Approved by order No 126 of 3 June 2024 of the Director for Administration

In force from: 03.06.2024

Procedure for Managing Security Vulnerabilities

Table of Contents

1 General information

The purpose of the Procedure for Managing Security Vulnerabilities is to establish the policy and control measures for assessing and managing technical vulnerabilities in the information systems and IT assets of Tallinn University of Technology (hereinafter referred to as “the university”), with the aim of maintaining a risk rating accepted by the university.

2 Scope of application

The Policy applies to all information systems, IT assets, processes, and stakeholders within the scope of application of the university’s information security management system.

3 Management of security vulnerabilities

A prerequisite for managing security vulnerabilities is maintaining a registry of information systems and IT assets. The vulnerability management process includes asset accounting, vulnerability identification, assessment, prioritisation, mitigation, remediation and testing.

4 Identification of security vulnerabilities

Automated vulnerability detection tools are used to scan information systems and IT assets in order detect security vulnerabilities. The Chief Information Security Officer, in collaboration with the Information Security Division of the Information Technology Services, is responsible for identifying security vulnerabilities.
The technological solutions employed by the Information Security Division to detect vulnerabilities have been accounted for as assets, and the sources of vulnerability information have been indicated.
In addition, the university’s information systems and IT assets are scanned by the Information System Authority (CERT.EE), which notifies the Information Security Division of any potential vulnerabilities.

5 Assessment and prioritization of security vulnerabilities

Detected vulnerabilities are assessed using standard vulnerability assessment methodologies (CVE, CVSS, OVAL, SCAP, VMF, PVG, etc.). The assessments are partially automated, depending on the IT tools used. Based on the assessment results, the Information Security Division determines the priority (risk rating) of vulnerabilities, including the timeframe for implementing mitigation measures (Table 1 Vulnerability risk ratings and response time).
The Information Security Division shall inform the business project manager and the and the system administrator of the information system or the owner of the IT asset of the detected security vulnerability and its risk rating as soon as possible after detection, but no later than within three working days.
Table 1 Vulnerability risk ratings and response time

Vulnerability risk rating	Response time
Critical	Less than 3 days
High	Less than 7 days
Medium	90 days
Low	180 days

6 Mitigation and remediation of security vulnerabilities

The system administrator is responsible for mitigating and remedying security vulnerabilities in an information system or IT asset. If a system administrator has not been appointed, the information system owner or the business project manager shall be responsible for remediation.

When critical and high-risk vulnerabilities have been detected and notified of, mitigation measures must be implemented promptly, but no later than the designated response deadline, to address the associated risk. If a security patch or update is available, it should be applied to mitigate or remedy the vulnerability. If an update cannot be installed due to technical constraints or if the manufacturer has not released an appropriate patch, the following mitigation measures should be implemented:

- Disable the information system or IT asset affected by the vulnerability;
- Restrict network access to the information system or IT asset;
- Protect vulnerable information systems or IT assets using suitable traffic filters.

- Apply other appropriate measures to mitigate the risk.

To remedy security vulnerabilities, updates from trusted sources should be used, with their performance assessed and tested prior to deployment.

For medium- and low-risk vulnerabilities, mitigation measures should be implemented no later than the specified response deadline. If possible, measures should be applied within this period to permanently remedy the security vulnerability.

If the information system administrator, business project manager, or IT asset owner fails to apply mitigation measures for critical or high-risk vulnerabilities within the prescribed timeframe after notification, the Chief Information Security Officer or persons authorised by the Chief Information Security Officer are entitled to apply the measures. This may result in the loss of availability of the information system or IT asset. In such cases, the Information Security Division shall not be held liable for any consequential damages.

If the information system administrator, business project manager, or IT asset owner has applied mitigation measures or remedied a security vulnerability, the Information Security Division must be notified thereof in writing. The Information Security Division then conducts a follow-up assessment to ensure that the vulnerability has been remedied or mitigated.

7 Testing

Regular security and penetration tests, conducted at least once a year on critical system components or by trusted external partners following significant changes, are an integral part of benchmark performance in security vulnerability management. Based on the test results, mitigation measures shall be applied, and security vulnerabilities shall be remedied based on the vulnerability risk rating.

8 Exceptions

In certain instances, exceptions to the vulnerability management procedure may be required due to technical constraints or contractual obligations of third parties. Such exceptions must be documented in writing and approved by the Chief Information Security Officer.

9 Supervision

Supervision of the implementation of the Security Vulnerability Management Procedure shall be conducted by the Internal Audit Office in accordance with its work plan, but not less frequently than once every three years.