(English translation provided for informational purposes. If the English and German versions allow different interpretations, the German version is legally binding. Note: In the text are used the German abbreviations for the roles.)

Information Security Guideline of the University of Göttingen/ University of Göttingen Public Law Foundation

– Information Security Guideline / Informationssicherheitsrichtlinie (ISRL) –

Published in the Official Announcements I of the

University of Göttingen dated 24.01.2020/No. 4, pages 46-89

(http://www.uni-goettingen.de/de/amtliche+mitteilungen+i+ausgabe+4+%2824.01.2020%29/619701.html)

Presidential Board and Management Board of the University Medical Center:

The Presidential Board of the University of Göttingen and the Management Board of the University Medical Center have issued the revised version of the Information Security Guidelines of the University of Göttingen/University of Göttingen Public Law Foundation on 01.10.2019 based on the recommendation of the Senate Committee for Information Management (KIM) on 09.05.2019 and the opinion of the Senate and the Faculty Council of the Faculty of Medicine on 22.05.2019 and on 27.05.2019 (§ 37 Section 1 Sentence 3 Clause 1 NHG (Higher Education Act of Lower Saxony); § 63 e Section 1 Sentence 1 NHG; § 41 Section 2 Sentence 2 NHG; § 63 h Section 2 Sentence 2 NHG).

The Staff Councils of the University and the University Medical Center gave their consent on 18.12.2019 and 17.12.2019 (§ 66 Section 1 No. 10. NPersVG (Staff Representation Act of Lower Saxony))

Table of Contents

Section I: Principles

§ 1 Subject matter and scope

(1) The information security guideline defines responsibility structures, assignment of tasks and the cooperation between those involved as well as the content-related specifications of the University's information security process.

(2) It applies to all employees of the University of Göttingen/University of Göttingen Public Law Foundation including the University Medical Center (hereinafter collectively referred to as University of Göttingen Foundation). Especially when they use the IT infrastructure of the University of Göttingen Foundation or process data of University of Göttingen Foundation or their customers to the entire IT infrastructure of the University of Göttingen Foundation, including the IT systems that are operated.

§ 2 Framework conditions

(1) Running a university and a maximum-care university hospital increasingly requires the integration of procedures and processes that are based on the possibilities offered by the communication and information technology (IT). Functional and secure IT processes are therefore the key basis for the efficiency of the University and its administration, especially in the areas of research, teaching, medical care, public health services, training, advanced training and continuing education as well as technology transfer.

(2) Information security is of fundamental and strategic importance here, and it requires the development and implementation of an information security guideline. Not least, secure IT processes are the basic requirement for all data protection measures that have to be implemented when personal data is processed.

(3) Due to the complex subject matter, the rapidly developing technical possibilities and the limited financial and human resources, this can only be done through a continuous information security process. This information security process must be developed and updated based on the tasks and the rights of the University on the one hand and, on the other hand, can only be achieved through continuous information security process within regulated responsibility structures.

(4) The information security guideline not only aims at meeting the existing legal requirements, but also at fundamentally protecting the data and applications used in the University as well as protecting the University from material and immaterial damage and, in the process, taking into account the freedom of research and teaching, worldwide cooperation based on professional exchange, common project structures, high staff turnover, various user groups with their different roles and rights and the rapid development cycles of information technology.

§ 3 Security goals

(1) For the purposes of this guideline, information security means to establish and maintain

(a) "confidentiality"; i.e., to guarantee that only authorised persons have access to information,

(b) “integrity”; i.e., to ensure the correctness and completeness of information and processing methods,

(c) “availability”; i.e., to guarantee need-based access to information to authorised persons.

(2) This information security guideline is intended to ensure that security measures are taken, which are appropriate for the respective protection purpose and which correspond to the state of the art, in order to minimise the occurrence of information security incidents. These measures particularly serve

(a) reliable support of processes by the IT and the continuity of workflows,

(b) patient security and treatment effectiveness in medical care by the University Medical Center,

(c) the preservation of official, company, business and other secrets,

(d) that the requirements resulting from legal specifications are met,

(e) that the right of self-determination with respect to information of the person concerned is ensured when his or her personal data is processed,

(f) compliance with the regulation of the University of Göttingen to ensure good scientific practice,

(g) the reduction of material and immaterial damage resulting from information security incidents and

(h) the implementation of secure and trustworthy procedures for exchanging information, for communication and for transactions with cooperation partners.

§ 4 Information security process

(1) The information security process is used for securing data, whereby the security of data processing systems and entities must be guaranteed, and particularly includes the following tasks:

(a) Definition and determination of responsibilities,

(b) Determination of protection requirements and recognition of risks,

(c) Definition and determination of access to information as well as the type and scope of authorisation,

(d) Determination of security and control measures in accordance with the information security guideline,

(e) Implementation, review and updating of security and control measures to protect information.

(2) All information shall be assigned to categories with approximately equal protection requirements; where:

(a) “Normal protection required” means that the impacts of damage are limited and manageable,

(b) “High protection required” means that the impacts of damage could be considerable,

(c) "Very high protection required" means that the impacts of damage could reach an existentially threatening, catastrophic extent.

(3) Based on possible damaging events and their causes and effects, risks must be assessed and handled with the help of a risk treatment plan by taking risk mitigation, risk avoidance, risk transfer or risk acceptance measures, considering the financial and organisational effort. Any remaining risks within the framework of risk acceptance must be described and the management should assume responsibility for them.

Section II: Organisational specifications

§ 5 Presidential Board and Management Board

(1) The overall responsibility of information security and the information security process lie with the management of the University and respectively, with the Management of the University Medical Center (UMG).

(2) The Presidential Board and Management Board delegates the organisation and implementation of information security management to the extent specified in 11 and 12 to the Information Security Officer (Informationssicherheitsbeauftragter, ISB) or the Information Security Manager (ISM).

(3) The competent management of the respective unit specified in Addendum 1 (hereinafter called: competent management) is responsible for performing the tasks specified in § 8 at a decentralised level. The Presidential Board or the Management Board can cancel the delegation according to Sentence 1 and decide for themselves.

§ 6 IT Steering Group and CIO

(1) The IT Steering Group and the joint Chief Information Officer of the University and the UMG (CIO) perform tasks for the IT and thus also for the information security of the University of Göttingen Foundation.

(2) Specific responsibilities are defined in the “Operating Procedures for Joint IT Governance of the University of Göttingen and the University Medical Center for the IT Steering Group and the Chief Information Officer” in the currently applicable version.

§ 7 IT service providers

(1) IT systems and IT services for the University of Göttingen Foundation are primarily provided by the following IT service providers cooperatively:

(a) Department of Digital Library of the Göttingen State and University Library (SUB),

(b) The IT department of the University,

(c) The Information Technology division of the UMG,

(d) Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG).

(2) By providing professional and secure IT services, IT service providers make a significant contribution to the information security of the University of Göttingen Foundation.

(3) If a task is not performed by the IT service providers mentioned in Section (1), institutions can use their own IT systems and IT services and have them operated by other service providers. In such IT systems, IT service providers help with fundamental issues of IT operation and information security.

§ 8 Competent management

(1) The competent management as specified in Addendum 1 can, in its sphere of responsibility, entrust subordinate managements of a subdivision with the performance of its tasks, thus making the subordinate management the competent management in their sphere of responsibility. This must be documented and communicated to the ISM. This does not affect the representative performance of these tasks by a deputy in the event of absence.

(2) In its sphere of responsibility, the competent management is responsible for:

a) appointing an Information Security Coordinator according to Section (3),
b) appointing specialist managers according to Section (5),
c) deciding on the respective specific information security concepts according to Section (6),
d) deciding on the further handling of information security incidents according to § 16.

(3) The competent management can appoint an employee of the University of Göttingen Foundation as the Information Security Coordinator (ISK) for the respective unit. The appointment must be documented. If an ISK is not appointed, then his or her tasks are the responsibility of the competent management. The competent management can also appoint one or more deputies for the ISK.

(4) Competent management can mutually appoint joint ISKs for their units.

(5) The competent management can appoint an appropriate number of specialist managers for the data sets, IT procedures, IT systems and infrastructures assigned to a unit. The appointment must be documented. If a specialist manager is not appointed, then his/her tasks are the responsibility of the competent management.

(6) The competent management decides on the specific information security concepts based on the opinion of the ISK and upon getting an approval from the ISB and is responsible for the risks undertaken in these concepts.

§ 9 Information Security Coordinators (Informationssicherheitskoordinatoren, ISK)

(1) Information Security Coordinators (ISK) coordinate the information security process within their sphere of responsibility and monitor its implementation by IT users. ISK's report on this to the competent management.

(2) The competent management is responsible for ensuring that ISKs are equipped with the authority and the resources necessary to carry out their tasks. The competent management is obliged to ensure that it participates in the necessary further trainings in the field of information security; participation in further training is a duty arising from the individual employment or service relationship.

(3) The tasks of the ISK particularly include:

(a) Recommendation of awareness-raising and training measures,

(b) Providing advice to specialist managers for the performance of their tasks,
(c) Initiation of the preparation and updating of protection requirement assessments and risk analyses,
(d) Giving opinion on specific information security concepts,
(e) Immediate submission of specific information security concepts to the ISB,
(f) Gathering and providing specific information security concepts of the respective unit,
(g) Assessing the severity of the reported information security incidents; checking whether an information security incident could also be a data protection incident and preparing the recommended course of action according to § 16 for the competent management,

(4) ISKs may seek advice from the ISB and the ISM to perform their tasks.

§ 10 Specialists responsible (Fachverantwortliche)

(1) Specialists reponsible are responsible for implementing the information security processes for the datasets, IT procedures, IT systems and infrastructure assigned to them. This particularly includes the following tasks:

(a) Identification of the protection requirement for information, IT procedures, IT systems and infrastructure as well as the analysis of risks,
(b) Preparing and updating operational concepts based on the protection requirements assessment and risk analysis,
(c) Regular review of the protection requirements assessment, risk analysis and the operational concept according to the intervals to be defined in the operational concept,
(d) Initiating and controlling the implementation of the measures laid down in an operational concept, particularly also when using external IT service providers (e.g., order processing).

(2) To perform their tasks, specialists responsible may seek advice from the may seek advice from the ISK, ISB or other staff of the respective unit or the internal IT service provider.

(3) A protection requirements assessment and risk analysis may also result in a decision that no further measures over and above the implementation of the information security guideline and the catalogue of measures for basic IT protection are required for a dataset, IT procedure, IT system or an infrastructure (Addendum 2).

§ 11 Information Security Officer (Informationssicherheitsbeauftragte*r, ISB)

(1) The Presidential Board and Management Board appoint an Information Security Officer (Informationssicherheitsbeauftragte*r, ISB). The appointment must be documented.

(2) The tasks of the ISB particularly include:

(a) Coordination and further development as well as the monitoring of the implementation of the information security process for the University of Göttingen Foundation,

(b) Preparing recommendations for the Presidential Board and Management Board for the following topics:

(i) Preparation and updating of the catalogue of measures for basic IT protection,

(ii) Additional information on the information security guideline (e.g., recommendations for internal University technical standards, model solutions, and contingency plans),

(iii) Changes to specific information security concepts based on security incidents (with respect to §16 Section (5)),

(iv) Training concepts.

(c) Providing advice to the following:

(i) The Presidential Board, Management Board, IT Steering Group and CIO for information security related issues,

(ii) Managements of IT service providers,

(iii) Data protection officers and data protection managers for technical and organisational measures,

(iv) Units for the implementation of the information security guideline,

(v) ISK for the elimination of information security risks,

(vi) Specialists responsible for the preparation of specific information security concepts.

(d) Approving specific information security concepts of the units; in the event of disagreement, the decision is made by the Presidential Board or the Management Board

(e) Preparing and updating an index of all specific information security concepts,

(f) Assessing information security incidents and deriving structural and conceptual recommendations in accordance with § 16,

(g) Preparing the annual report on information security for the Presidential Board and the Management Board, including recommendations for the revision of this information security guideline and other overarching information security concepts; if necessary, this report is also submitted to other authorities.

(3) During the information security process, the ISB has to consider data protection issues and involve the Data Protection Officer in the formation of measures and concepts in the event of a conflict of objectives between information security and data protection.

§ 12 Information Security Manager (ISM)

(1) The Presidential Board and Management Board appoint an Information Security Manager (ISM) for the University and the University Medical Center.

(2) The tasks of the ISM particularly include:

(a) Assignment for the management and monitoring of the implementation of information security measures in the context of risk treatment plans, including awareness-raising and training measures, as well as documentation of measures of the respective sphere of responsibility,

(b) Assessing and forwarding information security incident reports and preparing the recommended course of action for handling information security incidents in the operational area in accordance with § 16 Section (4).

(c) Preparing an information security report insofar as it concern:

(i) the progress and problems involved in the implementation of information security measures (operational aspects) or

(ii) information security incidents of the respective sphere of responsibility.

§ 13 Data Protection and Information Security Advisory Council (DIB)

(1) The Data Protection and Information Security Advisory Council (DIB) comprises:

(a) the ISB,

(b) a deputy of the ISB,

(c) the ISMs of the University and the UMG,

(d) the Data Protection Officers (Datenschutzbeauftragte*r, DSB) of the University, the UMG and GWDG,

(e) the Data Protection Manager (Datenschutzmanager*in, DSM) of the University and the UMG,

(f) one representative each from GWDG, the Information Technology division of the UMG, SUB and the University's IT department,

(g) two representatives of University faculties and one representative of the medical faculty,

(h) one representative of Department 2 (Medical Care) of the UMG,

(i) one representative each of the departments and staff units of the central administration and of Department 3 (Economic Management and Administration) of the UMG,

(j) one member each of the Staff Council of the University and the UMG as well as

(k) other persons appointed by the ISB as required.

(2) The meetings of the DIB take place as often as the state of business requires, but at least four times a year. They are convened and chaired by the ISB.

(3) The DIB serves the following purposes:

(a) Information exchange between those involved in the information security process and the data protection process,

(b) Consideration of the interests of the areas of research and teaching, medical care and administration as well as of those involved in the information security process,

(c) Involvement of IT service providers in the information security process,

(d) Advising the ISB, DSB, the ISM and the DSM on information security and data protection issues,

(e) Drafting recommendations for amending the information security guideline and overarching concepts or advisories on information security and data protection.

Section III: Content-related specifications

§ 14 Catalogue of measures for basic IT protection

(1) Content-related specifications for IT systems with a normal protection requirement (basic IT protection) are defined in the "Catalogue of measures for basic IT protection", which is subdivided into measures for IT users and IT staff.

(2) The provisions of the catalogue of measures are binding; deviating from them is possible solely in accordance with Section (3).

(3) Provisions that deviate from the catalogue of measures may be drawn up in specific information security concepts for restricted datasets, areas of the IT infrastructure or IT systems taking into account specific risks and protection requirements, provided that no information security or data protection requirements with regard to the data to be processed or the IT infrastructure are in conflict with them.

(4) The GWDG as an IT service provider for the University is contractually obliged to comply with the information security guideline.

(5) External IT service providers entrusted with performing tasks on IT systems are obliged to comply with the information security guideline, insofar as this is in line with the protection requirement. Compliance with the information security guideline by external IT service providers must be verified by the competent IT staff of the client External IT service providers are obliged to inform the client of the risks that can arise in the IT system as a result of the services they provide.

§ 15 Additional measures

(1) For all IT systems, the respective specialist responsible must check if there is a higher protection requirement over and above basic IT protection.

(2) Where a higher protection requirement is identified, additional measures within the framework of an operational concept must be determined by the specialists responsible.

(3) IT systems for which a higher protection requirement has been identified may be put into operation only after operational concept for these has been decided upon, implemented and released for operation based on risk assessment.

§ 16 Handling of information security incidents

(1) Employees of the University of Göttingen Foundation must immediately notify the responsible ISK about incidents relevant to information security (information security incidents).

(2) The ISK assesses the severity of the information security incident and forwards his or her recommended course of action to the competent management.

(3) The competent management decides on the further handling of the information security incident. The management also decides whether the ISM must be informed owing to the severity of the information security incident and, if necessary, immediately informs the ISM itself or asks the ISC to do so. Information security incidents relating to data protection must be reported to the DSM and the ISM.

(4) The ISM informs the ISB of the reported information security incident and seeks his/her statement. Based on his/her own assessment and the statement of the ISB, the ISM informs the Presidential Board or the Management Board about the reported information security incident immediately and/or in the form of an information security report. In consultation with the ISB, the ISM prepares the recommended course of action for the operational processing of the information security incident for the competent body.

(5) After an information security incident, the ISB checks whether there is a need to change information security regulations, in particular the guideline as well as overarching and specific information security concepts and prepares the recommended course of action for the Presidential Board, the Management Board, the competent management and the ISK based on the opinion of ISM, the competent ISK, the competent management and the DIB.

(6) The ISM reports information security incidents to the competent authorities. Insofar as information security incidents are also data protection incidents, the DSM reports them to the competent authorities.

(7) The Presidential Board or the Management Board can, in a guideline document, regulate further details on how to handle information security incidents.

§ 17 Threat intervention

(1) In order to avert a current threat to information security, the IT staff and internal IT service providers (including the GWDG), in their respective spheres of responsibility, takes the necessary measures to prevent or eliminate the impact of the damaging event. If the threat is significant, blocking of network connections and user accounts may be taken as a necessary measure.

(2) If there is an important reason, network connections and user accounts may be blocked without giving prior notification to those affected by the blocking.

(3) The competent ISC and the ISM must be informed immediately.

(4) The measures are lifted with the consent of the ISM and the ISK after the necessary IT security measures have been carried out.

Section IV: Final provisions

Entry into force and expiry

(1) The information security guideline of the University of Göttingen/University of Göttingen Public Law Foundation will come into force on the day after its publication in the Official Announcements I of the University of Göttingen.

(2) At the same time, the general safety guideline of the University of Göttingen and the University Medical Center in the version contained in the announcement dated 15.06.2007 (Official Announcements 11/2007 p. 493) and the organisational guideline for IT security of the University of Göttingen and the University Medical Center in the version contained in the announcement dated 15.06.2007 (Official Announcements 11/2007 p. 522) will cease to be in force.

Addendum 1 Assignment of the competent management for a respective unit

Unit	Competent management
Faculties	the respective Dean
Interdisciplinary institute and central academic institutions (e.g., centres, Lichtenberg-Kolleg)	the respective Director/Management
Interdisciplinary and central infrastructure institutions (e.g., SUB, labs)	the respective Management
Institutions for special tasks (e.g., XLAB)	the respective Director/Management
Departments and staff units of the central administration	the respective Management
University hospitals and institutes of the UMG	the respective Management
departments, divisions and central institutions of medical care or administration of the UMG	the respective Management

Addendum 2 Catalogue of measures for basic IT protection

A. Measures for users

A.1 User qualification

Responsible for initiation:	Competent management
Responsible for implementation:	ISK

(1) Staff members must be trained in a task-specific manner for the IT procedures used in the workplace. Training objectives are:

(a) Secure handling of the application,

(b) Sensitisation towards information security issues,

(c) Encouraging self-assessment when problems occur (When should experts be involved?),

(d) Knowledge of existing provisions,

(e) Knowledge of data protection requirements.

A.2 Reporting of IT problems

Responsible for initiation:	ISK
Responsible for implementation:	IT users, IT staff

(1) The respective IT user must report any type of IT problem (system crashes, faulty behaviour of applications that have run error-free so far, hardware failures, intrusion by unauthorised persons, manipulations, virus attacks etc.) to the competent IT staff.

A.3 Consequences and penalties in case of security breaches

Responsible for initiation:	Competent management
Responsible for implementation:	Competent management

(1) Violations can have disciplinary or employment law consequences. Moreover, violations of legal provisions (e.g., data protection laws, medical confidentiality) can be prosecuted as a criminal or administrative offence.

(2) Culpable non-observance of the information security guideline particularly constitutes a violation according to Sentence 1 especially if it

(a) significantly impairs the security of the members of the University of Göttingen Foundation, users, contractual partners, advisers,

(b) jeopardises the security of data, information, IT systems or the networks,

(c) causes material or immaterial damage to the University of Göttingen Foundation,

(d) facilitates unauthorised access to systems and information and their disclosure and/or modification,

(e) facilitates the use of information of the University of Göttingen Foundation for illegal purposes and

(f) facilitates unauthorised access to personal data and confidential University data.

(3) If there are sufficient factual indications of a violation, the IT employees can take measures - even without the knowledge of the person/persons concerned - that are appropriate for preventing, intercepting or recording the imminent damage as a result of the violation. The competent Data Protection Officer, a representative of the respective Staff Council and a representative of the internal auditing department (hereinafter collectively referred to as: parties to be involved) must be consulted before taking action; their consent for the measures to be taken is required before they are implemented. The IT staff carrying out the measures informs the following about the course and the result of the measures:

(a) the parties to be involved,

(b) in every case the person concerned, if necessary, the supervisor and other persons; in all cases in coordination with the parties to be involved.

(4) The data collected must be destroyed immediately after the measure has been completed. The parties to be involved must determine that a measure has been completed.

A.4 Controlled use of software

Responsible for initiation:	ISK
Responsible for implementation:	IT staff, IT users

(1) Only that software which is necessary for the fulfilment of official and study-related tasks may be installed on the IT systems of the University of Göttingen Foundation.

(2) IT users are not permitted to install or run additional software without authorisation. This particularly applies to downloading software from the Internet or launching software received via email.

A.5 Protection against viruses and other malware

Responsible for initiation:	ISK
Responsible for implementation:	IT staff, IT users

(1) An up-to-date virus scanner, which automatically checks all files when they are accessed, must be installed on all workstation computers. This is intended to detect and prevent the intrusion of malicious programs.

(2) The competent IT staff must be informed if malware infection is suspected.

A.6 Access control

Responsible for initiation:	ISK
Responsible for implementation:	IT staff, IT users

(1) Rooms that have workstation computers must be locked outside the normal working hours (especially at night and on weekends) and when there is no one in them. Deviation from this may be allowed only if work organisation urgently necessitates this and if other security measures allow it.

(2) In rooms open to the public, workstations must be set up such that sensitive data cannot be viewed from screens by unauthorised persons.

(3) When sensitive data is printed, the removal of the printouts by unauthorised persons must be prevented (ensuring confidentiality).

A.7 Locking and shutting down systems

Responsible for initiation:	ISK
Responsible for implementation:	IT staff, IT users

(1) When leaving the workstation, the workstation computer must be locked with a password.

(2) Locking must also be automatically time-controlled when the computer is not used.

(3) In general, workplace computers are to be shut down at the end of the shift.

(4) Deviation from the rules for locking and shutting down systems is possible only if work organisation urgently necessitates this (e.g., in the case of measurement and control computers) and if appropriate security measures allow it.

A.8 Securing notebooks, mobile storage media, smartphones

Responsible for initiation:	ISK
Responsible for implementation:	IT users

(1) In principle, mobile end devices and storage media must be protected against theft using appropriate security measures.

(2) Unauthorised access to mobile end devices and the data stored on them must be prevented by means of appropriate access protection measures (e.g., passwords, PINs, biometric procedures).

(3) Storing of sensitive data on notebooks, mobile storage media (e.g., smartphones, USB sticks, etc.) is permitted only if there is a business need and the data is encrypted in accordance with the current security requirements[1]. Furthermore, it must be ensured that unauthorised access to data by unauthorised persons is excluded.

[1] Algorithm, key length according to the Federal Network Agency

A.9 Personal user accounts

Responsible for initiation:	ISK
Responsible for implementation:	IT staff, IT users

(1) All IT systems (including smartphones) that are used for official purposes must be set up such that only authorised persons have access to them. This primarily requires a login with a suitable authentication method (password, smart card, biometric procedure, etc.).

(2) The allocation of user accounts for working on IT systems must be person-related-specific principally. Working under another person's user account is not permitted.

(3) Deputies (temporary delegation of duties) must not be organised by passing on login data for personal user accounts, but by appropriately assigning rights.

(4) An IT user is prohibited from passing on login data required for the authentication process.

(5) Dispensing with personal user accounts is permitted for IT systems, in which a quick change of user is required due to the work organisation (e.g., control centres in the UMG, reading rooms) or which are intended for general public access (e.g., kiosk systems, query stations for library catalogues).

A.10 Use of passwords

Responsible for initiation:	ISK
Responsible for implementation:	IT staff, IT users

(1) Every person is responsible for all actions performed using his/her user account.

(2) The passwords used for the use of IT systems of the University of Göttingen Foundation must not be identical or similar to passwords used for the usage of other IT systems.

(3) The following must be observed when dealing with passwords:

(a) Passwords must not be saved on programmable function keys.

(b) Saving passwords for IT systems of the University of Göttingen Foundation in applications, especially browsers, is generally not permitted. If exception regulations allow storage, then access to the password memory must be secured with a master password.

(c) If passwords cannot simply be memorised, for example because of their large number, but have to be noted, they have to be saved in a password manager with a secure master password.

(d) Writing down of passwords on paper must be avoided. If writing down of passwords cannot be avoided, the passwords must be kept at least as securely as a bank card or bank note.

(e) A password must be changed if it has become known to unauthorised persons.

(f) Ensure that passwords are not observed by others when entered.

(4) If an IT system or an application does not prompt a password change or explicit rules have not been laid down for this, the following rules for password change must be followed:

(a) The password must be changed regularly. A period of three months to one year is recommended as the deadline for changing passwords.

(b) New passwords must differ significantly from the old passwords over several change cycles.

(5) If an IT system or an application does not prompt password rules or explicit rules have not been laid down for certain passwords, the following rules for password strength must be followed:

(a) Letters and/or character sequences that are common or easy to guess, such as names, license plate numbers, birth dates, individual words in German or a different language or only slightly varied versions of such character strings, must not be used.

(b) The password must have at least 8 characters. A length of 10 characters is recommended.

(c) Every password must contain at least one upper case and one lower case letter, one number and one special character.

(d) Alternatively, it is possible to deviate from (c) if it is ensured that the selected password is just as secure, for example because it is longer, as the one that is selected as per (b) and (c).

(6) If, for unexplained reasons, a user does not get access to the system when logging in with his/her password, this could indicate that an attempt has been made to determine the password by trial and error to gain illegal access to the system. Such incidents must be reported to the competent superior and the IT staff (see A.2).

(7) If a user forgets his or her password, he or she shall request a reset from the responsible IT staff or, if available, via self-service functions without repeated attempts. This provision is intended to prevent the process from being logged and treated as an attempted intrusion.

A.11 Access rights

Responsible for initiation:	ISK
Responsible for implementation:	IT staff

(1) A user may only be given those access rights that he/she needs to carry out his/her official tasks. In particular, work that does not necessarily require higher privileges not allowed to be performed using privileged user accounts (“administrator”, “root”, etc.).

(2) Privileged user accounts may only be assigned to the IT staff, or persons with privileged user accounts must be regarded as IT staff and must observe and implement the measures laid down for the IT staff.

(3) In addition to technical measures, organisational rules must also be observed (e.g. for accessing patient data in the University Medical Centre).

A.12 Network access

Responsible for initiation:	ISK
Responsible for implementation:	IT staff, IT users

(1) IT systems may only be connected to the data network via the infrastructure provided for this purpose. Set-up or use of additional network access (routers, switches, modems, WLAN access points, etc.) that is unauthorised or carried out without the prior consent of the network operator is prohibited.

(2) The “Network Operation Regulation of the University Medical Center” and the “Usage Regulation of GWDG” must be observed during implementation.

A.13 Teleworking, mobile working and home office

Responsible for initiation:	Competent management
Responsible for implementation:	IT staff, IT users

(1) In teleworking, data goes out of the spatially limited area of the data processing body.

(2) For the establishment and operation of such workplaces, the existing company agreements[2] as well as further regulations on data protection and data security shall be observed.

A.14 Secure network usage - general requirements

Responsible for initiation:	ISK
Responsible for implementation:	IT staff, IT users

(1) As far as technically possible, the use of encrypted communication services must be preferred over the use of unencrypted services.

(2) The transmission of sensitive data must be encrypted or secured by other appropriate measures (e.g., isolated separate networks).

A.15 Secure network usage - email

Responsible for initiation:	ISK
Responsible for implementation:	IT staff, IT users

(1) Only official email accounts may be used for official email communication.

[2] See appendix “Related documents”

(2) Automated forwarding of official emails to external providers (Internet providers) is not permitted.

(3) Existing technical solutions for secure and encrypted data transmission or data provision[3] must be used for the electronic forwarding of sensitive data.

(4) If official emails are accessed from outside the University of Göttingen Foundation, it is mandatory to use encrypted transmission protocols. The regulations laid down in measure (A.8) must be observed.

(5) If official emails are accessed from non-university IT systems, it must be ensured that no content remains on the external systems after use.

(6) It is generally prohibited to log in via Internet links stored in emails. This does not apply to emails that have been triggered to verify identity by one’s own actions when registering for services.

(7) It is expressly prohibited to respond to requests contained in emails for the disclosure of login data.

(8) Attachments and Internet links received by email can be opened only if their harmlessness can be assumed, e.g., through their origin and context.

A.16 Data storage

Responsible for initiation:	Specialists responsible
Responsible for implementation:	IT staff

(1) Official data must always be stored within the IT systems of the University of Göttingen Foundation (including the IT systems that the GWDG operates for the Foundation University).

(2) The options of storing data on central servers must be used.

(3) Storing of sensitive data on the hard disk of the workstation computer or on other local storage media is permitted only if the operational concept for the respective data set allows this and if the security measures specified therein have been taken.

(4) Storing (and processing) of official data outside the IT systems of the University of Göttingen Foundation (e.g., on cloud services or private devices) is permitted only if this is required for official purposes and if the operational concept for the respective data set allows such storage. If data is stored externally, then it must be protected against loss of data, confidentiality and data integrity in a manner appropriate to the protection requirement. It must be possible to recover and delete data from an external storage.

[3] For example Cryptshare in the UMG at the time the guidelines were created.

(5) Storing of sensitive data outside the IT systems of the University of Göttingen Foundation is permitted only in the states of the European Economic Area and secure third countries in accordance with the data protection law.

A.17 Use of external communication services

Responsible for initiation:	ISK
Responsible for implementation:	IT users

(1) The IT systems of the University of Göttingen Foundation can be accessed via the Internet when external communications services (e.g., Skype, Teamviewer) are used.

(2) The use of such services is permitted only if the operational concepts for the data processed on the computer used and the used sub-areas of the infrastructure allow such use.

A.18 Use of private hardware and software

Responsible for initiation:	ISK
Responsible for implementation:	IT users

(1) Using private hardware and software in connection with the official data or IT infrastructure of the University of Göttingen Foundation is permitted only if the operational concepts for the respective data or sub-area of the infrastructure allow it.

(2) Using private devices in designated areas and at designated connections especially in libraries, connections for lecturers in lecture halls and seminar rooms, in student work areas or guest networks and generally in the eduroam and GuestOnCampus wireless networks of the University of Göttingen Foundation is expressly permitted.

(3) Admission of private devices in other parts of the infrastructure of the University of Göttingen Foundation necessarily presupposes that the end devices connected there meet the requirements of the catalogues of measures for basic IT protection of the Foundation University.

(4) A.16 must be observed when storing and processing official data on private hardware.

(5) The ISK must be informed in the event of loss of private hardware on which official data was stored. If personal data are affected by the loss, the DSM must also be informed.

A.19 Data backup and archiving

Responsible for initiation:	Specialists responsible
Responsible for implementation:	IT staff, specialists responsible

(1) Data must be protected against loss resulting from faulty operation, technical faults, etc. To do so, data backups (creating copies of the data on separate storage systems) must be performed on a regular basis.

(2) If storage on central servers with regulated data backup is not possible, the respective specialists responsible are responsible for data backups.

(3) In the case of central data backup, specialists responsible must learn about the applicable regulations for data backup frequency and procedure.

(4) The long-term archiving of academic data that is necessary for the implementation of the “Regulation of the University of Göttingen for ensuring good scientific practice” must be distinguished from a data backup for protecting data against loss. This must be ensured by specialists responsible.

A.20 Handling data storage devices

Responsible for initiation:	Specialists responsible
Responsible for implementation:	Specialists responsible

(1) Data storage devices must be stored in secure locations. Data storage device safes must be procured if necessary.

(2) Furthermore, data storage devices must be marked if the identification of the data storage device is not carried out by a different technical procedure.

(3) Data storage devices must be protected from damage during transport. Encryption is required for sensitive data.

A.21 Deletion and disposal of data storage devices und confidential papers

Responsible for initiation:	Specialists responsible
Responsible for implementation:	IT staff, IT users

(1) Data storage devices containing sensitive data must be securely deleted before being passed on to unauthorised persons. This can be done with suitable programmes or other suitable technical measures (e.g., with a device for magnetic flood erasure for hard disks and magnetic tapes).

(2) Data storage devices that need to be discarded or are defective must be rendered completely illegible if they contain or have contained sensitive data.

(3) More information can be obtained from the following authorities: GWDG, the Information Technology division of the UMG, the IT department of the University administration, the Data Protection Officer of the UMG.

A.22 Secure disposal of confidential papers

Responsible for initiation:	Specialists responsible
Responsible for implementation:	IT staff, IT users

(1) Papers containing confidential contents must be destroyed using a shredder. Alternatively, disposal can also be carried out centrally via a service provider.

(2) University regulations must be observed when the disposal is carried out via a service provider.

I. Measures for IT staff

I.1 Early consideration of information security issues

Responsible for initiation:	Competent management
Responsible for implementation:	IT staff, IT users

(1) Issues related to information security and data protection must be taken into account at the planning stage itself when new IT systems have to be procured or significant changes have to be made to IT procedures.

(2) Insofar as personal data is processed, the competent Data Protection Officer must also be involved from an early stage.

I.2 Definition of responsibilities and role separation

Responsible for initiation:	Specialists responsible
Responsible for implementation:	IT staff, IT users

(1) For each IT process, responsibilities must be clearly defined in the respective operational concepts. A role concept is required for all administrative applications that have to meet legal requirements and for applications that have a special protection requirement.

(2) Each person must be informed of the responsibilities assigned to him or her and of related provisions.

I.3 Documentation and description of IT procedures

Responsible for initiation:	ISK
Responsible for implementation:	IT staff, IT service providers

(1) Documentation and description must be prepared in order to ensure information security of an IT procedure. This particularly includes the following information:

(a) Purpose of the procedure

(b) System overview, network plan

(c) Interfaces to other procedures

(d) Data description

(2) Documentation, which at least includes the following points, must be prepared in order to ensure information security of an IT procedure:

(a) Delegation/deputisation regulations, particularly in the administration area

(b) Access rights

(c) Organisation, responsibility and execution of data backup

(d) Installation and release of software including software updates

(e) Purpose, release and use of self-created programs

(f) Instructions

(g) Work instructions for administrative and similar tasks

(h) All types of information security events that occur

(i) Emergency procedures

(j) Maintenance agreements

(k) Description of processing operations in accordance with Art. 30 GDPR

I.4 Documentation of information security events and incidents

Responsible for initiation:	ISK
Responsible for implementation:	IT staff, IT users

(1) Information security events and incidents must be documented by the competent IT staff and immediately reported to the ISK.

I.5 Regulations on order processing

Responsible for initiation:	Specialists responsible
Responsible for implementation:	Specialists responsible

(1) A written agreement is required for all IT procedures operated on behalf of the University of Göttingen Foundation. The responsibility for information security and the corresponding control options must be clearly assigned.

(2) Regulations of the GDPR (particularly Art. 28) must be observed if personal data is processed in the context of order processing. The Data Protection Officer of the University of Göttingen or the University Medical Center must be involved.

I.6 Standards for technical equipment and configuration

Responsible for initiation:	CIO
Responsible for implementation:	Specialists responsible, IT staff

(1) Standardisation of technical equipment and configuration should be sought in order to achieve an appropriate security level for IT systems. The ISB and professionally qualified IT service providers advise the operators of IT procedures.

I.7 Provision of central IT services

Responsible for initiation:	CIO
Responsible for implementation:	IT service providers

(1) Central IT services, such as user service, data backup measures, storage of data on central file servers, execution of programs on application servers, software distribution, software updates, software inventory and software license management, as well as email, support smooth IT use and improve the level of information security. Corresponding services must be offered centrally as far as possible.

(2) Protection measures against malware must also be centralised.

(3) For installation and inventory tools that are used across the network and for remote access, for example by the user service, special protection measures must be taken to prevent misuse. Users must be informed before such tools are used.

I.8 Use of central services

Responsible for initiation:	Competent management
Responsible for implementation:	IT staff

(1) The central provision of essential IT services by IT service providers relieves the burden on the institutions of the University of Göttingen Foundation so that they can better fulfil their actual tasks. Improved information security is achieved by centralising IT services.

(2) The institutions of the University of Göttingen Foundation must use the central IT services. provided by IT service providers. They may operate their own IT systems only if the corresponding central IT services are not available for their tasks.

I.9 Delegation/deputisation

Responsible for initiation:	Competent management/specialist responsible
Responsible for implementation:	Competent management

(1) Delegation regulations are required for all tasks performed by the IT staff. Deputies must master all tasks required for this; work instructions and documentation must be made available to them.

(2) The delegation regulation must be mapped in the system and must not take place by sharing passwords. This does not apply to system-specific, non-personal user accounts (for example root on UNIX systems). In this case, the deputy must be able to access the password of the user account stored in a suitable place only when necessary.

(3) Compliance with the requirements for role separation must be ensured.

I.10 Qualification

Responsible for initiation:	Competent management/specialist responsible
Responsible for implementation:	Competent management

(1) The IT staff may work on IT procedures only after receiving adequate training.

(2) Training must also include the applicable security measures, legal framework conditions and data protection requirements.

(3) Continuous advanced training of the IT staff in all matters relating to their area of responsibility must be ensured.

I.11 Basic measures

Responsible for initiation:	Real Estate and Facilities Management/ISK
Responsible for implementation:	Real Estate and Facilities Management

(1) A large number of structural and technical specifications must be observed to secure the IT infrastructure. Technical measures for infrastructure are described in BSI's (Federal Office for Information Security)[4] basic protection compendium for example. The fire brigade is responsible for fire protection and the Security/Environmental Protection staff unit of the University is responsible for other security infrastructure. The following measures must be observed for securing the IT infrastructure:

(a) Uninterruptible Power Supply (UPS)

(b) Fire protection

(c) Protection against water damage

(d) Protected cable routing

I.12 Securing server rooms

Responsible for initiation:	ISK
Responsible for implementation:	Real Estate and Facilities Management

(1) All IT systems with typical server function, including peripheral devices (consoles, external disks, drives, etc.), must be installed in separate, specially secured rooms.

(2) Access to these rooms by unauthorised persons must be reliably prevented.

(3) It is necessary to determine which server rooms cleaning and external service staff are permitted to enter only under supervision.

(4) The doors shall only be openable by means of suitable locking systems and shall close automatically; the keys used must be copy-protected.

(5) Key management requires special regulations that prevent keys from being handed over to unauthorised persons. Access must be limited to those who need access to the rooms due to the nature of their work.

(6) Depending on the need for protection and external conditions (public accessibility, position towards the street, etc.), special constructural measures, such as burglar-proof windows and doors, motion detectors, etc., must be provided to prevent forced entry.

(7) Centralised server rooms are desirable.

[4] See https://www.bsi.bund.de/grundschutz

I.13 Securing network nodes

Responsible for initiation:	Real Estate and Facilities Management/IT service providers
Responsible for implementation:	Real Estate and Facilities Management

(1) Networking infrastructure (switches, routers, wiring Centers etc.) must be set up in closed rooms or in closed cabinets in areas that are not accessible to public. These rooms or cabinets must be protected against unauthorised access and destruction. Measure (I.12) shall apply accordingly.

I.14 Cabling and wireless networks

Responsible for initiation:	Competent management
Responsible for implementation:	IT service providers, Real Estate and Facilities Management, IT staff

(1) The network infrastructure must be clearly structured and its documentation must be up-to-date and complete.

(2) Requests for extensions and changes to the network infrastructure (e.g., cabling, network distributors, wireless networks) must be coordinated with the relevant ISC and submitted to the relevant central bodies (Real Estate and Facilities Management for the University, G3-7 for the University Medical Center).

I.15 Induction and supervision of external staff

Responsible for initiation:	ISK
Responsible for implementation:	ISK, IT service providers, Real Estate and Facilities Management depending on the client

(1) External staff that has to work in secure rooms that have IT equipment (e.g., server rooms) must be supervised and the work must be documented.

(2) Supervision may be waived for regularly deployed, instructed and committed external personnel. The exceptions have to be documented.

(3) Non-specialist persons (e.g., cleaning staff), who needs to access secure IT rooms, must be instructed on how to handle the IT equipment.

(4) If there is a possibility of the external staff accessing sensitive data, even if during remote maintenance, they must be obliged to maintain data secrecy. They must also be obliged to maintain data secrecy when accessing personal data. Contracts for maintenance and service must then be concluded in accordance with Art. 28 GDPR.

I.16 Procurement, software development

Responsible for initiation:	ISK
Responsible for implementation:	Specialists responsible

(1) The procurement of software and hardware and the development of software must be coordinated with the competent ISK. In the process, standards according to I.6 and state

of the art security measures must be observed. The specialist and technical requirements must be specified in advance.

I.17 Controlled use of software

Responsible for initiation:	ISK
Responsible for implementation:	IT staff

(1) Only software that is required to perform official tasks may be installed on the IT systems of the University of Göttingen Foundation.

(2) Using software from the Internet, or launching software received via email, is permitted only if it is ensured that this software does not pose a risk to the IT systems or data network.

(3) Consent of the competent management must be obtained in case of doubt. The ISB can advise the management if needed.

I.18 Separate development environment

Responsible for initiation:	ISK
Responsible for implementation:	IT staff

(1) The development or customisation especially of server-based software must not be carried out in the production environment. Transferring the software from development to production facilities requires the approval of the competent specialists responsible.

I.19 Protection against malware

Responsible for initiation:	ISK
Responsible for implementation:	IT staff

(1) A virus scanner, which automatically checks all incoming data and files, must be installed on all workstation computers. The virus scanner, including signatures, must be updated regularly (if possible, in an automated manner).

(2) The use of virus scanners must be checked for all other IT systems (e.g., servers, measurement and control computers) and carried out as far as appropriate and technically possible.

(3) If malicious program code is detected on a system, this must be reported to the competent ISC and the outcome of the measures taken must be documented.

(4) A malware search must be carried out on all IT systems at risk at regular intervals as well as when there is a specific requirement or suspicion; the results must be documented.

(5) Software updates provided by manufacturers to eliminate security gaps must be installed promptly, provided that no problems with the update are apparent.

(6) Operating systems and applications for which manufacturers no longer provide software updates must not be used on the data network. If, for overriding reasons, the continued usage of such systems cannot be avoided, these systems must be documented, and

operational concepts must be developed for their continued usage and submitted to the ISB for his/her statement.

(7) Applications, especially network applications such as mail programs and web browsers, must be configured securely.

(8) Applications are to be executed with the minimum required rights in the operating system.

I.20 Interfaces for external data storage devices in case of increased protection requirement

Responsible for initiation:	Specialists responsible
Responsible for implementation:	IT staff

(1) If there is an increased protection requirement, all external accesses to the PC (e.g., CD drives, USB ports, removable storage devices, wireless connections) must be removed, blocked or controlled if they are not required for official tasks. The possibility of using application servers and drive-less workstations or terminals is to be examined.

(2) Access to the computer BIOS must be protected by a password.

I.21 Failure safety

Responsible for initiation:	ISK
Responsible for implementation:	IT service providers, IT staff

(1) Failure safety measures must be taken in accordance with the respective requirement.

(2) IT systems that are necessary to maintain orderly operation must be kept adequately available by means of fallback solutions (e.g., through redundant system design or use of similar devices) or maintenance contracts with short response times.

I.22 Use of anti-theft devices

Responsible for initiation:	ISK
Responsible for implementation:	Real Estate and Facilities Management, IT staff

(1) To reduce the risk of theft, anti-theft devices must be used at all places where things of significant value need to be protected and where other measures ((e.g., suitable access control to the workstations (see A.6)) cannot be implemented or where there is a particular risk of theft (e.g., due to public traffic or fluctuation of users).

(2) Data storage devices containing valuable research data and personal data must be adequately protected.

I.23 Personal user accounts (authentication)

Responsible for initiation:	ISK
Responsible for implementation:	IT staff

(1) The following must be observed in addition to measure A.9:

(2) Each person should only be assigned one user account. The assignment of several user accounts to one person within an IT system should take place if special roles are mapped

and special rights are assigned via the additional accounts. The additional accounts should also be allocated per person.

(3) The creation and activation of a user account may only take place in a regulated procedure. The creation and activation must be documented.

(4) Pre-installed standard accounts are to be deactivated or deleted if not required.

I.24 Administrator accounts

Responsible for initiation:	ISK
Responsible for implementation:	IT staff

(1) Administrators receive a personal administrator account for their tasks. The use of this administrator account must be restricted to the tasks for which administrator rights are required. User accounts without administrator rights must be used for non-administrative work.

(2) Predefined administrator accounts must be renamed as far as technically possible so that their meaning is not immediately evident.

I.25 Administration of user accounts upon entry, change or withdrawal

Responsible for initiation:	Competent management
Responsible for implementation:	Competent management, superior of the person leaving the organisation

(1) In the organisational procedure, a process for the administration of user accounts and user rights must be reliably established when a person joins, is reassigned within the organisation or leaves.

(2) In the event of an organisational change or if a person leaves, the competent management has to decide on the use of the official data that is assigned to that person’s user account.

(3) All authorisations for admission and access rights set up for the reassigned or leaving person must be withdrawn or deleted.

(4) In exceptional cases, if user accounts for an IT system have been shared between several persons, the password must be changed after one of the persons is reassigned or leaves.

I.26 Passwords

Responsible for initiation:	ISK
Responsible for implementation:	IT staff, IT users
Responsible for implementation:	IT staff, IT users

(1) In addition to the provisions laid down in measure A.12, IT staff must also observe the following:

(a) For privileged accounts, more stringent requirements must be set for password strength (complexity and/or length of the password).

(b) Preset passwords (e.g., set by the manufacturer when systems are delivered) must be immediately replaced with individual passwords.

(2) If technically feasible, the following framework specifications must be observed:

(a) The technical options for enforcing compliance with password guidelines must be activated.

(b) Every user must be able to change their own password at any time.

(c) Passwords must be assigned for the signup of new users. These passwords must be changed after being used once.

(d) The number of incorrect login attempts on a system within a period must be limited. If no other algorithms are available for the limitation, the limitation can be done by blocking the account, which can either only be lifted by the system administrator or is time-limited.

(e) During authentication in networked systems, passwords may only be transmitted in encrypted form. Only one-time passwords are used in networks in which passwords have to be transmitted without encryption.

(f) When a password is entered, it must not be displayed on the screen.

(g) Passwords must be securely stored in the system, e.g., by means of one-way encryption.

(h) Repetition of old passwords during a password change must be prevented by the IT system (password history).

(3) If the system itself cannot enforce compliance with password guidelines, suitable organisational measures must be taken to inform users of the password guidelines and to oblige them to comply with these.

(4) Deviations from the rules mentioned in Sentences (1) and (2) are permitted only for systems for which special password guidelines expressly allow this.

(5) The IT staff must check the use of alternatives and extensions (two-factor procedure) for authentication by means of passwords particularly where such procedures should or must guarantee increased protection requirements.

I.27 Access rights

Responsible for initiation:	Competent management, ISK
Responsible for implementation:	IT staff

(1) Access rights determine which persons are authorised to use IT systems, IT applications or data within the scope of their functions. The user may work with only those access rights that are intended for the performance of his or her tasks.

(2) The procedures for granting access rights as well as the documentation of the granting and of the rights must be defined technically and organisationally.

(3) It is necessary to examine the extent to which access authorisation can be limited to specific end devices.

(4) It is also necessary to examine the extent to which access authorisation can or must be limited to specific times (e.g., restricted to normal working hours).

(5) For users with privileged rights, especially for administrator accounts, access must be limited to the required systems (usually the server and end devices or applications in question).

(6) For all administrative applications that have to comply with legal requirements (data protection, commercial code, etc.), the access rights for individual users are granted and modified when the users submit a written request. Separation of roles must be taken into account when granting access rights; administrators are not allowed to manage their rights themselves.

I.28 Locking, logging out and shutting down

Responsible for initiation:	ISK
Responsible for implementation:	IT staff, IT users

(1) The following applies in addition to (A.6):

(2) As far as technically feasible, the activation of automatic locking must be configured centrally.

I.29 Teleworking

Responsible for initiation:	Competent management
Responsible for implementation:	IT staff, IT users

(1) The following applies in addition to A.13:

(2) Appropriate technical measures must be taken to ensure that

(a) confidentiality and integrity of the data transferred during the communication between the external workplace and the office are guaranteed,

(b) only authorised persons can access official data from home,

(c) official data at the external workplace is treated confidentially and

(d) the entire process of external work meets existing revision security requirements.

(3) The existing company agreements[5] must be observed when setting up and working on external workplaces.

(4) If personal data is processed during external working, the Data Protection Officer must be involved in the approval process.

[5] See appendix "Related documents"

I.30 Need for logging and monitoring

Responsible for initiation:	ISK/specialist responsible
Responsible for implementation:	IT staff

(1) Appropriate logging, auditing and inspection are essential aspects of information security. An evaluation of such protocols using suitable tools makes it possible to ascertain whether, for example, the bandwidth of the network corresponds to the current requirements or whether systematic attacks on the network can be identified.

(2) Depending on the use of an IT procedure, adequate logging measures must be taken to ensure data security, data protection and inspection capability.

(3) Depending on the data logged, the evaluation of the log files must be coordinated with the Data Protection Officer, the staff council and the Internal Auditing department.

I.31 Logging on servers and in case of application programs

Responsible for initiation:	ISK/specialist responsible
Responsible for implementation:	IT staff

(1) Depending on the capabilities of the operating system, the services and the applications, all access attempts, both successful and unsuccessful, must be logged automatically.

(2) Changes to the parameters of system services and application programs, the booting and shut down of the IT system or system services as well as security-related events must be logged.

(3) The principle of purpose limitation as per Art. 5 Section 1 Letter b) GDPR and the principle of data minimisation as per Art. 5 Section 1 Letter c) GDPR as well as the storage limitation according to Art. 5 Section 1 Letter e) GDPR must be observed.

(4) If technically possible, the logs must be stored on dedicated servers.

(5) They must be evaluated regularly and immediately after they are created. Hereby must be ensured that only those persons, who need the logs to complete the tasks assigned to them by the competent body, have access to them.

I.32 Logging of administrative activities

Responsible for initiation:	ISK
Responsible for implementation:	IT staff

(1) Depending on the protection requirement of the procedure or of the data to be processed, administrators must be obliged by organisational regulations (instructions, etc.) to log the activities they carry out within the scope of their tasks. As far as possible, logging should take place automatically in the system.

I.33 Secure network administration

Responsible for initiation:	ISK
Responsible for implementation:	IT staff, IT service providers

(1) It must be regulated in operating and security concepts and ensured that network administration is carried out by designated IT staff only.

(2) Active and passive network components and servers must be protected against unauthorised access.

(3) Network documentation must be kept locked and protected from unauthorised access.

I.34 Network monitoring

Responsible for initiation:	ISK, IT service providers
Responsible for implementation:	IT staff, IT service providers

(1) Suitable measures must be taken to detect and localise overloading and faults in the network at an early stage.

(2) It must be regulated in operating and security concepts and verified that the tools and data used for this purpose can be accessed by authorised persons only.

(3) The group of authorised persons must be limited to the necessary number.

I.35 Controlled network accesses

Responsible for initiation:	ISK, IT service providers
Responsible for implementation:	IT staff, IT service providers

(1) Unauthorised use of network access must be prevented by means of organisational and technical measures.

I.36 Division into areas based on varying protection requirements

Responsible for initiation:	ISK
Responsible for implementation:	IT staff, IT service providers

(1) The data network must be structured such that different IT systems have different sub-networks commensurate to their respective protection requirements.

(2) IT systems with varying protection requirements must not be operated in the same sub-network. This way, IT systems with a higher protection requirement are not endangered by insufficiently secured systems in the same subnet or by insufficient protection measures at network ports. Conversely, this also ensures that the use of IT systems with a lower protection requirement is not made unnecessarily difficult because other IT systems with higher protection requirements in the same subnet have to be taken into account.

I.37 Controlled communication channels

Responsible for initiation:	ISK
Responsible for implementation:	IT staff, IT service providers

(1) All communication between the various sub-networks of the University of Göttingen Foundation or with external parties may only take place via controlled channels that are managed by special protection systems (Firewall, proxy, etc.).

(2) Protection systems must be configured such that only desired communications are possible (whitelisting), thus preventing unnecessary communications and minimising attack targets.

(3) Besides the network connections of the University of Göttingen Foundation, the installation and operation of other communication connections are generally not permitted. If the installation of other communication channels cannot be avoided due to special circumstances (e.g., operating a modem for remote maintenance purposes), this requires prior approval of the network operator. I.15 must be observed for access by external service providers.

I.38 Secured transmission procedure

Responsible for initiation:	ISK
Responsible for implementation:	IT staff, IT service providers

(1) If technically feasible, encrypted transmission procedures must be used for electronic communication.

(2) Sensitive data must be transmitted in encrypted form.

(3) Encrypted transmission procedures must be used for administrative activities and remote maintenance.

I.39 Organisation of data backups

Responsible for initiation:	Specialists responsible
Responsible for implementation:	IT staff

(1) Data backups must be carried out according to a documented data backup concept that is in line with the protection requirement of the data to be backed up. The data backup concept includes all data backup regulations (which data is backed up by whom, using which method, when, how often and where).

(2) In the case of personal data, the required or permitted retention periods must be observed.

(3) Original data and backup copies must be kept in separate fire-protected areas.

(4) As a rule, data must be stored on central file servers, on which a central data backup takes place on a regular basis. If storage on central file servers is currently not possible, a suitable data backup must be set up for the local system.

(5) In order to minimise recovery times, the extent to which system and program areas are also backed up along with data must be checked.

(6) The configurations of all active network components must be included in a regular data backup that takes place at least once daily.

I.40 User information for data backups

Responsible for initiation:	Specialists responsible
Responsible for implementation:	IT staff

(1) All users, who can use data backup systems, must be informed about the data backup regulations so that they can point out deficiencies (e.g., unsuitable time interval for their needs) or make individual additions if necessary.

I.41 Verification of data backups

Responsible for initiation:	Specialists responsible
Responsible for implementation:	IT staff

(1) The consistency of data backup runs must be ensured by checking the readability of the data backup. Data backups must be restored on a test basis at least once a year to a reasonable extent.

I.42 Deletion and disposal of data storage devices and confidential documents

Responsible for initiation:	Specialists responsible
Responsible for implementation:	IT staff, IT users

(1) The following applies in addition to A.21:

(2) Repairing of damaged data storage devices on which sensitive data is stored is permitted only in particularly justified exceptional cases.

(3) If data storage devices can only be repaired by external service providers, the contractor must be obliged to maintain data confidentiality. The obligation must be a part of the written agreement.

I.43 Secure disposal of confidential documents

(1) The following applies in addition to A.22:

(2) DIN 66399 must be observed when procuring shredders.

(3) If documents have to be disposed via a service provider, it must be ensured that the contractor is certified for this. The contractor must be obliged to log the destruction.

Addendum 3 Glossary

Application

A computer program or a set of interacting computer programs that are used to execute IT procedures.

Application server

A server, on which applications (instead of a workstation computer) are running.

Dataset

A set of digitally stored data.

Data archiving

Is data storage on a system that is intended for long-term storage of data.

For research data in particular, data archiving requires the storage of additional data (metadata) to describe the data content and data format.

Data backup

Creation of additional copies of data on separate data storage devices as protection against data loss through hardware damage or accidental deletion.

Data backups usually protect against loss through accidental deletion only for a limited time because data backup procedures usually also delete copies of deleted data from the data backup data storage device after a predefined time.

Data storage

Is the process in which data is written on a data storage device.

Data storage device

Media on which data is stored, e.g., hard disks, disks, USB sticks, memory cards.

Increased need for protection

Summary for high or very high protection needs as opposed to normal protection needs.

Threat

a) Current threat:

A threat in which the impact of the damaging event has already begun or in which this impact is imminent immediately or in the very near future with a probability bordering on certainty.

b) Significant threat:

A threat to an important legal asset such as life, health, freedom, not insignificant assets and other goods protected by criminal law.

Information security events

(According to ISO 27000) Detected occurrence of a system, service or network condition that indicates a possible violation of the information security guideline, the failure of measures or a previously unknown situation that could be security-relevant.

Information security incidents

(According to ISO27000) Individual or a series of undesirable or unexpected information security events with a significant probability that business processes will be compromised and information security will be threatened.

Initiation

Under "Responsible for initiation", the catalogue of measures for basic IT protection specifies which person is responsible for starting and implementing a measure.

IT users (german: IT-Anwender)

Users of an IT system with a non-privileged user account who only use computers, operating systems and applications provided by other entities to process their data and to carry out their tasks.

IT staff (german: IT-Personal)

IT staff includes all members of the University of Göttingen Foundation who are entrusted with the performance of tasks in the planning, support, maintenance and administration of IT systems that go beyond the mere use of IT systems. Here, it is irrelevant whether these people perform these activities as their main job. In particular, all persons with rights to change the installation of operating systems and applications on IT systems are considered as IT staff.

IT system

An IT system or information technology system is understood as an electronic data-processing system. This includes any computer from smartphones to mainframes, but also combinations of individual devices to form a composite system for joint data processing.

IT procedure

Defined procedure for electronic data processing including electronic communication.

Network operators

Institutions and their employees entrusted by the University of Göttingen Foundation with the installation and operation of data networks. The network operators of the University of Göttingen Foundation are:

GWDG for the University and the Information Technology division for the UMG.

Users (german: Nutzerinnen und Nutzer)

People who use an IT system for electronic data processing.

User ID

The name assigned to a user in an IT system.

User account

A representation of a user within an IT system, which is usually associated with a user ID and login data for the system and through which objects and rights in the IT system can be assigned to the user.

User account, privileged

Special user account that is associated with elevated rights in the IT system. This particularly also includes user accounts that have rights to install or modify the operating system or applications.

Risk acceptance

(According to ISO 27000) An informed decision to bear a specific risk.

Risk mitigation

Mitigation of risks through measures that reduce the probability of occurrence or extent of damage.

Risk transfer

Transfer of risks to others (e.g., through insurance).

Risk avoidance

(According to ISO 27000) Avoiding a risk by deciding not to start or continue the activity that gives rise to the risk.

Sensitive data

Sensitive data within the context of this information security guideline is particularly

- Personal data pursuant to Art. 4 No. 1 GDPR (e.g., student data, staff data, patient data),
- Business data (e.g., financial data, confidential internal information/protocols),
- Patents as well as
- in individual cases, other data that has been classified as sensitive by an IT user (e.g., research results).

Transfer of data

Copy processes from one IT system to another via data networks.

Login data

Information that is used to verify a user's identity when the user accesses his/her user account, for example passwords and PINs, cryptographic keys or biometric data.