Organisational Guideline for IT Security of the Georg-August University Göttingen and the University Medical Center Göttingen

Preamble

The conduct of University operations needs an increasingly high degree of integration of methods and processes based on the possibilities of communications and information technology (IT). IT processes that run smoothly and safely are an essential basis for the performance of the university and its administration in the areas of research, teaching, care for the sick, services in the public healthcare system, basic and advanced training and permanent education, as well as technology transfer.

Considering these circumstances, “security of information technology” (IT security) has immense basic and strategic relevance, to such an extent that it necessitates the development and implementation of a unified university-wide general guideline for IT security. One must bear in mind that secure IT processes are the basis for any data protection measures, which are particularly important when processing personal data.

Due to the complexity of the matter, the technological possibilities developing further at a fast pace and the limited financial and personal capacities, data protection can only be ensured within a continuous IT security process. The planning and extrapolation of this process must go by the given duties and legal rights of the university, on the other hand it can only be realised by means of a continuous IT security process within the frame of clearly defined responsibility structures.

The aim of this Organisational Guideline for IT Security is not only to achieve compliance with existing legal obligations but also and primarily to protect applications and data processed, transferred and stored at the university, and to protect the university itself from material and immaterial damages as far as possible.

We would like to state explicitly that successful implementation of the IT security process can only be achieved with the support of all members of staff and everyone working at the University and the University Medical Center.

1 Object of Guideline

The guideline defines and regulates the responsibilities, responsibility structure, assignment of tasks, and the cooperation between the people involved, for the university-wide IT security process, as well as its funding.

2 Scope

This guideline applies to all University and University Medical Center institutions, to their complete IT infrastructure including the IT systems in operation, and all users.

3 IT Security Concept

(1) The IT security concept of the university is based on
- this guideline for IT security
- the general IT security guideline of the University and the University Medical Center published in the bulletin (“Amtliche Mitteilungen”)
- the utilisation arrangements for the University Medical Center IT infrastructure
- individual regulations referred to in the general IT security guideline.

(2) The security concept follows the IT Baseline Protection Manual (“Grundschutzhandbuch”) issued by the Federal Office for Information Security (BSI).

4 Organisational Structure of the IT Security Process

(1) The presidential board of the University and the management of the University Medical Center are responsible for IT security and the IT security process.

(2) The coordination of the IT security process is managed by the “IT Strategy” workgroup of the presidential board of the University and the management of the University Medical Center, within its capacity as the Chief Information Office (CIO) of the University and the University Medical Center.
The “IT Strategy” workgroup consists of
- the member of the presidential board responsible for IT
- the member of the presidential board responsible for library affairs
- the member of the management of the University Medical Center responsible for economic affairs and administration
- additional members appointed by the presidential board and the management of the University Medical Center.

(3) The “IT strategy” workgroup appoints the “IT security” workgroup which consists of
- one representative for the computer centres (GWDG and G3-7) and the NSUB each
- the data protection officers of the University and the University Medical Center
- additional members appointed by the “IT Strategy” workgroup.

(4) The heads of divisions are responsible for the implementation of IT security within the respective institutions. It is recommended that the heads of divisions nominate IT officers for their respective sections who cooperate with the “IT Security” workgroup in implementing the IT security process within the division. If no one is nominated as IT officer, the function of IT officer is filled by the head of division.

(5) Different institutions can nominate a common IT officer. The function of IT officer can be filled by someone belonging to a superordinate organisational level.

5 Responsibility Assignment

(1) The “IT Strategy” workgroup coordinates the IT security process.

(2) The “IT Strategy” and “IT Security” workgroups act as IT security advisers to the presidential board of the University and the management of the University Medical Center.

(3) The “IT Security” workgroup develops and reworks drafts for internal technological standards at the university, guidelines, and IT security emergency procedures, to be put into force by the presidential board of the University and the management of the University Medical Center. The “IT Security” workgroup supports the “IT Strategy” workgroup in implementing and monitoring the IT security process; it also coordinates training and further education of IT officers and supports them in implementing the guidelines. On behalf of the presidential board of the University and the management of the University Medical Center, the “IT Security” workgroup annually compiles an IT security report in cooperation with the “IT Strategy” workgroup.

(4) The IT officers continually monitor the implementation of the IT security process in their respective divisions. In order to do that, they must be provided with the necessary powers by the respective heads of division. They regularly inform the management of their institution and the “IT Security” workgroup about the progress and state of implementation. They immediately report security-relevant events to the “IT Security” workgroup and the management of the institution. They are obligated to keep themselves up-to-date concerning IT security, a process in which the management of the respective institutions assists them.

(5) All members of staff and persons working at the university are obligated to report security-relevant incidents to the responsible IT officer immediately.

(6) The computer centres are responsible for system, network and operational aspects of IT security. They closely cooperate with the “IT Strategy” and “IT Security” workgroups.

6 Emergency Intervention

(1) The computer centres (GWDG and/or G3-7) take measures to avert danger from IT systems; these measures may include blocking network access points and user accounts (if necessary without notification of those concerned). The responsible IT officer and the “IT Security” workgroup must be notified immediately. The emergency intervention measures are cancelled by the computer centres upon agreement with the “IT Security” workgroup after sufficient IT security measures have been taken; the responsible IT officer is informed about the course of events.

(2) If necessary in order to repel an acute danger, the IT officers take the appropriate measures, which may include shutting down IT systems within their area of responsibility. The “IT Security” workgroup and the management of the institution must be notified immediately. The emergency intervention measures are cancelled by the IT officers upon agreement with the “IT Security” workgroup after sufficient IT security measures have been taken.

7 Funding

Human and financial resources of all central and peripheral IT security measures are funded from the budgets of the IT service providers, the central administration, and the central institutions and faculties. This applies to training measures for IT officers and users, whether they are conducted centralised or decentralised.

8 Coming into Effect

This guideline is put into force by the University chairmanship and the management of the University Medical Center. It comes into effect on the day after its announcement in the bulletin.

Göttingen,

Für die Georg-August-Universität Göttingen
(ohne Universitätsmedizin)
- Der Präsident -
Prof. Dr. Kurt von Figura

Göttingen,

Für die Universitätsmedizin Göttingen
- Der Sprecher des Vorstands -

Prof. Dr. Cornelius Frömmel