Attachment to Ordinance No.33
of the Rector of Poznan University of Technology
of 18 October 2024 (RO/X/33/2024)

INFORMATION SECURITY POLICY OF POZNAN UNIVERSITY OF TECHNOLOGY

Table of Contents:

1. Purpose and Scope of the Information Security Policy 3
2. Terms and Definitions 3
3. Responsibility for Information Security 4
4. Human Resource Security 6
5. Rules for Cooperation with External Parties 6
6. Cooperation with Public Authorities and External Specialists 7
7. Security of Transmitted and Shared Information 7
8. Security of Assets and Systems 7
9. Physical and Environmental Security 8
10. Incident Management 8
11. Audits, Reviews, Corrective Actions and Improvement 9

1. Purpose and Scope of the Information Security Policy

Poznan University of Technology, recognising the importance of information security, establishes the Information Security Policy with the aim of:

a) supporting the implementation and achievement of objectives of fundamental significance for the functioning of the University,
b) protecting the confidentiality, integrity, and availability of information, in accordance with the requirements of legal provisions, the University's internal regulations, guidelines, and standards, in particular striving to ensure compliance with the ISO/IEC 27001 standard,
c) fostering continuous improvement through raising awareness of the importance and necessity of adhering to the principles of information security,
d) preventing information security incidents by identifying and classifying information, analysing risks, and undertaking preventive actions designed to minimise the likelihood of events or information security incidents,
e) ensuring cost-optimal conditions for the operation and development of IT resources,
f) communicating that compliance with the principles of information security and undertaking actions to safeguard it, in order to maintain the continuity of the University's operations, is the responsibility of every employee, student, as well as external persons cooperating with the University.

The detailed rules for the security of information processed at the University are defined in this Information Security Policy and the related procedures and internal regulations, including those concerning processes and projects in which data and information are processed, systems already in place and those being implemented now or in the future, and all locations, buildings, and rooms where information subject to protection is or will be processed.

2. Terms and Definitions

The terms used in this Policy shall have the following meanings:

a) Information Security Management System (ISMS) – a set of policies, procedures, and guidelines managed collectively by the organisation to safeguard information assets,
b) University – Poznan University of Technology,
c) Rector – the Rector of Poznan University of Technology,
d) Data Protection Officer (DPO) – the person designated to perform tasks in accordance with the General Data Protection Regulation (GDPR),
e) Information Security Officer (ISO) – the person responsible for maintaining, monitoring, and improving the ISMS,
f) User – a person processing information, including personal data, with access to the University's IT systems,
g) Employee – a person performing work for the University under an employment contract,
h) Student – a first-cycle or second-cycle student, Ph.D student, or participant in studies making use of the University's teaching process,

i) External Person – a natural person, legal person, or organisational unit without legal personality, who is not an employee or student, but has access to information in the course of cooperation with the University (e.g. carrying out tasks commissioned by the University),
j) University IT System – computer hardware, software, and servers operated centrally at the University, forming a set of interrelated devices, programmes, information-processing procedures, and software tools; this system includes at least one central computer and constitutes the data controller's telecommunications network,
k) Personal Data – information relating to an identified or identifiable natural person ("data subject"),
l) Information – assets essential for ensuring the proper functioning of the organisation and the execution of its assigned tasks, which require protection. Information may be stored in various forms: electronically, on paper, or immaterially as knowledge held by employees,
m) Processing – any operation or set of operations performed on information, including personal data or sets of personal data, whether automated or non-automated (such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction),
n) Password – a sequence of letters, numbers, or other characters, known only to the user,
o) Identifier (login) – a sequence of letters, numbers, or other characters that uniquely identifies a person within the IT system,
p) Integrity – the property of safeguarding data from being altered or destroyed in an unauthorised manner,
q) Confidentiality – the property that data is not made available or disclosed to unauthorised entities,
r) Availability – the property of information being accessible and usable on demand by an authorised user within the required timeframe,
s) Authentication – the act of verifying the declared identity of a subject,
t) Risk – the probability of a threat materialising which may cause damage to the University's assets, or result in interruptions or disruptions to its functioning and the achievement of its planned objectives and tasks,
u) Threat – a situation or event, intentional or accidental, which creates a potential possibility of damage, interruption, or disruption to the functioning of the University,
v) Information Security Incident – an event classified as significant or critical, evidencing a breach of information security, the occurrence of which results in a loss of confidentiality, availability, or integrity of data.

3. RESPONSIBILITY FOR INFORMATION SECURITY

Responsibility for information security is borne by all employees, in accordance with their re-

spective duties, as well as students and external persons processing the University's information.

The **Rector** is responsible for taking the necessary and appropriate steps to ensure information security, in particular by:

a) providing guidance and support for information security activities in accordance with legal provisions, standards, and other regulations,
b) establishing objectives for information security,
c) appointing the Information Security Officer and ensuring the resources necessary to fulfil the assigned tasks,
d) establishing and approving ISMS documentation.

The **Information Security Officer** is responsible for monitoring and improving the ISMS and adapting it to the changing organisational and legal environment, in particular by:

a) supervising compliance with the provisions of the ISMS and updating its records,
b) undertaking actions aimed at increasing awareness of information security among employees, students, and external persons,
c) providing information and guidance concerning the ISMS,
d) carrying out, in cooperation with organisational units, risk assessments and analyses of ISMS components, as well as developing plans for responding to identified risks,
e) reporting to the Rector on actions undertaken as part of the implementation and maintenance of the ISMS,
f) coordinating internal and external audits concerning information security,
g) coordinating the handling of information security incidents.

Heads of organisational units are responsible for:

a) supervising the implementation of the provisions arising from the ISMS within their subordinate units,
b) determining access for their subordinate employees to data and information in IT systems and in traditional form, as well as monitoring access and introducing modifications where necessary,
c) taking action in situations where risks materialise or information security incidents occur,
d) cooperating with the Information Security Officer in maintaining and improving the system, including the identification and classification of information and the analysis of risks in this area.

The Heads of:

a) the Services and Operation Office,
b) the Integrated IT Office,
c) the Software Development Office,
d) the Student Affairs Centre,
e) the Security Office,

and

f) the Data Protection Officer,

due to the fundamental scope of tasks established by internal regulations, are particularly responsible for ensuring information security and for undertaking actions aimed at maintaining and developing the ISMS.

Employees, students, and external persons are responsible for:

a) complying with the documentation comprising the ISMS, including procedures, instructions, and ordinances,
b) maintaining the confidentiality of protected information to which they gain access in connection with their duties, both during the course of employment or other legal relationship, and after its termination,
c) making every effort to protect the information entrusted to them and the resources used, including safeguarding them against disclosure to unauthorised persons,
d) preventing attempts to breach security rules and reporting all events and incidents relating to breaches of the ISMS in accordance with the applicable procedures,
e) submitting comments and proposals for amendments to the ISMS,
f) engaging in raising awareness with regard to the ISMS.

4. HUMAN RESOURCE SECURITY

As part of employment, employees are required to familiarise themselves with the applicable regulations, including the completion of introductory and job-specific training, among others in the field of security and protection of assets and personal data, physical security rules, and access control. At the commencement of employment, an employee is granted access rights necessary for the performance of assigned tasks. In the event of a change in employment conditions, access rights are appropriately modified on the basis of a request submitted by the supervisor.

In the case of a change or termination of employment, access rights are revoked or altered. Revocation or modification of access applies both to physical access and to access within IT systems.

5. RULES FOR COOPERATION WITH EXTERNAL PERSONS

An external person granted access to selected information and data of the University is obliged to comply with the requirements of legal provisions, as well as internal regulations related to ensuring information security.

The University applies rules governing access to the network and to specific resources within those networks, under which access rights for external persons cooperating with the University are granted upon the request of the employee coordinating the cooperation.

6. COOPERATION WITH PUBLIC AUTHORITIES AND EXTERNAL SPECIALISTS

The University maintains contact with public authorities and supervisory bodies in cases indicated by legal provisions and in accordance with the University's internal regulations, both in the field of physical security (the Security Department coordinating contact, among others, with state services responsible for maintaining public order and safety), and in the field of cybersecurity (the Information Security Officer coordinating contact with CSIRT NASK).

The University also enables the maintenance of contacts with external specialists, associations, and partners, which allows for:

a) broadening knowledge in the area of information security from legal and technical perspectives,
b) obtaining immediate information about threats that may affect the University's activities,
c) exchanging experience with entities from the higher education sector.

7. SECURITY OF TRANSMITTED AND SHARED INFORMATION

When sharing data and information subject to special protection, particular attention is paid to the correctness of the recipient's details.

In the case of transmitting special categories of personal data (as defined in Article 9 of the General Data Protection Regulation) or information subject to special protection (e.g. trade secrets, financial data, unpublished know-how, in particular concerning technological solutions, and access credentials to resources) by means of electronic tools, such data shall be encrypted by securing the files with a password, which must be communicated to the recipient via a different communication channel than the one used to transmit the information.

In situations where regular data transmission between the University and other entities is required, it is recommended that the method of information exchange be agreed between the parties.

Procedures concerning classified data and information, and the manner of their processing and sharing, are governed by separate external and internal regulations relating to the processing of classified information.

8. SECURITY OF ASSETS AND SYSTEMS

At the University, mechanisms of multi-layered protection of network traffic, systems, and University servers are implemented, developed, and maintained in order to protect against unauthorised access. These include mechanisms for filtering e-mail, as well as security measures for end devices (computers, servers, printers, drives), comprising configurations

that ensure regular software updates, installation of monitoring tools, and protection against malicious software.

The University applies the principle of restricted access, under which access to physical resources, data, and information in IT systems is limited in particular to elements necessary for the proper execution of tasks by an employee, student, or external person, in accordance with the functional capabilities of the IT system. Access to IT systems is based on user authentication procedures, which also provide for the possibility of two-factor authentication.

The University has established rules for working with portable devices, data carriers, and the use of IT resources as part of work carried out off-site (remote work). As part of the management of the University's IT systems, rules are also implemented and maintained concerning:

a) designing system architecture and functionality with due consideration of security aspects,
b) carrying out pre-implementation tests to verify mechanisms ensuring the security of data and information,
c) creating and testing backups of software,
d) supervising services delivered by external entities and third parties,
e) password management and user authentication.

The aim of the security measures implemented at the University is the safe operation and maintenance of the University's IT assets and systems, the security and continuity of services, and the minimisation of risks and the effects of security events and incidents.

9. PHYSICAL AND ENVIRONMENTAL SECURITY

In order to reduce risks arising from physical and environmental threats, the University applies access control procedures and physical security measures, including:

a) managing physical access to facilities, rooms, and other locations where information is stored, including the implementation of physical barriers to prevent unauthorised access,
b) monitoring the movement of persons within University buildings and rooms,
c) applying environmental safeguards to protect information and other assets from destruction or damage caused by natural phenomena.

The purpose of the physical security measures implemented at the University is to reduce the likelihood of unauthorised access, loss, damage, theft, or compromise of the University's assets.

10. INCIDENT MANAGEMENT

Employees, students, and external persons are obliged to inform the University's services of any suspected or actual breach of information security, in particular in the event of:

a) disclosure to third parties of information such as login, password, PIN number, etc., or identification of an access breach in this respect,

b) unauthorised access to an ICT device, ICT network, IT system, or data stored in the IT system,
c) intentional suspension of the operation of an ICT service or causing unavailability of a system or service,
d) detection of attempts at user impersonation,
e) identification of malicious software, suspicion of such software, or attempted attacks on the University's ICT infrastructure,
f) discovery of electronic or physical traces of attempted break-ins into University premises,
g) identification of an event or incident concerning the physical security of the University's property, in particular as a result of fire, flooding, etc.

The person identifying the event shall immediately report this fact to the University using:
a) the Central Incident Reporting System, available at pomoc.put.poznan.pl,
b) the e-mail address pomoc@put.poznan.pl, if the Central Incident Reporting System is unavailable,
c) telephone number 61 663 6111, if it is not possible to carry out the operations listed above.

Until the report is resolved, the reporting person is obliged to comply with the instructions of first-line support, the Information Security Officer, or persons indicated by them, in particular by taking actions aimed at preventing further escalation of the incident's effects, including:
a) securing a potentially infected device,
b) disconnecting the device from the network by unplugging the network cable or disconnecting from the wireless network – without switching the machine off,
c) securing the physical location where an attempt at unauthorised access has been identified.

The report shall include all relevant information, in particular:
1) data of the reporting person:
2) name, surname, e-mail address, contact telephone number,
3) time and place of occurance,
4) description of the course of the event or incident (manner of identification, actions taken),
5) indication of the IT/physical asset concerned by the event or incident,
6) observed effects of the event or incident,
7) other relevant information.

The Information Security Officer is obliged to notify the Rector in the event of identifying a risk that may affect the University's core activities. The Officer also coordinates the process of reporting the incident to external services and authorities, including, for example, CSIRT NASK, and oversees the communication required during incident handling.

11. AUDITS, REVIEWS, CORRECTIVE ACTIONS AND CONTINUAL IMPROVEMENT

In order to ensure a high level of information security, internal audits are periodically planned

with the aim of ensuring that the applied procedures, safeguards, and measures are:

a) compliant with applicable laws, standards, internal regulations, guidelines, and procedures,
b) effective and adequate,
c) implemented in accordance with the intended objectives.

The scope of the audit is defined by the Information Security Officer in consultation with the Rector or designated persons, and is determined on the basis of risk analysis, information obtained from University employees and collaborators, results of internal and external inspections, as well as guidelines issued by external institutions.

On the basis of audit activities, management reviews, reports, events, and incidents, corrective actions are undertaken at the University with the aim of ensuring the continual improvement of the Information Security Management System (ISMS).