IT Security Guidelines of the Max Planck Society

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

Contents

Preamble

The present IT Security Guidelines are based on the IT Security Policy of the Max Planck Society, which took effect on 21 June 2017, and specify the IT security provisions for the facilities of the Society (institutes, research units, Administrative Headquarters, and central facilities) and their employees as well as for the users of their IT infrastructure.

The Guidelines define the permanent IT security structures of the Max Planck Society, their function, and their interaction as well as the necessary processes to enable the implementation, operation, and further development of a functioning management system to control IT security in the Max Planck Society.

The Guidelines are intended to be sufficiently generalized so as to avoid specifying provisions and solutions, but remain specific enough to be a framework for tangible implementation. Due to the rapid pace of developments in information technology, they must be flexible enough to remain applicable and, in particular, open to new IT security concepts. Nevertheless, they define a series of minimum requirements that ensure the actions of an individual facility have no negative repercussions for other facilities of the Max Planck Society or for the Max Planck Society as a whole. The minimum requirements should also ensure adherence to legislation, regulations, and compliance provisions.

The Guidelines are based on the interests of the Max Planck Society, its facilities, and its employees. These take precedence over the interests of individual persons.

The Guidelines promote close cooperation between all involved parties in order to do justice to the decentralized nature of the IT infrastructure of the Max Planck Society. It is only possible to conduct a realistic assessment of a threat situation and decide on which measures to take if all IT security incidents are openly shared. Handling errors in an open and sensitive manner is a precondition for this exchange.

The aim of the IT Security Guidelines is to protect the integrity, confidentiality, and availability of data, applications, and technical infrastructure. IT security controls must be

aligned to the requirements of scientific projects and the fulfilment of official duties. These controls should only restrict use, esp. for scientific purposes, insofar as it is absolutely necessary.

The processes described in the IT Security Guidelines must be implemented within a reasonable period of time.

A. Organizational Structures

A.1 Interfacility Organizational Structures

1. The Executive Committee of the Max Planck Society

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. In addition, it establishes the IT Security Policy of the Max Planck Society and these IT Security Guidelines of the Max Planck Society.

2. The IT Security Commission of the Max Planck Society

The IT Security Commission is established pursuant to the IT Security Policy. It is composed of up to ten members (a Vice President (Chair), at least three Directors, the IT Security Officer of the Max Planck Society, the Spokesperson of the IT Security Competence Network, one representative each for employees and for the Advisory Committee for IT Equipment in the MPG (BAR), and other persons).

The Chair shall appoint a deputy chairperson from among the Directors who are members of the Commission. This person is responsible for the competent operational management and organization of the body, insofar as the Chair does not perform such duties.

The Commission presents proposals, as necessary, to the Executive Committee of the Max Planck Society for the amendment of the IT Security Policy and the IT Security Guidelines. Both documents shall undergo a requirements review at least every five years and be subjected to necessary updates, which are subsequently presented to the Executive Committee to be reconfirmed by resolution.

In light of the pace of development in terms of IT security requirements, the IT Security Commission may, in cases of urgent need, effect amendments to Part C of these IT Security Guidelines in place of the Executive Committee. The Executive Committee must be informed subsequently.

Moreover, the IT Security Commission may issue further recommendations in the pursuit to fulfill the IT Security Policy and Guidelines. It shall present an annual report to the Executive Committee on the current state of IT security in the Max Planck Society.

In the case of a particularly severe IT security incident, the Chair of the IT Security Commission shall call together a crisis team and shall, in consultation with the President, take the necessary actions.

3. The IT Security Officer of the Max Planck Society

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/She is a member of the IT Security Commission and supports the bodies and facilities of the Society in fulfilling their

duties in the field of IT security. The necessary authority and resources are made available to him/her.

4. The IT Security Competence Network

The IT Security Competence Network is composed of IT security specialists in the facilities of the Max Planck Society and the IT Security Officer of the Max Planck Society, who work together in the field of IT security. The Network develops detailed proposals for the IT Security Commission and is available as a contact to the facilities and, in particular, to their IT groups. It acts when called and also operates independently and proactively, developing appropriate proposals, as it deems necessary. In particular, the IT Security Competence Network prepares measures for a severe IT security incident and is prepared to support the recovery of the Max Planck Society's operational abilities at short notice.

The Network elects a spokesperson who then becomes a member of the IT Security Commission. The Competence Network defines its own Rules of Operation. The necessary resources are made available to it.

A.2 Facilities

1. The Management of Each Facility

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

2. The IT Security Officers of the Facilities

The Management of each facility must appoint an IT Security Officer to whom the responsibility for IT security and further development of the same may be delegated. The IT Security Commission shall create a template for an effective letter of delegation. The role of the IT Security Officer may also be carried out by the head of IT. In the case of facilities with multiple locations or various requirements, it may be advisable to distribute these responsibilities among several IT Security Officers working collaboratively.

The IT Security Officers work in consultation with the Management and the IT Group. They produce a facility-specific IT security concept, which must be reviewed on a regular basis in accordance with new requirements, and develop the necessary controls to improve and maintain IT security. They are responsible for the maintenance and further development of a facility's documents relating to IT security.

3. The IT Groups and Administrations of the Facilities

The IT Groups and Administrations implement the necessary technical and organizational IT security controls laid out in the IT security concept. They thereby select the most suitable solution for their facility.

4. The Central Facilities of the Max Planck Society

Administrative Headquarters takes appropriate IT security measures for the administrative IT systems it operates and supports the facilities of the Max Planck Society in their efforts relating to IT security.

The central IT facilities of the Max Planck Society provide services across institutes with an appropriate level of IT security. They actively participate in the IT Security Competence Network and thereby support and enhance their work, e.g. with services, software tools, training, and training materials.

5. Superiors and Responsible Personnel

The responsibility for personnel, projects, devices, and data is also tied to the responsibility for the related IT security. The responsibility of a superior or responsible person also encompasses the introduction and implementation of the necessary IT security measures and controls as well as user compliance monitoring in the IT infrastructure in their respective area of responsibility. They work together with their facility's IT Security Officer in determining the level of IT security for their area.

6. Users

The IT security regulations are to be observed by all users. Users are obligated to participate cooperatively and responsibly in completing IT security-related tasks.

Users of information and communication technology take responsibility for the proper use of the services, data, and devices they use and are, in this sense, responsible for their IT security and protection.

All users are to be thoroughly informed about IT security to the extent necessary for their duties. The IT Security Officer of the Max Planck Society and the IT Security Competence Network shall provide the necessary materials.

B. IT Security Processes

1. Classification of Data and Infrastructure

Each facility of the Max Planck Society must be aware of its assets, that are significant in terms of the facility's work and which require the protection of IT security. These include, for example, data, applications, research equipment and IT systems as well as the network and communication infrastructure. These assets must be classified with regard to the classic protective aims of IT security. These are:

- the availability of information and communication technology, including applications and data
- the confidentiality of data and protection against unauthorized access
- the integrity of infrastructure and data

In order to achieve an appropriate level of protection, it is also necessary to identify the essential value of research activities.

To this end, one aim is to provide a comprehensive classification of all the facility's assets.

Individual assets that require special protection must be handled separately. Information and recommendations on carrying out this classification can be found in the "Guidelines For The Classification of Assets".

The classification of data, applications, and infrastructure is not a task for IT personnel, but rather for a facility's Management, a specific department, or a research group, as they are the proprietors of data and applications, and only they can evaluate their sensitivity.

The classification process must be documented in an appropriate manner.

2. Risk Assessment

Systematic actions to address risks to information security serve as a basis for determining the required level of IT security as well as for planning and implementing controls and activities in the context of IT security.

The basis for risk assessments is the classification of data and infrastructure as well as the identification of threats.

A regular survey and evaluation of IT security incidents in the Max Planck Society and its facilities is an important component in the process of identifying threats. The survey is prepared by the Competence Network in the form of a corresponding questionnaire and is carried out by the IT Security Commission on an annual basis. The facilities' IT Security Officers must collect the corresponding data for their respective facilities and convey this to the IT Security Commission. The results of this survey form the basis of the IT Security Commission's report to the Executive Committee of the Max Planck Society on the state of IT security and is provided anonymously by all facilities. They allow the facilities' Management and IT Security Officers to re-estimate the risk levels in their respective facilities and adapt their risk assessment accordingly.

In order to achieve a better data pool for the assessment of risks, collaborations with other research organizations and a mutual exchange of anonymized statistical risk data should be an aim.

Each facility's risk assessment must be documented in an appropriate manner.

3. IT Security Concept

Each facility of the Max Planck Society shall determine the necessary controls and activities to protect both the assets belonging to them and those entrusted to them against risks (data, applications, infrastructure, but also non-material assets such as work capacity or the reputation of the facility and of the Max Planck Society). The selected controls must be customized to the protective needs of the facility, take into account state-of-the-art standards and be proportionate to the envisaged risk mitigation. These controls must be agreed upon by the facility's Management, defined in a facility-specific IT security concept, and implemented within an appropriate period. The facility's IT security concept and the implementation and efficacy of controls must, on a regular basis, be reviewed, updated and, where appropriate, adapted according to any amended risk assessment.

The Max Planck Society makes an (electronic) catalogue of controls available to the facilities; it contains the potential controls to defend against various risks and achieve a particular level of IT security. This catalogue of controls is guided by DIN ISO/IEC 27001/2 norms, developed, updated, and further developed on a regular basis by the IT Security Competence Network, approved by the IT Security Commission, and recommended for implementation by the facilities. The individual facilities can adopt the appropriate controls

for their IT security requirements from this catalogue of controls. However, they may also lay down modified, individual, or additional controls.

Some of the controls in the catalogue serve to protect the Max Planck Society as a whole or aim to prevent IT security incidents at one facility from impacting others. These controls to avoid repercussions are listed in detail in Part C under "Minimum Requirements" and must be implemented by all facilities. The IT Security Commission rules on justified exceptions.

4. IT Security Incidents

In the event of an IT security incident, the facility's IT Security Officer and the IT Manager must be informed immediately. Depending on the seriousness of the incident, the management of the facility may also need to be informed. Facility Management shall then decide whether the IT Security Officer of the Max Planck Society and the IT Security Competence Network should be informed.

The IT Security Officer of the Max Planck Society and the Competence Network must be informed if a severe incident has occurred or if an incident may have repercussions for other facilities. The IT Security Officer of the Max Planck Society decides whether a prompt warning is to be issued to all facilities in order to protect them through appropriate measures. All IT security notifications are handled confidentially.

In particularly severe cases, the IT Security Commission and the President must also be notified. Detailed regulations on the classification and notification of IT security incidents are defined in Max Planck Society IT Security Standards on how to handle IT security incidents. These standards must be approved by the IT Security Commission. The facility's Management must implement corresponding regulations to ensure that IT security incidents in their area get reported.

Each facility shall document all its IT security incidents in an appropriate manner.

5. Quality Assurance

Quality assurance methods and procedures are to be implemented to identify discrepancies and continuously improve IT security.

Documents on processes, procedures, measures, and controls in the context of IT security must be produced and maintained in an appropriate manner and, if necessary, be approved by the responsible persons in order to ensure the planning, implementation, and monitoring of IT security. The documentation should be reviewed and updated on a regular basis as well as communicated to all parties concerned via the appropriate channels.

Continuous IT security improvements particularly require monitoring, internal reviews, and audits by third parties (e.g. by other facilities or service providers).

C. Minimum Requirements

1. Organization

The Management of each facility must appoint one person to be their IT Security Officer.

The facility must, within a reasonable period of time, develop and implement a facility-specific IT security concept on the basis of the valid IT Security Guidelines.

2. User Administration and Terms of Use

Each facility must establish a controlled process for user administration. In particular, the allocation of special access rights must be clearly regulated and accordingly documented.

The facility must regulate the rights and obligations of users of the IT infrastructure through terms of use and must guarantee that these have been made available to all users. These regulations must make users aware, in particular, of their role and responsibility regarding IT security.

3. Physical IT Security

Each facility must define the security areas in which their IT infrastructure requires special protection (servers, network components, storage devices telecommunications systems and the like) and regulate access to these areas. Appropriate measures must be implemented in order to restrict access to authorized persons only.

4. Network

Each facility must regulate the responsibilities and processes for the administration and the monitoring of its network.

A facility's network must be protected against threats from the Internet by firewall technologies that are technically up-to-date. Depending on the protective requirements, the network may need to be divided into separate network domains and equipped with a secured cross-domain access. Incoming connections from external sources are only permitted on approved servers.

External access to non-public resources must be provided encrypted and access-controlled.

Access to public resources must also be encrypted, insofar as technically sensible.

All active network components must be secured against unauthorized entry and access.

5. Backup

Each facility must produce, document, and update a data backup concept that corresponds to the IT security requirements of the facility. This must regulate, in particular, the location of backup media and the test of data recovery.

6. Archiving

Pursuant to the "Rules of Good Scientific Practice", each facility must secure the electronic records of its scientific activities against loss, destruction, or falsification and preserve the same over a longer period of time. A corresponding procedure that uses the facility's own or centrally provided technical archiving modalities must be established.

7. Patch Management

Each facility must inspect its IT infrastructure for technical weaknesses on a regular basis and implement appropriate measures for handling the ascertained risks. These must be documented accordingly. In particular, the actions to address safety patches must be regulated.

8. Malware

Each facility of the Max Planck Society must have a documented security concept regarding malware.

Software that identifies and, if possible, removes malware must be installed on operating systems that may contain viruses. If this is not possible, other actions to minimize risk must be taken. This software must be updated on a regular basis in order to be able to identify and deal with new versions of malware.

9. Email

Incoming emails must be inspected for malware and spam. Additionally, the transmission of malware and spam must be prevented.

10. Confidential Data

Confidential data must be protected by encryption if one of the following conditions is fulfilled:

- it is to be sent by email
- it is to be saved on a mobile device
- it is saved on an external service provider's servers (e.g. in the Cloud)
- an external service provider has access to internally saved data

Insofar as encryption against a service provider is not technically possible, contractual arrangements must be made with the service provider to ensure that confidentiality requirements are met for saving and processing data.

An appropriate measures for key management must be implemented.