications, etc. should have as few access rights as possible. This means that rights and permissions to access, read or create, write, change, and delete data, execute files, and transfer authorizations should always be limited to the minimum that is required for the task to be performed in each case (principle of least privilege).

4.1. Intended security level

Implementing information security is always a trade-off between risk and cost.

At the security level that this directive is aiming for, risks are assessed based on the following types of attackers, and information security measures are implemented to protect against the threats posed by them:

- **Criminal groups:** These are organized groups of hackers who penetrate computer systems for economic gain. These groups use phishing, spam, spyware, and malware for extortion, theft of private information, and online fraud.
- **Hackers:** Individual hackers target companies using a variety of attack techniques. Their motives usually include personal gain, revenge, financial gain, or political activism. Hackers often develop new types of attacks to improve their criminal skills and increase their personal standing in the hacker community.
- **Malicious insiders:** These are people who are legitimately authorized to access organizational resources and who abuse their access privileges to steal information or

damage computer systems for economic or personal gain. Insiders may be employees, contractors, suppliers, or partners of the targeted organization.

4.2. Roles, rights, and duties in the organizational framework for information security

This section defines the organizational structure of the information security framework.

The following list defines the information security responsibilities within the information security management system (ISMS). Individuals with assigned responsibilities may delegate tasks to others, but they remain responsible for the activities in question and must review them to make sure that all tasks have been performed properly.

Rector's Council

The Rector's Council regards information security as a matter of strategic importance and decides on the overall strategy. This strategy is proposed to the Rector's Council by the CISO, along with proposals for the implementation of individual measures or a package of measures. The Rector's Council then instructs the appropriate Vice-Rector to implement the package of measures or individual measures.

Chief Information Security Officer (CISO)

The CISO provides advice and prepares guidelines in all matters relating to information security and, in this capacity, reports directly to the Vice-Rector responsible for these matters. Reports should be submitted to the Vice-Rector at least once a month. In addition, a report must also be submitted to the Rector's Council once a year (see 4.3.).

As part of their responsibilities, the CISO in particular has co-decision and veto rights vis-a-vis the organizational units that implement measures relating to information security (e.g. storage of data, transmission of data). The CISO specifies the level of protection that is required but not the means by which this level of protection is to be achieved. The Rector's Council may decide to approve exceptions to the information security requirements (see section 6).

The CISO's agendas may be supplemented by other functions managed centrally by the CISO: Information Security Officer (ISO), Information Security Risk Manager (ISRM), Cyber Security Architect (CSA), and Cyber Defense Center (CDC) staff.

Management personnel

Management personnel have a special responsibility to act as role models in all matters related to information security. In addition, all management staff members are obligated to ensure and monitor compliance with the ISMS in their respective areas of responsibility (as specified in the WUPOL documents that form part of the ISMS, see 4.4.).

Employees

All WU employees are required to comply with the ISMS (as specified in the WUPOL documents that form part of the ISMS, see 4.4.).

Students

All WU students are required to comply with this directive.

4.2.1. Independence

The function of the CISO is only bound by the technical and budgetary instructions given by the Vice-Rector in charge of this area of responsibilities.

The CISO is neither responsible for the technical implementation of security measures, nor does the CISO make decisions on the technical means to be employed. These tasks are the responsibility of the head of the respective academic teaching and/or research unit or the head of the respective service unit (according to the Organizational Structure Plan of WU). Upon request, the CISO or the CSA may provide assistance in these tasks.

Likewise, the CISO is not responsible for implementing information security policies in the individual organizational units. This responsibility lies with the management personnel of the respective unit.

4.3. Senior management review

The Rector's Council regards information security as a matter of strategic importance and must therefore be informed about the effectiveness and operation of the ISMS on a regular basis. For this reason, a senior management review[2] must be scheduled and carried out at least once a year. This includes reports on the following items:

- A report on the measures defined as part of the previous review and their current status
- A status report on information security matters within and outside of the organization
- Relevant information security incidents and follow-up measures
- Results of the audits conducted according to the audit plan (see 4.6.)
- Results of the information security risk analyses
- Suggestions for improvement and steps to be taken

If necessary, the Rector's Council may decide to shorten the reporting interval.

4.4. Regulatory hierarchy

The hierarchy of the documents included in the ISMS adheres to the specifications of the WUPOL Regulations Management Guidelines (reference), section "Categories and categorization of regulations."

All **WUPOL documents** included in the ISMS follow the naming scheme "WUPOL Information Security Requirements for [subject of WUPOL]."

4.5. Interfaces

4.5.1. ICT systems operation

The organizational unit responsible for the operation of the respective ICT systems must ensure compliance with the ISMS. The applicable regulations are defined in the relevant WUPOL documents on information security requirements.

[2] The term "senior management" is defined in ISO/IEC 27002:2022. In the case of WU, the senior management corresponds to the Rector's Council.

4.5.2. ICT change management

Changes to ICT systems that have an impact on information security must be evaluated and documented before the change is made. This includes the creation of an operating manual for the system, documentation of the interfaces involved, including the protocol, port, and direction of data traffic, and documentation of the responsibilities with regard to information security.

4.5.3. Physical security

Physical security regulations are specified in the WU House Regulations (see link) issued by Campus Management.

4.6. Independent information security audits

To ensure that the requirements specified in the applicable directives, norms, standards and other relevant specifications are met, audits must be carried out. The CISO submits an annual audit plan to the Rector's Council for information, which is based on the chapters of ISO27001 and a risk-based approach. In addition to the scheduled audits according to the annual audit plan, the auditing activities of the CISO also include ad hoc audits, which the CISO initiates or which are initiated voluntarily by the organizational unit responsible (for the operation of the respective ICT system):

- The audit can be performed by an internal auditor or an external organization but not by the organizational unit responsible (for the ICT system to be audited)
    - Access to information required for the audit has to be arranged with the appropriate management personnel.
    - The scope and date of the audit must be defined and communicated.
- The results of the independent audit must be recorded and reported to the head of the respective academic teaching and/or research unit (according to the Organizational Structure Plan of WU) or the head of the respective service unit, as well as to the CISO.
- All auditing activities are to be monitored and documented by the person who has initiated the audit.
- Any shortcomings are to be documented and discussed with the head of the academic teaching and/or research unit (according to the Organizational Structure Plan of WU) or the head of the respective service unit. Shortcomings are to be recorded in a central vulnerability tracking register. In case of imminent danger, the Rector's Council must be informed immediately.

5. Invalidation of previous regulations

- WUPOL Informationssicherheitspolitik (*WUPOL Information Security Policy*) dated April 1, 2019
- WUPOL Informationssicherheitsstrategie (*WUPOL Information Security Strategy*) dated April 1, 2019
- WUPOL InfoSec Regelungshierarchie (*WUPOL InfoSec Regulatory Hierarchy*) dated April 1, 2019
- WUPOL Privacy by Design dated April 1, 2019

6. Exceptions

All requirements listed in this directive must be met for the introduction of new ICT systems. For existing ICT systems, the requirements must be met within a period of six months from publication of this directive.

If certain requirements cannot be met, the organizational unit responsible (for operating the ICT system in question) must take appropriate compensatory measures or draw up an appropriate implementation plan and obtain the CISO's approval for this plan.

If no agreement can be achieved through these procedures, the Rector's Council may approve an exception.

7. Quality assurance

This document will be subject to annual evaluation to ensure that it is up to date.

8. Document details

Short title	DIR Information Security
Long title	Directive on Information Security Management at WU
File name	DIR_Information_Security
Replaces	WUPOL Informationssicherheitspolitik (WUPOL Information Security Policy) dated April 1, 2019 WUPOL Informationssicherheitsstrategie (WUPOL Information Security Strategy) dated April 1, 2019 WUPOL InfoSec Regelungshierarchie (WUPOL InfoSec Regulatory Hierarchy) dated April 1, 2019 WUPOL Privacy by Design dated April 1, 2019
Title of German version	RL Informationssicherheit
Version (number, date)	2023-1.0, dated July 4, 2023
Responsible for content	Matthias Harrer / CISO
Author*	Matthias Harrer / CISO
Contact for content-related questions and practical implementation	Matthias Harrer / CISO

Communication (multiple selection is possible)	☐ email ☐ WU Bulletin ☒ WU regulations database
Publication in the WU Bulletin (*Mitteilungsblatt*)	German version: academic year 2022/2023, issue 42, no. 256, dated July 12, 2023

Valid as of	July 12, 2023
Valid until	June 30, 2028
Approved by	Rector's Council, on July 11, 2023
Further information	information security, ISMS, data protection