Metropolia’s Information Security Policy

Table of Contents

Administrative information

Title: Metropolia's Information Security Policy
Version: Second edition
Validity date: 27 February, 2024
Owner(s): Metropolia's Management Group
Approver(s): Metropolia's Management Group
Classification: Public
Intended audience: Metropolia university community
Change history:

- First edition published on 13 June, 2022
- Second edition published on 25 March, 2024

Definitions

Information assets= Any information that has value for an organization and therefore requires protection. Information assets should be identified, considering that the information system consists of protectable functions, processes, and data.

Information asset owner = A person or entity responsible for data/information assets and determining their use for custodians and users. The information asset owner has the responsibility and authority to manage risks related to information assets, such as compliance with data protection legislation.

Custodian = Refers to all individuals responsible for the technical maintenance of ICT services, such as an IT administrator. Additionally, they handle system management tasks and provide support and guidance to users based on criteria defined by an information asset owner. Broadly comprehended, a custodian encompasses anyone with extensive rights compared to a normal user within ICT services and technologies, regardless of the purpose of the service, system, or technology. This definition also includes students who manage the university's ICT systems, services, or technology as privileged users, similar to the employees of the university's IT Services.

User = Means an individual who possesses a Metropolia account and has access to information assets by the principles determined by the information asset owner. Custodians are responsible for granting user permissions, for example, as an IT administrative user.

Information security = Procedures, ensuring the availability, integrity and confidentiality of information.

Minor information security incident= An event related to the activities of an information system or organization, resulting in a change in the state of data or services, which may impact security. Minor security incidents do not trigger business continuity and (disaster) recovery plans. Examples of this incident category entails, among other things, attempted denial-of-service attacks, neglect of personal security practices, failure to update hardware security patches, and violations of access control rules.

Major information security incident = One or more related unexpected or undesirable security events that jeopardize the security of data and services and adversely affect the organization's business. Serious security incidents activate business continuity and recovery plans by ICT systems and technology. This security incident class encompasses, for instance, denial-of-service attacks, ransomware, severe weather conditions, power outages, data breaches involving sensitive information, disruptions in the supply chain, stolen credit card data, and endangerment of human life due to data asset malfunction.

Data lifecycle planning = Information systems and assets regard to the data's complete life circuit. During this lifecycle, assets are established, defined, planned, developed, tested, and implemented. They are then used, maintained, and eventually retired and securely obliterated. Security considerations should be examined at all storage and stages of information, including data in transit.

Data privacy breach = Unauthorized interference with personal data, resulting in data destruction, loss, alteration, unauthorized disclosure, or access by an entity without processing and viewing permissions. Privacy violations can lead to loss of control over personal data, identity theft, fraud, damage to reputation, or exposure of pseudonymized or confidential personal information.

Topic

Metropolia's information security policy is a continuously maintained and updated framework that includes a streamlined policy based on the core needs of the university (as outlined in this document), accompanied by associated guidelines and diagrams. The information security policy is derived from Metropolia's general risk management policy, which is approved by the Board of Directors by the university. This document defines how (information) security matters are implemented within Metropolia, combined with outlining the roles and responsibilities related to security (Annex 1). The policy is guided by Metropolia's strategy, IT strategy, legislation, guides, and standards (Annex 2). Through the information security policy, Metropolia promotes desired security behaviour when interacting with the university, ensuring that both Metropolia staff and students in addition to the university's cooperation partners adhere to the principles described in the policy. The policy reflects the vision of Metropolia's Management Group for cybersecurity management and its management system, explained in the Scope Statement of Cybersecurity Management System by the Metropolia University of Applied Sciences.

Objectives

In information security management, the responsibility as well as commitment of senior management are highlighted. It is crucial for the leadership to have a clear awareness of the role of security for the university's vital functions, while simultaneously ensuring that the adopted IT strategy is sufficiently business oriented as per the needs of the university. Via the information security policy, Metropolia's Management Group expresses its intentions and perspectives on information security. Metropolia's business more and more depends on information technology throughout the entire organization. Vital functions at Metropolia include student education, research, development and innovation (RDI), and business undertakings. As part of Metropolia's IT strategy, creating a security-oriented awareness culture is a top priority. Data asset lifecycle planning ensures proper use and security of assets throughout their usage phases. Concretely, security activities are implemented through training, guidelines, alongside hardware and software acquisitions. Metropolia's chosen security controls encompass technical, organizational, physical, and people-related methods. As a higher-education institution, Metropolia bears the liability of keeping updated the security competence of its staff and students. Looking after own digital security is becoming an essential civic skill that affects every member of Metropolia. Metropolia aims for a proactive risk management approach in security, where the university's risk appetite is low at the organizational level. Spell out clearly, Metropolia maintains a low-risk appetite concerning legal compliance, safety and security. Digital security risk management incorporates identifying, assessing, and addressing risks in proportion to security management model and its policy approved and endorsed by Metropolia's Management Group together with the Board of Directors. Data handling is based on recognizing the nature of information and assessing risks, while adhering to legal requirements. The development of Metropolia's cybersecurity management system for safeguarding information assets is lead by the information security policy, security principles, and risk assessments.

Responsibilities

Students, staff, partners, and stakeholders are accountable for compliance with the security rules. Additionally, every student and staff member must report any observed security risks, deviations, or hazardous situations, such as serious security incidents, to their supervisor or the IT Services. It is the liability of each employee and student to complete Metropolia's basic-level information security training. Regular security training is provided to both students and staff. Information asset owners possess authority for their assets and their use. Custodians, such as IT administrators, manage information assets under the

criteria set by the information asset owner, including controlling access rights. Users are obligated to work with information assets by following the security rules defined by the asset owner. The IT Service fosters the positive development of information security throughout the Metropolia university.

Communication

When public communication is needed, it is decided by Metropolia's Management Group in cooperations with the Communication and Marketing department. Internal communication in respect of information security is managed by the IT Services. Information about maintenance work is provided on the IT Services' Wiki page and as needed, via targeted announcements on the OMA intranet. The custodian of a service or information system is accountable for communicating any service-specific features to the IT Services.

Review, consequences and compliance

An IT violation is considered any action that breaks Metropolia's rules regarding the use of ICT services, security principles, or any activity that is contrary to Finnish laws. Within the IT Services, the security-related principles and guidelines are reviewed yearly. These principles and guidelines are updated regularly as necessary. External parties are commissioned to conduct security assessments and audits if demanded. This document is reviewed and updated as necessitated, typically once a year. The liability for reviewing the security policy belongs to the Chief Information Officer, CIO, who has the authority to make minor adjustments to the policy's content when required. If the security policy or its content deviates significantly, for example, due to the university's new strategy, the updated security policy must receive approval from the Management Group. The CIO, reports on the security situation to the senior management on normal circumstances and planning, as well as whenever necessary, such as in the case of a serious information security incident.

Annex 1: Information security roles in the Metropolia university

Role	Responsibilities
The Board of Directors	1. Responds to appropriate organization of risk management in conformity with operational principles of the university risk management. 2. Addresses major risks and uncertainties in respect of the university's business and teaching.
Management Group	1. Perceives the component of information security to the university's vital functions as well as its part for broader security. 2. Guarantees that Metropolia has an up-to-date information security policy. 3. Helps the President in university's risk management together with other security matters. 4. Acts the highest risk management element at Metropolia. 5. Has an accountability to recognise strategic risks and utilize topical risk information in day-to-day functions and management.
Chief information officer, CIO	1. Has the authority to lead the IT Services of the university as part of Metropolia's activities, with focus on the requirements of the university's business and ICT service users. 2. Monitors the ICT processes and their progress in addition to the strategic management and organizing of the ICT service production. 3. Executes comprehensive development, direction, review, and the leadership of university's information security. 4. Determines the IT Strategy for Metropolia.
Leaders, directors, chiefs, managers and forepersons	1. Liable for digital risks and their management in their organizational limits, e.g., their department, unit, responsibility area etc. 2. Report and inform the IT Services about information risks that need controls for their treatment.

Project owners, project managers, team leaders, and other controllers of research and data material.	1. Handel information security and data risk management as part of a leader of a project or team. The controller of research and data material is accountable for the proper implementation of information security in their work. Risk management for projects, initiatives, and workgroups specifically involves identifying, analyzing, treating, and reporting data-related risks regarding to carrying out work and achieving goals.
User support (HelpDesk)	1. In charge of the acquisition and installation of computers and mobile devices, as well as software maintenance, installation, and personnel instruction.
System maintenance	1. Accountable for the functioning and development of IT infrastructure, with primary focus on Windows and Linux server environments, data centres and machine rooms.
ICT systems development	1. Develops, acquires, and implements information systems that support common processes. 2. Manage the accuracy and timeliness of information in the systems.
Information security specialist(s)	1. Maintaining the cybersecurity management system and implementing information security within Metropolia's business operations. Simultaneously, they are responsible for training staff, providing guidance, maintaining guidelines, and handling serious information security incidents. 2. Monitoring the state of information risk management, coordinating information risk management, and ensuring procedural consistency. They are a professional in cybersecurity management systems, creating, implementing, maintaining, and continuously improving one or more processes within the management model.

Data Protection Officer, DPO	1. Is the point of contact for the entire Metropolia organization regarding advice, development, and monitoring of data protection work in accordance with legislation. 2. Provides guidance on DPIA matters. The Data Protection Officer serves as the organization's liaison for data protection matters with the Office of the Data Protection Ombudsman. 3. Reports serious data protection and information security incidents from Metropolia to the Office of the Data Protection Ombudsman (acting as the intermediary between the Ombudsman and data subjects).
Risk management manager	1. Is charge of risk management, occupational safety, and comprehensive security management in the university.
HR Services	1. Handles employment matters, organizes personnel training, and facilitates the orientation of new employees.
Personnel and students	1. Adhere to Metropolia's rules for using information systems, guidelines, and information security principles. 2. Report possible data risks or exceptional situations to the IT Services.
Consultants, service companies, and partner organizations.	1. Follow Metropolia's rules for using information systems, guidelines, information security principles, and best practices in information security. 2. Monitor and maintain the desired level of information security when dealing with Metropolia. 3. Report information security matters and related factors to the IT Services. 4. Comply with contractual obligations set by the client.

Annex 2: Documents directing Metropolia's information security enforcement

Legislation

- The legislation governing higher education is detailed on the Metropolia University of Applied Sciences' IT Service Wiki page.

Standards

- *ISO 27001:2022: Information security, cybersecurity, and data protection. Information security management systems. Requirements.*
- *ISO 27002:2022: Information security, cybersecurity, and data protection. Information security controls.*
- *ISO 27005:2022: Information security, cybersecurity, and data protection. Guidelines for managing information security risks.*
- *The NIST Cybersecurity Framework*
- *ISO 31000:2018: Risk management. Guidelines.*
- *ISO 22313:2020: Security and resilience. Business continuity management systems. Guidance for using ISO 22301 standard.*

Guidelines

- The Finland Security Committee's *Vocabulary of Cyber security* (only available in Finnish)
- Instructions and manuals for cybersecurity professionals from the National Cyber Security Center.

Strategies

- Metropolia's Strategy 2021 - 2030: A bold reformer of expertise and an active builder of sustainable future
- The IT Services own IT strategy and focus areas.