The Scope Statement of Cybersecurity Management System by Metropolia University of Applied Sciences

Table of Contents

Administrative Information

Title: The Scope Statement of Cybersecurity Management System by Metropolia University of Applied Sciences
Version: First 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 25 March, 2024

The Scope Statement of Cybersecurity Management System by Metropolia University of Applied Sciences
Scope Statement

25/03/2024

Definitions

Availability = Property of being accessible and usable on demand by an authorized entity

Confidentiality = Property that information is not made available or disclosed to unauthorized individuals, entities or processes

Integrity = Property of accuracy and completeness

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 security = Arrangements aimed at ensuring the availability, integrity, and confidentiality of information assets.

Cybersecurity management system; information management system = The cybersecurity management model consists of principles, procedures, guidelines, and related resources and functions that the organization collectively manages to protect its information assets

Cybersecurity management professional = Person who establishes, implements, maintains, and continuously improves one or more cybersecurity management system processes.

Documented information = information required to be controlled and maintained by an organization and the medium which it is contained.

Scope statement; The scope of cybersecurity management system = The organization must decide on the boundaries and application of the information security management system in order to define the system's scope. The scope statement describes, among other things, the organization and its business environment, the needs and expectations of stakeholders, and the organization's dependencies in relation to other actors. The scope must be documented information.

Cybersecurity governance = Management perspective by which an organization's cybersecurity measures are directed and supervised. Cybersecurity governance guides the cybersecurity management system.

Continual improvement = The aim of continual improvement of cybersecurity management system is to increase the probability of achieving objectives concerning the preservation of the confidentiality, availability and integrity of information. The focus of continual improvement is seeking opportunities for improvement and not assuming that existing management activities are good enough or as good as they can. The cybersecurity management system is improved by following the quality management principles, such as Plan, Do, Check and Act, a PDCA cycle, of the university.

The Purpose of the document

Metropolia University of Applied Sciences develops its information security in accordance with the cybersecurity management system. The purpose of this document is to document the scope of the university's cybersecurity management system, as specified in the scope statement (this document). The cybersecurity management system is a systematic approach to creating, implementing, using, monitoring, reviewing, maintaining, and improving Metropolia's information security, all aligned with the objectives set by the university. The current management model is based on risk assessment and the university's acceptance levels for risks, designed for effective risk handling and management. By analyzing information asset protection requirements and implementing suitable technological, organizational, people, and physical control measures, successful implementation of the information security management model (ISMS) can be achieved. The scope statement is particularly aimed at external stakeholders who evaluate Metropolia's level of information security and its processes.

The Scope of Cybersecurity Management System

Within the scope

The whole Metropolia community, including university staff and students, fall within the scope of this document. The cybersecurity managements system extends to cover the entire university, including all innovation hubs, schools, and other administrative domains necessary for the university's daily business. The principles of the management model apply across all university information services. The implementation of the cybersecurity management system belongs to the purview of the IT Services. Here, the university's IT management makes decisions regarding the university's cybersecurity solutions and management approaches. The IT management consults with information security specialists and those knowledgeable about security, who serve as cybersecurity management professionals in the ISMS. Regular communication from the IT management to the top management, the Management Group by the University—preferably twice a year—drives the development of the cybersecurity management system in line with continuous improvement in information security. The Management Group also serves as the high-level steering group for the ISMS. In this way, the cybersecurity management system enables Metropolia's business-oriented practices while adhering to robust security governance.

Out of the scope

The Metropolia University of Applied Sciences does not directly apply its cybersecurity management system to the information security practices of its stakeholders. However, Metropolia provides guidance on how it expects stakeholders to behave in matters related to security, such as adhering to the principles outlined in Metropolia's information security policy.

Metropolia's stakeholders

The key stakeholders of Metropolia include the Metropolia Student Union (METKA), collaborating educational institutions, authorities, software vendors, research and development partners, and business partners.

University's geographical location

Metropolia University of Applied Science locates at the Helsinki capital region of southern Finland, where the university has four campuses in three cities: Arabia Campus and Myllypuro Campus in Helsinki, Karamalmi Campus in Espoo, and Myyrmäki Campus in Vantaa.

Cybersecurity management system's information security objectives

The term *information* security is generally based on the idea that information is considered an asset, valuable and hence, requiring appropriate protection. This protection includes safeguarding against loss of information's availability, confidentiality and integrity. Making accurate and complete information available to those who need it enhances business efficiency. The principles of Metropolia's cybersecurity management system are drawn from the broader strategy and values of Metropolia, its Code of Conduct, and the needs of its IT Services' clients. Essentially, the ISMS is accomplished along with Metropolia's IT strategy on which the university's information security and IT activities are implemented. This includes executing the management controls outlined in the cybersecurity management system and the distinct security procedures set for each year. Above all, through ISMS, the university's IT Services aims to understandably communicate the security practises set by the cybersecurity management system.

Monitoring and review

The scope statement is reviewed annually with the Chief Information Officer (CIO) in a manner similar to the information security policy. The document is updated if Metropolia's high-level strategy or the objectives of the IT strategy significantly change. A new statement for the cybersecurity management system, where its security controls should be applied, must be approved by Metropolia's Management Group. Writing a new statement inclines to the responsibility of Metropolia's information security specialist and the IT management.

Annex 1: Responsibilities of cybersecurity management and its governance

Responsible party	Responsibilities
The Board of Directors	Ensures the appropriate organization of risk management in accordance with Metropolia's current risk management policy. Additionally, the board approves the organization's risk management policy and any related changes, as well as addresses significant risks and uncertainties related to the organization's business.
Management Group	Serves as the High-level steering group for the cybersecurity management system and guides the objectives of information security management. The Management Group demonstrates commitment to the needs of the cybersecurity management system, such as regularly reviewing its business matters. Additionally, the Management Group supports the President, CEO, in decision-making, defines broader risk management issues relevant to the entire Metropolia, and makes critical decisions regarding significant or central risk management measures and actions. This includes determining responsibilities, timelines, resources, and follow-up related to these measures.
The Implementation Group of Cybersecurity Management Systems	Executes the ISMS according to the objectives of the cybersecurity management system. The duty for implementing the management model lies with the IT Services, where the primary responsibility rests with the IT management and the cybersecurity management professionals, such as the information security specialist.
IT Management	The IT management is liable for defining the objectives and management measures of the cybersecurity management system. It within the IT Services enforces the overall fulfilment of the cybersecurity management system.

Annex 2: Cybersecurity management system's security areas and responsibilities

Security area	Responsible party
Physical controls	Facilities Management Services is responsible for the physical security aspects of the cybersecurity management system. Risk Management Services and IT Services play an advisory role in implementing physical and people controls.
People controls	HR Services is charge with the people controls of the cybersecurity management system. Risk Management Services and IT Services have a consultative function regarding physical and people controls.
Technological controls	IT Services carries out the technological controls of the cybersecurity management system. Besides, IT Services enforces technical-related aspect to overall digital security.
Organizational controls	IT Services, Risk Management Services, and Metropolia's Management Group have a collaborative role for the organizational and administrative controls concerning information security. With organizational controls, they address the methods by which cybersecurity management system integrates into the entire organization's functions. The criteria for this aspect of the security, aims to ensure that the university has a well-functioning cybersecurity management system and procedures to make sure that personnel and students handling information act appropriately.
Preparedness, disaster recovery and business continuity	As needed, coordination groups can be formed on a case-by-case basis to lead risk management for a specific temporally or functionally limited matter. The chairperson of such a coordination group is the President of the university or their appointed representative. In normal circumstances, IT Services develops preparedness and continuity procedures for information security along with Metropolia's cybersecurity management system. Key criteria in this area include preparedness measures for various serious disruption scenarios, business continuity plans, and information system recovery plans together with their practice.

	Continuity management is closely related to the management processes for normal disruptions, security incidents and emergency situations.
Privacy protection	IT Services is a charge of implementation of data protection within the university's ICT services as well as technology. Legal and Archive Services in addition to Metropolia's Data Protection Officer, act as a consultative role in data protection.
Risk management	Safety and security risks are assessed and analysed at Metropolia as per to the risk management system in use. If needed, individual risk assessments will be performed. Risk Management Services is liable for the university's broader risk management. In terms of cyber and information security risks, IT Services possesses a consulting element.