Policy for Cybersecurity culture and training

Type of document	Topic specific policy
Managed by	Head of HR and HSE Division
Approved by	Director of Organization and Infrastructure
Applies from	12.06.2023
Next revision by	12.06.2025
Classification	Open
Reference ISO	ISO 27002:2022; 6.3
Reference LOV/Rule	The work environment act § 4-2
Reference intern documents	Policy of Information Security

1. Purpose

The purpose of this policy is to define responsibilities, target groups, and arenas for activities related to targeted training, competence-enhancing measures, and the development of awareness regarding information security within the organizational culture. An organizational culture entails a cybersecurity culture where collectively ingrained values and norms influence employees' thoughts and expectations regarding security.

2. Applies to

The policy applies to all individuals who have access to, process, and manage information through NTNU's ICT infrastructure.

3. Key Principles

a. As a guiding framework for working with cybersecurity culture and training at NTNU, the current action plan for information security in the state administration is always considered. The current action plan describes *knowledge, competence, and culture* as a separate area of action.
b. The work with cybersecurity culture and training should also be based on NTNU's overall risk profile for societal security, where information security is identified as a distinct risk area.
c. The work with cybersecurity culture and training should be a systematic and continuous improvement process.
d. The content of all development work and training should support the main message that information security is about the interaction between people and information systems.
e. All training should contribute to increasing risk understanding and strengthening the ability and willingness to act correctly.

4. Cybersecurity Culture and Training

The goal of working with cybersecurity culture and training is to achieve NTNU's established information security goals. Achieving these goals involves a systematic and continuous improvement process where risk management and embedded information security are maintained

through leaders' and employees' active risk awareness and understanding. Embedded information security is a fundamental principle in information security work and is achieved when information security is:

a. Incorporated into organizational management and supports the organization's goals
b. Incorporated into the organization's processes and projects from the start
c. Considered throughout the life cycle of ICT solutions
d. A topic that all employees are aware of and understand its implications for their tasks

The phases in the improvement process consist of planning, implementation, evaluation, and revision. This work should primarily be developed and managed centrally, in line with other quality and development work at NTNU. Line management is responsible for participating in the development and training measures made available. Line management is also responsible for following up on particularly risky areas within their unit through targeted local training measures. The content of the training should be based on the identified information security requirements for the classified information elements in the relevant systems, services, and processes for the targeted groups of the different training modules.

4.1. Cybersecurity Climate

Cybersecurity climate refers to the visible emphasis on security. Cybersecurity climate includes aspects such as the leader's prioritization of security, emphasis on security systems, and the degree of risk tolerance. It is also used to monitor and control one's own security.

Leaders must assist in identifying areas for necessary training and competency-building measures to create a continuous process of developing the unit's cybersecurity culture through systematic assessment of the cybersecurity climate. The cybersecurity climate should be reported to the controlling part of the management system.

4.2. Action Plan

Based on the risk profile and analysis of NTNU's security climate, a central action plan should be established at the organizational level for working with security culture and training in a multi-year perspective. The action plan should have clear effect and result objectives for the entire NTNU. The action plan must include a training plan and communication plan for the relevant period. The action plan must be reported to the controlling part of the management system.

4.3. Training Plan

The training plan must include target group-oriented, module-based training offerings for all employees, with measurable operationalization of how the objectives in the action plan will be achieved. Over time, the training plan must cover the three categories of measures defined in the superior Information Security Policy:

a. Implementation of risk management by leaders in the units
b. Development of cybersecurity culture, competence, and attitudes
c. Development of a robust infrastructure that ensures digital security

The training modules and courses should also be integrated into NTNU's other training programmes for leaders and employees.

4.4. Communication Plan

The communication plan must in its strategic objective and structure, follow a communication model that, over time, contributes to:

a. Awareness and attention to information security

b. Desire to support and participate in the change process
c. Knowledge of how to secure NTNU's information assets
d. Ability to receive new knowledge and use new working methods
e. Anchoring new practices and ensuring compliance

The communication that follows the training plan must be aligned with increased risk understanding and maturity regarding the training content. This is to ensure that the communication supports and reinforces the training being conducted and to ensure that employees within the services and processes covered by the management system perceive a connection between available information and training.

For all target groups, information and communication about information security must primarily happen on established meeting arenas and channels. Additionally, tailored and target group-specific information will be produced on Innsida, faculty channels, administrative department channels, as well as written information used as supplements when needed.

4.5. Evaluation

The content, operationalization, and goal achievement of the action plan must be evaluated at the end of the period. Learning points will be incorporated into the design of subsequent training plans and communication plans to ensure continuous improvement and targeted development. The evaluation will be reported to the controlling part of the management system.

5. Roles and Responsibilities

5.1. Director of Organization and Infrastructure

a. Ensures the development of action plans that facilitate systematic and continuous work with cybersecurity culture and training in information security

5.2. Head of HR and HSE Division

a. Responsible for organizational development and change management in information security, including ensuring that leaders are aware of and have sufficient competence and risk understanding to fulfil their responsibility in practising risk management in information security
b. Responsible for assessing the cybersecurity climate by conducting surveys among leaders, with a frequency of every other year
c. Responsible for developing an overall action plan for working with security culture and training, along with corresponding training and communication plans for leaders and other employees
d. Responsible for evaluating the work on cybersecurity culture and training, ensuring that information and training in security are consistent, aligned with overarching principles, and cover relevant work processes
e. Responsible for that the work on cybersecurity culture and training are following up on focus areas from management reviews and other control activities
f. Responsible for reporting on the implementation progress, effectiveness, and efficiency of training and awareness efforts

5.3. Dean/Head of Department/Line Manager

a. Responsible for ensuring that employees in the unit have sufficient training in information security and can fulfil their obligation to assess risks in new projects and all information processing, as well as report and handle deviations from information security

5.4. Head of HSE and Emergency Preparedness Section

a. Must be consulted in the planning of continuity and emergency preparedness work to ensure that the work is conducted in accordance with the Policy for Emergency Preparedness

5.5. Head of Digital Security Section

a. Must be consulted in the development of communication and training materials to ensure professionally relevant content and updated risk and threat assessments.

5.6. System Owner

a. Responsible for developing and communicating training materials related to the use of ICT systems in accordance with the applicable policies.