IT Security Policy of the Max Planck Society

The German version of this document "IT-Sicherheitsleitlinie der Max-Planck-Gesellschaft" has been passed by the Executive Committee on 21.06.2017

Preamble

The Max Planck Society depends on information and communication technology that functions reliably for the fulfillment of its tasks. Furthermore, scientific research requires a high degree of data safety and integrity that correspond to the respective areas of research. It is, therefore, essential to implement comprehensive controls for the protection of infrastructure and data.

The secure handling of data is of the utmost importance for the Max Planck Society, making IT security a foremost objective for the protection of the Society's infrastructures and data.

This document defines the IT Security Policy for the Max Planck Society. It constitutes the basis for IT Security Guidelines and subsequent resulting measures for the continual improvement and long-term maintenance of security in the area of information and communication technology (IT).

The spectrum of IT applications in the Max Planck Society includes scientific applications and simulations, the performance of tests and experiments, the presentation of scientific results, office applications, administrative work, the control and operation of technical systems, and communication with both internal and external partners.

The diversity of the fields of research, one of the significant characteristics of the Max Planck Society, is mirrored in these fields' methods and equipment and in the protection requirements of their facilities, which strongly influences the requirements on the respective IT infrastructures. As a result, the effects of disruptions or outages in the various application areas also vary in scope. The same applies for IT security controls and measures.

Objectives

The Max Planck Society protects its interests and its public reputation by securing its working capacity, trustworthiness and reliability for its collaboration partners. Its IT security objectives include:

- Ensuring the availability of IT systems, applications, and data
- Maintaining the integrity of IT systems, applications, and data
- Maintaining the confidentiality of data
- Preventing the inappropriate use of IT systems, applications, and data (improper use, use by unauthorized persons), for both self-protection and the protection of third parties
- Compliance with legal requirements, provisions of public funding providers, or contractual obligations relating to information security
- Protecting personal rights of employees as well as all persons in any way affiliated with the Max Planck Society

Systematic actions to address risks to information security serve as a basis from which to determine the required level of IT security as well as to plan and implement controls and activities in the context of IT security. The basis for risk assessment is the classification of data and infrastructure as well as the identification of threats.

Due to the continually changing risks, requirements, and new technical possibilities, the maintenance and improvement of IT security is a permanent task that must aspire in all ongoing processes to achieve continual enhancement on all affected levels. In addition to requiring the cooperation of every individual, this also necessitates both personnel and financial resources.

Responsibilities

The Executive Committee and the management of all facilities of the Max Planck Society (institutes, research units, Administrative Headquarters and central facilities) as well as the employees and users of the IT infrastructure of the Max Planck Society contribute through their conduct to ensuring IT security in the Max Planck Society. The Executive Committee expects the management of legally independent facilities of the Max Planck Society to also fulfill this responsibility and establish corresponding regulations, according to their individual circumstances. Due to the decentralized structures of the Max Planck Society and the collaborative and mobile working methods in the science sector, the management bodies of the Max Planck institutes and their scientific employees play a significant role in the institutes achieving their objectives.

The **Executive Committee of the Max Planck Society** bears the ultimate responsibility for IT security and ensures that the required attention and priority is afforded to issues of IT security. Moreover, in addition to the present IT Security Policy of the Max Planck Society, the Executive Committee establishes the IT Security Guidelines of the Max Planck Society, with further regulations governing organizational, procedural, and technical matters. In light of the pace of change in IT security-related issues, however, the IT Security Guidelines of the Max Planck Society should also provide a procedure for the IT Security Commission to make provisions for the minimum level of protection, in which cases the Executive Committee would then only examine the issues at a subsequent time.
.

The **IT Security Commission of the Max Planck Society** is a permanent governing body, appointed by the President of the Max Planck Society and under the leadership of a Vice President of the Max Planck Society. It initiates and coordinates all IT security-related activities.

The **IT Security Officer of the Max Planck Society** is appointed by the Executive Committee of the Max Planck Society and reports directly to the same. He or she is a member of the IT Security Commission and supports the Society's facilities in the fulfilment of their duties regarding IT security. The necessary authority and resources are made available to him or her.

The **management of each facility** bears the responsibility for IT security in that facility. On the basis of risk management, each one defines the specific level of security for its individual facility and creates the required framework conditions to give IT security the requisite level of importance in its area of operation. The management makes available the resources needed to attain these security objectives.

Every user of information and communication technology is responsible for the security and protection of data in their area of responsibility. The user is obligated to contribute to the completion of IT security-related tasks by being cooperative and responsible.