Procedure number: 09-0301 Effective from: 06.10.11 Edition: 3 Last update date: 20.11.24 **Page 1 of 5**	**The Technion** **Israel Institute of Technology** **Procedures** **Information security procedure**

1. Background

Information security at the Technion is designed to prevent, as much as possible, harm to information, its databases, and the computing systems of the Technion, thereby reducing the risk of disruption to its regular operations. Additionally, it aims to raise awareness and personal responsibility among the various populations within the Technion.

Information security requirements will be determined according to legal and standard regulations on the subject.

2. Purpose

This document defines the Technion's policy regarding information security and the proper use of its computing resources.

3. Definitions

3.1. **Information** - Data, symbols, concepts, or instructions, excluding software, stored on a computer or other storage media (external disk, portable disk, etc.).

3.2. **Department Information Owner** - The manager to whom the information belongs within the department. It is important to emphasize that the information owner is not necessarily the manager in the technological sense or the one holding the information technologically.

3.3. **Confidentiality** - Ensuring that information is accessible only to authorized parties.

3.4. **Integrity** - Preserving the accuracy and completeness of information and processing methods.

3.5. **Availability** - Ensuring that authorized users can access information and resources as needed.

3.6. **Information Security** - Maintaining the confidentiality, integrity, and availability of information.

3.7. **Information Security Forum** - A forum that includes faculty computing engineers appointed by the Technion management, staff from the Computing and Information Systems Division, and the CISO. Its purpose is to raise relevant issues, problems, and various information security requirements at the Technion and to provide recommendations, guidelines, and/or operational solutions.

3.8. **Information Security Officer (CISO)** - A professional guide leading the field of information security at the Technion, implementing and initiating ways to realize management decisions on the subject.

3.9. **Information Security Trustee** - The department representative for information security matters.

3.10. **Entire Technion** - The Technion - Israel Institute of Technology and the Technion Research and Development Foundation Ltd.

3.11. **Employees** - Researchers, trainees, students, employees of the Entire Technion, contract workers, visitors, and anyone present within the Entire Technion.

3.12. **Guest System** - A computerized system that connects to the Technion's computing infrastructure and is not under Technion responsibility.

3.13. **User** - Anyone who uses the Technion's computing resources.

3.14. **Information Security Risk Survey** - A process that provides an up-to-date overview reflecting the state of information security in the organization's computing infrastructure.

3.15. **Technion Cyber Concept Document** - A document that holistically reviews the Technion's cyber concept and includes an analysis of risk factors, defense architecture, and the various solutions that together are supposed to protect the Technion. This document is confidential.

4. Authority and Responsibility

4.1. Technion Management

4.1.1. The Technion management is responsible for promoting information security within the Entire Technion.

4.1.2. Department heads bear overall responsibility for implementing information security procedures within their areas of authority, ensuring appropriate conduct of department personnel regarding information security, and handling information security incidents in collaboration with the department's Information Security Trustee and the Technion's Information Security Officer.

4.1.3. A department head will designate an Information Security Trustee who will be responsible for the information security of all computerized assets (hardware, software, applications, or data) within their department.

4.2. Information Security Officer (CISO)

4.2.1. The CISO is responsible for establishing the information security infrastructure at the Technion and for the existence of standards, procedures, and technical guidelines to support this process.

4.2.2. The CISO will initiate continuous monitoring and inspection activities to ensure the security of the Technion's computing systems.

4.2.3. The CISO is responsible for providing advice and guidance to Information Security Trustees, faculty engineers, and all users of the Technion's computing systems.

4.3. Information Security Trustee

4.3.1. Inform all computing users within their department about the information security procedures as published or conveyed to them by the Technion's CISO.

4.3.2. Address computing systems where information security breaches are found, either directly or by forwarding the handling to relevant parties within their department.

4.3.3. Notify the Technion's CISO of any information security incident within their department and handle it according to the instructions received.

4.4. Users

Every user is personally responsible for all the information in their possession, including that which is sent or transferred to them. Additionally, the responsibility to adhere to the Technion's information security guidelines and policies rests on every user in the organization.

4.5. Information Security Forum

The forum is responsible for providing recommendations, solutions, and various tools to improve information security at the Technion.

5. Method

5.1. Awareness and Training in Information Security

5.1.1. The CISO, in collaboration with the Human Resources Division, will develop training and refresher programs on information security topics for the entire Technion population.

5.1.2. Information security training will be included in the onboarding process of new employees at the Technion.

5.2. Physical Security

The Technion's CISO, in cooperation with the Security Officer, will guide the Information Security Trustees in the various departments on all matters related to physical security.

5.3. Information Security Incident Management

Information security incidents detected by Technion entities or others will be reported to the CISO (ciso@technion.ac.il) and managed according to the Information Security Incident Response Procedure.

5.4. Audit Trail

Tools and/or mechanisms will be implemented to monitor changes in systems, information, or software, detailing the activities performed and the time of execution.

5.5. Implementation and Development of Servies and Technologies

At the beginning of any process involving the development of new services, supporting systems, the introduction of new systems, or changes to existing services in the field of information services, the Technion's CISO must be involved.

5.6. Control

5.6.1. Technion CISO

5.6.1.1. Will ensure the execution of an Information Security Risk Survey for central computing systems at the Technion by an external entity. The survey will be conducted on at least two different systems each year. The survey findings will be forwarded to the Technion management, and based on them, controls and processes will be determined to reduce risks.

5.6.1.2. Will initiate internal inspections in departments/elsewhere within the Entire Technion to detect information security breaches in the Technion's information systems and will act to correct any deficiencies discovered.

5.6.1.3. Will maintain the Technion Cyber Concept Document. The document will be accessible to members of the Steering Committee, senior management members, Computing Division management, and Information Security Trustees. The document will be discussed every two years in the Steering Committee and the Information Security Trustees Forum and updated accordingly.

5.6.2. Department Information Owner

Will validate, every two years, the access permissions to information granted to various role holders within their department and, if necessary, outside the department.

5.7. Resource Allocation

Resource allocation in the field of information security will constitute an integral part of the Technion's overall operational budget and will be incorporated as a fixed component in relevant annual and multi-annual plans.

The annual and multi-annual budget assessment at the Technion will be carried out by the Head of the Computing and Information Systems Division based on the following parameters:

5.7.1. The need to implement information security as detailed in the information security procedures.

5.7.2. The changing information security needs at Technion considering the significant technological dynamism in the computing field.

5.7.3. An assessment of changing risks according to circumstances and a different prioritization of treatment as a result.

5.8. Enforcement

Anyone using computing equipment/information owned and/or under the responsibility of the Technion must act according to this policy. This policy is an integral part of the Technion's policies. Violation of this policy will result in the revocation of access and/or disciplinary and/or civil action according to the law.

6. **Applicability and Validity**

6.1. This procedure applies to:

6.1.1. Employees of all departments within the Entire Technion (including the Technion Research and Development Foundation Ltd.) or users of guest systems.

6.1.2. This procedure is effective from the date of its publication.

Prof. Boaz Golany
Executive Vice President and Director General