ROSKILDE UNIVERSITY
RUC Digital/CISO 01-12-2024

Information Security Policy for Roskilde University

The information security policy is effective from October 1, 2024, and will next be revised in September 2025. The policy has been approved by the Executive University Management on October 25, 2024.

CONTENT

1.Purpose of the Information Security Policy

Information Security involves protecting information, such as data, information and knowledge, against misuse, unauthorized access, interruption, or destruction. It is defined as the tools and processes Roskilde University (RUC) uses to safeguard our information. This includes everything from physical security, protection of digital devices (servers, computers, tablets, phones etc.) and data encryption to network and infrastructure security as well as testing and audits

Universities are required to have an information security policy that outlines how relevant legislation is implemented within the organization. RUC's information security policy establishes how we at RUC work with information security, defined as the use and management of systems, solutions, projects, data, information, and knowledge. Data, information and knowledge may exist digitally, in print as handwritten notes or in other physical forms.

The information security policy outlines our common main objectives, responsibilities, proper behavior, and measures, which are actions or tools we implement to prevent unauthorized access, interruption, or destruction. The policy describes RUC's overall approach to information security and constitutes the foundation for anchoring information security throughout the organization and to external partners.

Information security at RUC aims to support the university's core values, vision and strategic goals, enabling RUC to maintain its reputation as a recognized educational and research institution

1.1 Reading Guide

The purpose of the information security policy is to communicate both rights and obligations related to information security at RUC. The policy is detailed and specified in several guidelines, which can be found on Serviceportalen and the Moodle platform for students.

1.2 Main Objectives

The information security policy reflects RUC's current level of information security, based on external requirements and internal needs, particularly compliance with applicable legislation, regulatory requirements, and agreements, as well as protection against current threats and related risks.

RUC follows a risk-based approach to information security, utilizing a risk management model built on quality management principles as specified in the ISO 27001 standard, recommended by the common national security project.

1.2.1 Description of Main Objectives

The work with information security includes three main objectives that everyone at RUC should know and understand: confidentiality, integrity and availability.

Confidentiality ensures that information and knowledge are not made available or disclosed to unauthorized persons or processes. Confidentiality aims to ensure that information is visible and accessible only to those who own it or have a documented work- or study-related need and are authorized to access it.

Integrity ensures that information and knowledge are accurate and complete so that it is reliable and not altered incorrectly, whether intentionally or unintentionally.

Availability ensures that information and knowledge are accessible and usable upon request by an authorized person or process.

1.3 Scope

The information security policy applies both to activities (e.g. data processing), individuals, and assets (e.g. software and hardware). The three main objectives – confidentiality, integrity and availability – must always be formalized in agreements and contracts where relevant, such as with collaborators, partners or other entities.

The information security policy and current guidelines must always be respected and applied, for example, when purchasing, acquiring or disposing of assets or participating in activities involving data, information and knowledge.

1.3.1 Description of Scope for Activities, Individuals, and Assets

The information security policy applies to all of RUC's data- and information-related *activities*, regardless of whether these are carried out by RUC employees - including the departments and the library - or by collaborators, partners or other persons associated with RUC.

The policy therefore applies to *individuals*, defined as all employees and students at RUC, as well as collaborators, partners or other persons connected to RUC who perform tasks or are enrolled as students at RUC.

The policy encompasses all usage, maintenance, and installation related to RUC's data and informational assets. It also applies to all of RUC's own *assets* and assets that are linked, connected, or involve the storage or exchange of data with RUC or across RUC's organization.

2. Organization and Responsibility

The responsibility for the implementation of information security at RUC always rests with the university's senior management, the Rectorate. The Rectorate may delegate tasks to specific functional units, including the guidance and instruction of employees, students, collaborators, partners, and others to whom the information security policy applies. Current procedures are formulated and communicated by the respective data, information, or system owners and/or deans or departmental leadership, based on the information security policy and relevant guidelines and instructions.

2.1 Internal Organizational Application

The information security policy is activated and applied in RUC's ongoing organizational operations. Information security must be incorporated both at the *strategic*, *tactical*, and operational levels within RUC's organization, with continuous reporting to management levels on the extent to which information security standards, guidelines, and instructions are being followed.

2.1.1 Description of Strategic, Tactical and Operational Levels

At the *strategic* level, the Rectorate sets the overall direction for information security at RUC, defining RUC's specific need for information security. This is based on information security analyses, assessments, and evaluations conducted by the Chief Information Security Officer (CISO), the Data Protection Officer (DPO), and RUC's common IT department, which must possess the necessary expertise to carry out and provide guidance on this work.

At the *tactical* level, the CISO is responsible for formalizing and communicating policies, as well as analyzing, assessing, evaluating, and future-proofing RUC's information security. The CISO defines the overall direction for information security at RUC and translates it into guidelines and instructions to ensure the university's decided security level is achieved.

At the *operational* level, everyone managing a solution or system (e.g., system owners and administrators) that is utilized to store or process data, information, or knowledge is obligated to design and implement these solutions and systems in compliance with RUC's information security guidelines and instructions. It is also required that during the subsequent operation of, for example, a solution or a system, mechanisms must be in place to continuously verify that the solution or system adheres to RUC's current standards and guidelines for information security.

2.1.2 Description of Reporting and Compliance with Standards and Guidelines

The person in charge of the operation of a solution or a system (e.g., system owner or administrator) is responsible for continuously collecting and reporting results to the CISO regarding whether the solution or system complies with RUC's standards and guidelines for information security. The CISO is responsible for consolidating the reported results into a report that provides a comprehensive overview and supports periodic management reporting. The purpose of the periodic management reporting is to enable the Rectorate to act and prioritize addressing information security challenges across all of RUC.

2.2 Collaborators, Partners and Engagements

Anyone who handles data, information, or knowledge for RUC must comply with RUC's requirements for information security. This applies not only to employees and students at RUC but also to collaborators and partners (e.g. suppliers, guest researchers, etc.) and other individuals who are affiliated with or have a relationship with RUC.

2.2.1 Description of Collaborators, Partners and Engagements in Relation to Information Security

If data, information, and knowledge are stored or processed outside of RUC, for example with an external collaborator of partner, this collaborator or partner must be informed of and comply with the same information security requirements as those applied internally at RUC. Similarly, if employees, students, collaborators, partners or other individuals affiliated with RUC transport or use data, information, or knowledge outside of RUC, the information security requirements from RUC must still be followed.

3. User Behavior

Exhibiting good information security behavior is not just an expectation, but an obligation, regardless of whether you are an employee, student, collaborator, partner, or otherwise affiliated with RUC. At RUC, we therefore work according to a set of behavioral principles, which are also embedded in your relationship with RUC through, for example, your employment, enrollment, or your collaboration agreement or contract with RUC. RUC strives to provide the necessary facilities (e.g., secure storage of data, information, and knowledge) to a reasonable extent. For data, information, and knowledge with specific requirements or of significant scope, the responsibility for facilitation primarily lies with the data owner.

3.1 Behavioral Principles

It is assumed that all employees, students, collaborators, partners, or other individuals affiliated with RUC always act professionally and exhibit common sense. To support this, three overarching principles for user behavior are followed: *transparency*, *acceptance*, and *accountability*.

3.1.1 Description of Behavioral Principles for Information Security

Transparency is defined as RUC's commitment to creating an information security environment that is clearly documented and communicated in guidelines and instructions, which allows all of us to act digitally responsibly in our daily activities.

Acceptance means that with the opportunity to access RUC's data and information comes the responsibility to comply with the information security policies at RUC, which you must consider, understand, and accept.

Accountability describes how at RUC, you are responsible for your own actions, and if you become aware of an information security issue, it is your responsibility to respond and report the issue to the appropriate authority.

3.2 Employment, Enrollment, Agreement, and Contractual Relationships

Access to data or information at RUC is always based on a documented work or study-related need, which must be approved by both the immediate supervisor and the unit responsible for the given data or information. If the current information security rules are not followed, sanctions will be imposed in accordance with the current regulations at RUC.

3.2.1 Description of Work-Related Needs and Sanctions

It is always a requirement for a work or study-related need in order to gain or maintain access to data, information, or knowledge at RUC. A work or study-related need must be documented when the necessary and sufficient access rights are to be granted. Such access must also be continuously monitored if required. The immediate supervisor must continuously ensure that the access reflects the current need. Employees, students, collaborators, partners, or other individuals affiliated with RUC who violate the current information security rules at RUC may be subject to disciplinary sanctions. The relevant regulatory sanctions will be determined in accordance with the current personnel policy, contracts, and formal agreements at RUC, and apply to employees, students, collaborators, partners, and others affiliated with RUC.

4. Segregation of Duties

At RUC, we work proactively to protect our organization from both intended and unintended incidents such as misuse, unauthorized access, disruption, or destruction, as well as to protect you as an employee, student, collaborator, partner or any other individual affiliated with RUC from unjust suspicion of having committed intentional incidents. In this work, segregation of duties, where tasks and responsibilities are separated to prevent errors and misuse of, for example, access rights, is essential. Everyone at RUC who handles data or systems is responsible for ensuring that segregation of duties is implemented where necessary.

4.1 Description of Segregation of Duties

Segregation of duties is defined as you being unable or prohibited of approving or concealing your own actions in certain areas. The specific and current scope of segregation of duties at RUC must be justified and documented based on internal business or organizational needs or external requirements. RUC provides a website where you can find specific guidance on how to handle segregation of duties.

5. Classification of Information, Data, and Systems

All of RUC's information, data, and systems have varying degrees of value and must be classified to ensure they are processed, stored, and, if applicable, shared correctly in accordance with current rules, regulations and legislation. Everyone at RUC who works with or stores data or operates a system or solution is responsible for ensuring that data, information, and knowledge are correctly classified.

5.1 Description of Classification of Information, Data and Systems

Classification means that information, data, and systems are labeled based on their type. This includes, for example, whether the data involves processing confidential or sensitive information, and whether there are requirements for pseudonymization or anonymization before the information can be processed, or if the system requires special measures due to the type of data, information, or knowledge being processed. By classifying information, data, and systems, their value is made visible in a systematic way, allowing them to be protected to the necessary and adequate extent on a consistent basis. RUC provides a website where you can find specific guidance on how to handle the classification of data, information, knowledge, or systems.

6. Risk Assessment and Analysis

At RUC, we work with information security based on risk assessments, which means that we continuously and proactively identify, evaluate, and manage risks associated with the use of systems, solutions, projects, data, information, and knowledge. A risk assessment is a systematic process aimed at understanding the threats and vulnerabilities that could impact security, as well as the potential consequences of these. Everyone at RUC is responsible for conducting risk assessments for the systems, solutions, projects, data, information, and knowledge they manage or are in charge of.

6.1 Description of Risk Assessment and Analysis

The proactive identification, evaluation, and management of risks are carried out by conducting a risk assessment and analysis of specific systems, solutions, projects, data, information, or knowledge according to RUC's method and guidelines. The purpose of the risk assessment and analysis is to familiarize oneself with the current information security risks present, so that we can make effective and informed decisions about how to best protect our data, information, knowledge, and systems. RUC provides a website where you can find specific guidance on risk assessment, including a description of RUC's method.

Version History

Version	Dato
0.1	08.02.2024
0.2	09.08.2024
0.3	02.09.2024