Current version dated May 9, 2025
(Amtliche Mitteilungen I Nr. 17 dated May 8, 2025, p. 312)

Unofficial version for reading

(English translation provided for informational purposes. If the English and German versions allow different interpretations, the German version is legally binding. Note: This text uses the German abbreviations for the roles defined in this policy.)

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

– Information Security Policy / Informationssicherheitsrichtlinie (ISRL) –

.

Table of Contents

Section I: Principles

§ 1 Subject matter and scope

(1) The information security policy defines responsibility structures, assignment of tasks, cooperation between those involved and content-related specifications in the university-wide information security process and in information security risk management (Appendix 3).

(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 objectives

(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 and their effects to the greatest extend. 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 and information security risk management

(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) The protection requirement of all information must be determined according to the categories normal, high and very high; where:

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

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

(c) “Very high protection requirement” 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.

(4) Appendix 3 contains additional requirements for information security risk management, including the assignment of tasks, the definition of criteria for assessing the need for protection, the effects of damage, the probability of occurrence and the risk classes.

(5) A further risk analysis is not necessary when implementing the measures in accordance with Addendum 2:

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). The overall responsibility includes responsibility for information security risk management; Supplementary requirements for information security risk management are contained in Appendix 3.

(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 management in charge of the respective unit specified in Addendum 1: (hereinafter called: management in charge) 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) attent to 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.

(4) As an IT service provider for the university, the GWDG is contractually obliged to comply with the information security guidelines.

§ 8 Management in Charge

(1) The management in charge as specified in Addendum 1: can, in its respective area 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 area of responsibility, the management in charge is responsible for:

a) appointing an Information Security Coordinator according to Section (3),

b) appointing specialists responsible according to Section (5),

c) deciding on the respective operating concepts according to Section (6),

d) deciding on the further handling of information security incidents according to § 18,

e) the performance of tasks within the framework of information security risk management in accordance with Appendix 3.

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

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

(5) The competent management can appoint an appropriate number of specialists responsible for the information assets, 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 operating concepts including the revised versions after reviews based on the opinion of the ISK and upon getting an approval from the ISB and is responsible for the risks taken over 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. ISC'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 operation concepts,
   (e) Immediate submission of operationconcepts to the ISB,
   (f) Gathering and providing operationconcepts 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 § 18 for the competent management,
   (h) Execution of tasks within the framework of information security risk management in accordance with Appendix 3.

(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 information assets, datasets, IT procedures, IT systems and infrastructure assigned to them. This particularly includes the following tasks:
   (a) Identification of the protection requirement for information assets, datasets, 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, whereby at least annual intervals must be specified in the area of the critical infrastructure operated by the UMG,
   (d) Initiating and controlling the implementation of the measures laid down in an operational concept including the risk treatment plan, particularly also when using external IT service providers (e.g., order processing).

(2) The specialists responsible are also responsible for carrying out the tasks within the framework of information security risk management in accordance with Appendix 3.

(3) 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.

(4) 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 operational 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 operationalconcepts.

(d) Approving operational concepts of the units including the revised versions after review by the specialists responsible; 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 operationalconcepts,

(f) Assessing information security incidents and deriving structural and conceptual recommendations in accordance with § 18,

(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.

(h) Execution of tasks within the framework of information security risk management in accordance with Appendix 3.

(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 § 18 Section (4).

(c) Preparing an information security report insofar as it concerns

(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.

(d) Execution of tasks within the framework of information security risk management in accordance with Appendix 3

§ 13 Data Protection and Information Security Advisory Council / Datenschutz- und Informationssicherheits-Beirat (DIB)

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

(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) the CIO of the university and UMG,

(g) the head of the audit department,

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

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

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

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

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

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

(2) A substitution must be appointed for each member in accordance with paragraph 1

(3) 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.

(4) 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) Recommendation of proposed changes the information security policy and overarching concepts or advisories on information security and data protection.

(5) The DIB is also responsible for carrying out the tasks within the framework of information security risk management in accordance with Appendix 3

§ 14 External service providers

(1) External IT service providers who are commissioned to carry out tasks on IT systems must be obliged to comply with the information security guidelines, to the extent that this is appropriate taking into account the need for protection.

(2) Compliance with the information security guidelines by the external IT service providers must be checked by the responsible IT staff of the ordering party.

(3) External IT service providers are obliged to inform clients of risks that arise in the IT system as a result of the services they provide.

Section III: Content-related specifications

§ 16 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 operational 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)

§ 17 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.

§ 18 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 in guidelines, overarching information security concepts and operational concepts and, following a statement from the ISM, the responsible ISK, the responsible management and the DIB, prepares recommendations for for the Presidential Board, the Management Board, the management in charge and the ISK.

(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 must, in a guideline document, regulate further details on how to handle information security incidents.

§ 19 Threat intervention

(1) In order to avert a current threat to information security, the decentralized 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. The necessary measures can also be initiated by the ISB or the ISM as soon as they recognize current threats.

(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 ISC after the necessary IT security measures have been carried out.

Section IV: Final provisions

Entry into force and expiry

(1) The new version of the information security policy of the University of Göttingen/University of Göttingen Public Law Foundation (Information Security Policy - ISRL -) will come into force on the day after its publication in the Official Announcements I of the University of Göttingen.

(2) (2) At the same time, the information security guidelines of the Georg-August University Göttingen/Georg-August University Göttingen Foundation of Public Law (Information Security Guideline - ISRL -) in the version announced on 24.01.2020 (AM 04/2020 p. 46 ff.) 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, unexpected, inexplicable or unusual behaviour of applications that have run error-free so far, hardware failures, intrusion by unauthorised persons, manipulations, virus attacks etc.) to the responsible IT staff in order to clarify the problem and, if necessary, report an information security incident to the responsible ISK or the responsible management.

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 responsible 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) Any additional data collected as a result of the measure or stored beyond the deletion period 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 or used 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 or during mobile working workstations must be set up by placement or privacy screens 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 creation of user accounts that are to be used jointly by several people (shared function accounts) is only permitted if such accounts are indispensable for the fulfillment of tasks.

(3) 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.

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

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

(6) 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 a user account assigned to the person.

(2) The passwords used for the use of IT systems of the University of Göttingen Foundation (in the following: official passwords) must not be identical or similar to passwords used for the usage of IT systems not belonging to the University of Göttingen Foundation. The differences between the passwords must be significant, and in particular there must be no systematic connections that could lead to the other being derived from one password.

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

(a) Passwords must be kept secret.

(b) Passwords for personal user accounts may not be shared with other people.

(c) The following applies to passwords for user accounts that are to be shared by several people (shared functional accounts):

(i) The password of a functional account may only be shared with those involved in the function.

(ii) If a person who knows the password of a functional account leaves, the password of the functional account must be changed.

(d) A password must be entered unobserved.

(4) The following rules apply to storing passwords in IT systems:

(a) Storing official passwords in applications, especially browsers, or on programmable function keys is principally not permitted.

(b) The following exemptions to the prohibition on storing official passwords apply:

(iii) Saving a work password in the Eduroam configuration is permitted on desktop and laptop systems and on smartphones.

(iv) It is permitted to store official passwords for email access on a smartphone.

(v) The storage of official passwords in a password manager with a secure master password in accordance with the regulation on password strength in paragraph (7)is permitted. Longer passwords as master passwords are recommended.

(5) The following rules apply to writing down passwords on paper

(a) Writing down of passwords on paper must be avoided.

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

(c) Leaving a password in a sealed envelope in a safe under the supervision of the entity for which the account holder works is permitted

(6) Rules for changing passwords:

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

(b) Initial passwords must be changed immediately before using the services.

(c) Old passwords may not be reused.

(d) New passwords and previously used passwords must differ significantly; in particular, there must be no systematic connections through which the new password could be derived from the previous password.

(7) Unless other rules have been explicitly enacted for certain passwords, the following password requirements apply:

(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 at least 10 characters is recommended.

(c) Each 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).

(8) 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).

(9) 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, mobile working and home office, 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) 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] See appendix “Related documents”

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

(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.

(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.

(6) The synchronization of emails on private devices and the associated data storage is permitted as long as it is not expected that emails contain particularly sensitive content in the sense of data protection or other confidentiality requirements. Synchronization on private devices is not permitted for email accounts where, due to the function of the account holder, it is expected that emails contain particularly sensitive content in terms of data protection or other confidentiality requirements.

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 or general instructions or service agreements 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 GuestOn-Campus 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 is affected by the loss, the ISK must be informed so that the ISK informs the responsible data protection officer

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) Papers with confidential content must be destroyed using a document shredder that meets the protection requirements. Alternatively, disposal can also be carried out centrally via a service provider.

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

(5) 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.

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.

(2) Conflicts in task assignments and areas of responsibility should be prevented by separating roles. In particular, for all administrative applications that must meet legal requirements and applications that require increased protection, a role concept must ensure the separation of roles.

(3) 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

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

(f) Access rights

(g) Organisation, responsibility and execution of data backup

(h) Installation and release of software including software updates

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

(j) Instructions

(k) Work instructions for administrative and similar tasks

(l) All types of information security events that occur

(m) Emergency procedures

(n) Maintenance agreements

(o) 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

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

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.

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 of user accounts that are to be used jointly by several people (shared function accounts) is only permitted if such accounts are indispensable for the fulfillment of tasks.

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

(5) 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 increased requirements for authentication procedures have to be imposed. Multi-factor authentication should preferably be enforced here. If this is not technically possible, at least an increased password strength (complexity and/or length of the password) must be decreed and enforced as far as technically possible..

(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) should be taken to detect password compromise.

(f) 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.

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

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

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

(j) For usage scenarios with different security requirements (e.g. accounts for daily work versus accounts for administration activities), different passwords or authentication procedures should be used.

(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 use of alternatives and extensions (multi-factor techniques) for authentication using passwords must be used to the extent that it is technically feasible where such techniques should or must ensure an increased need for protection. For applications with normal protection requirements, the use of multi-factor techniques should be examined and used if possible.

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, mobile working and home office

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.

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

[5] See appendix “Related documents”

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 should 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.

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

(5) 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.

V. Measures for administration and management

V.1 Checking when hiring personnel

Responsible for initiation:	Responsible management
Responsible for implementation:	managers, human resources department

(1) Qualifications and skills should be checked before employment

(2) A review of the information also serves to check its trustworthiness.

(3) Additional checks should be carried out (e.g. through police clearance certificates) for personnel who are subject to special trustworthiness requirements due to their intended activities.

V.2 Instruction upon hiring

Responsible for initiation:	Responsible management
Responsible for implementation:	managers

(1) After being hired, it must be ensured immediately that the newly hired personnel are appropriately instructed in the information security policy, in particular in the relevant catalogs of measures, for the assigned tasks and are obliged to comply with them.

(2) It must be ensured that newly hired personnel and personnel whose task assignment has been changed are instructed in the operational concepts that are relevant to the assigned tasks.

(3) Special authorizations should only be granted if appropriate instruction has been given and competence for the assigned task has been ensured.

V.3 Regular training of staff

Responsible for initiation:	Responsible management
Responsible for implementation:	managers

(1) Basic training on information security should take place regularly as mandatory classroom training or online training.

(2) Training for specific information systems should be carried out in accordance with the specifications of the respective operational concepts.

V.4 Regulations about substitutes

Responsible for initiation:	Responsible management
Responsible for implementation:	managers

(1) Managers must ensure that appropriate substitute arrangements are in place for all areas of responsibility.

(2) Substitute arrangements must be documented.

Addendum 3: Specifications for information security risk management

1 Principles

This appendix supplements the information security policy with the provisions on risk management in information security.

Information security risk management contributes to the university's overall risk management. Risks identified in information security risk management are incorporated into this in accordance with the regulations of the overall risk management, in particular the risk management concept of the Georg-August University (without UMG) . [1]

The principles and objectives of information security listed in the information security policy are assumed here. In order to achieve these objectives, the information security policy defines an information security process and sets out principles and distribution of tasks in risk management. The aim of this appendix is to define methods for risk management and criteria for risk assessment in addition to the information security policy and to present the organizational structure and the operational structure for information security risk management resulting from this and from the information security directive.

In the introduction, the appendix describes the organizational structure by taking up the role models of the information security policy and highlighting the tasks of the respective roles in information security risk management defined there.

The appendix then defines the risk analysis methodology to be used, by specifying the principles of information security risk management, in particular the methods and criteria of risk identification, risk analysis, risk assessment, risk treatment and risk acceptance.

Finally, the operational structure is derived and presented from the organizational structure and risk methodology.

The system is based on risk management standards, e.g. ISO/IEC 27005 [2], ONR 49000 to 49002-2 [3], [4], [5], [6] and the BSI standard 200-3 [7].

The appendix takes particular account of the framework conditions resulting from the BSI law for the critical infrastructure in the healthcare system operated by the Göttingen University Medical Center as well as the DIN EN 80001 standard for the consideration of networked medical devices [8].

2 Organizational structure

The organizational structure of information security is described in the information security policy. The roles defined in the information security policy are also assigned tasks for information security risk management. These are supplemented here with a focus on information security risk management.

The roles of the risk officers for the university's overall risk management are also listed in accordance with the university's risk management concept [1].

2.1 Presidential Board and Management Board

The Presidential Board of the University and the Management Board of UMG have overall responsibility for information security in their respective areas. This overall responsibility includes responsibility for information security risk management. The Presidential Board and Management Board are responsible for defining and coordinating the tasks, competencies, responsibilities, controls and communication channels associated with information security risk management, as well as defining appropriate risk management and risk controlling processes and related reporting obligations.

2.2 Information security officer (ISB)

The ISB controls the university-wide information security process of the foundation university on behalf of the Presidential Board and Management Board, including the information security risk management processes.

The role includes the role of Information Security Risk Manager.

The ISB contributes a report on information security risks to the annual information security report to the Presidential Board and Management Board. In the area of critical infrastructure operated by UMG, an additional half-yearly report must be prepared by the ISB to the Management Board on essential risks

2.3 Management in Charge

The management in charge is the risk owner.

2.4 Specialist responsible

As part of information security risk management, the specialists responsible support the management in charge in identifying all of the information assets as risk objects. Operational concepts in the area of the critical infrastructure operated by UMG must provide for at least annual reviews and, if necessary, updates by those responsible.

2.5 Information security coordinators

As part of information security risk management, the information security coordinators support the management in charge in identifying all of the information assets as risk objects and are involved in the creation of operational concepts by commenting on the operational concepts drawn up by the specialists responsible.

2.6 Risk Officers

For the university the role of the risk officer is defined in the risk management concept [1]. As part of information security risk management, the risk officers are responsible for reporting information security risks as part of the overarching risk management. They obtain the necessary information on information security risks from the management in charge (unless the management in charge is simultaneously the risk officer).

3 Methodology for risk analysis

3.1 Preliminary remarks

This chapter describes the methodology for risk analysis (risk methodology) for information security risk management at the Göttingen Foundation University.

Risks are identified by considering possible threats and the associated damage effects and probabilities of occurrence for damages. Classifications into risk classes are derived from this. In addition to the classification into risk classes, the risk methodology of the University of Göttingen considers classifications according to protection needs and criticality.

To assess the effects of the damage, different damage scenarios are considered for different information security objectives. The basis for determining the effects of the damage and the probability of occurrence is the consideration of threats, which in turn arise from the combination of basic threats and vulnerabilities.

The above terms are explained below and connections are presented. Specifications for classifications are made in the description of the process organization (Chapter 4) or in the supplementary information (Chapter 5).

3.2 Risk identification

3.2.1 Damage scenarios

To systematically determine the effects of the damage, various damage scenarios are considered. Based on BSI standard 200-1 [9] the following damage scenarios are considered in the information security risk management of the Göttingen Foundation University:

- Impairment of the ability to perform tasks (so-called performance fulfillment according to ONR 49002-2 [6]),
- impairment of the physical integrity of a person,
- negative internal or external impact (so-called reputation according to ONR 49002-2 [6]),
- Impairment of the right to informational self-determination,
- financial consequences,
- Violations of laws, regulations or contracts.

Patient safety and treatment effectiveness are essential objectives for patient care in the UMG. The impairment of the achievement of these objectives must be particularly taken into account in the damage scenarios “impairment of the physical integrity of a person” and “impairment of the ability to perform tasks”. The requirements of the DIN EN 80001 standard [8] for patient safety, effectiveness as well as data and system security are also covered by the above scenarios, in particular “impairment of the physical integrity of a person”, “impairment of the ability to perform tasks” and “impairment of the right to informational self-determination ”.

Data protection requirements are also integrated into the information security risk management process via the damage scenario “impairment of the right to informational self-determination”.

3.2.2 Information security objectives

In order to systematically determine the effects of the damage, effects on all information security objectives must be considered. Information security objectives in accordance with **Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.**of the Information Security Policy are:

- Confidentiality,
- Integrity,
- Availability.

For the critical infrastructure operated by UMG, the following objective must also be considered in accordance with the BSI Act:

- Authenticity, which means ensuring that the information was created by the specified source.

3.2.3 Effects of the damage

Effects of the damage are divided into five categories:

- insignificant
- minor
- noticeable
- critical
- catastrophic

The damage categories are assigned according to the table in Section 5.4for all damage scenarios from Section 3.2.1. The effects of threats on achieving the information security objectives must be 3.2.2The damage category results from the maximum principle, i.e. the highest damage category that results from considering all information security objectives and all damage scenarios is considered as the overall damage category.

3.2.4 Probabilities of occurrence

In order to evaluate risks, the probability of occurrence must be considered in addition to the effects of the damage. As long as there is a sufficiently large database for the probability of occurrence, a quantitative assessment based on previous events is possible. If there is a lack of data, which is to be assumed in many cases, an estimate or assessment must be used (experience-based, qualitative assessment).

A five-stage categorization of the probabilities of occurrence is used to assess the risk. The criteria for assignment are shown in the table below:

Level	Interpretation Frequency
Frequently	Once a month and more often
Possible	Once a quarter
Rarely	Once a year
very rare	Once in 3 years
unlikely	Less often than once in 3 years

To determine the probability of occurrence - based on the requirement ANF-RM 23 of the B3S [10] - the following factors should be taken into account:

- Damage frequency: Are new incidents or damage expected based on experience?
- Vulnerability discovery: How easy is the vulnerability to discover, especially by potential attackers?
- Attacker ability: What technical skills does a successful attack require?
- Exposure of the critical component: To what extent is the system exposed to a potential threat from a natural event due to its spatial location?
- Quality of the measures for attack detection: How quickly can an attack that is actually taking place be discovered by those being attacked?

3.2.5 Basic threats, vulnerabilities and threats[6]

Principally threats arise from the combination of basic threats and vulnerabilities. This policy assumes an all-hazards approach when identifying basic threats and threats.

For the risk analysis, the Göttingen University Foundation first uses pre-prepared risk catalogs. The catalog of elementary threats from the Federal Office for Information Security (BSI) in BSI standard 200-3 (see Section 5.3.1) is used as the basis for threat identification. For health care, the industry-specific safety standard (B3S) and the specific threats contained therein are also used (see Section 5.3.2).

An explicit consideration of basic threats and vulnerabilities and the derivation of further threats based on this must be carried out if the existing threat catalogs appear inadequate.

[6] The differentiation between basic threats (Bedrohungen) and threats (Gefährdungen) is derived from German information security standards.

For guidance in identifying threats, a list of possible basic threats is provided in Section 5.1.

Only by exploiting vulnerabilities do potential basic threats become real threats and the resulting risks. Considering vulnerabilities is therefore essential for identifying threats, since a basic threat can only become a threat if it coincides with a vulnerability. For the consideration of vulnerabilities, a list of possible vulnerabilities is listed in Section 5.2.

Both lists should be used for further analyzes if gaps in the threat catalogs have been identified.

3.3 Risk assessment

3.3.1 Protection requirements

The risk methodology of the Göttingen Foundation University, based on BSI standard 200-1 [9], provides for the protection requirements determination as the first step in the risk analysis.

The protection requirement for an information asset considers possible effects of the damage caused by potential threats, without taking into account the probability of occurrence and before a possible risk reduction through information security measures.

The information security policy states in **Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.**three categories of protection requirements.

To assign effects of the damage to the categories of protection requirements, the criteria for classifying effects of the damage according to Section 5.4used. The damage categories are assigned to the categories of protection requirements as follows:

- Normal protection requirements arise for the damage category insignificant,
- high protection requirement for the damage categories minor and noticeable,
- very high protection requirement for the damage categories critical and catastrophic.

For information assets for which a normal protection requirement is determined, a comprehensive risk analysis can be omitted. For these information values, the measures in the catalog of measures for basic IT protection Addendum 2:

High or very high protection requirements also arise from data protection legislation when processing special categories of personal data, especially when processing health data in the context of health care.

3.3.2 Criticality

For information assets and IT systems in the area of the critical infrastructure operated by the UMG in accordance with the BSI Act, the criticality of IT systems must be assessed, which results from the availability requirements of the information assets and IT systems. The classification is based on the industry-specific safety standard (B3S) for healthcare in hospitals [10], which provides for three criticality classes 1 to 3, depending on whether a system failure can be compensated for a short, medium or longer period.

The determination of criticality serves to prioritize the risk analyzes and risk treatment or the audits.

For the Göttingen Foundation University, the allocation is determined as follows:

- Class 1: Systems whose failure can be compensated for a maximum of 2 hours.
- Class 2: Systems whose failure can be compensated for more than two hours, but a maximum of 1 day.
- Class 3: Systems whose failure can be compensated for more than one day.

3.3.3 Risk classes

In a risk matrix, the effects of the damage is plotted against the probability of occurrence and pairs of these values are assigned to the risk classes.

The following risk classes have been defined for the Göttingen Foundation University:

- acceptable risks

  Risks that are viewed as sufficiently low that they can be accepted without further measures, such as risk reduction.

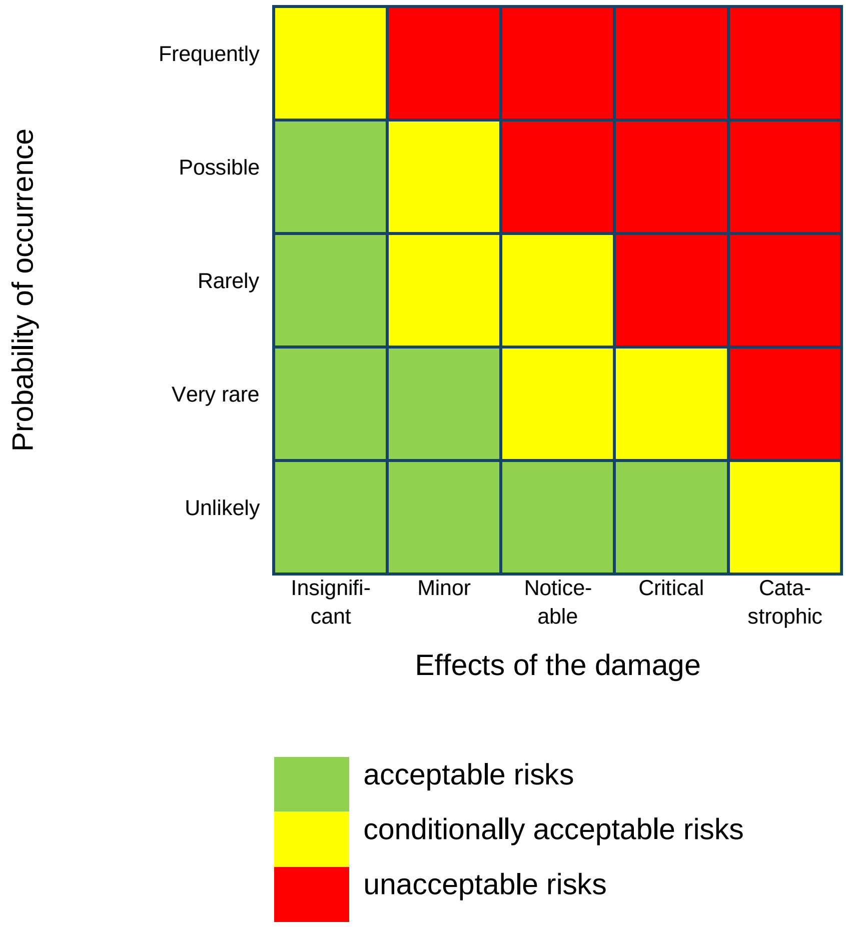
- conditionally acceptable risks

  can be accepted by the management in charge with justification as to why further risk treatment is not possible or sensible. Risk acceptance and the justification for this must be documented.

- unacceptable risks

  Risks that fundamentally cannot be accepted. Exceptions in special cases that are expressly justified with reference to the actual border crossing can only be decided by the Presidential Board or Management Board.

The risk classes are assigned according to the following risk matrix:



Probability of occurrence

	Insignificant	Minor	Noticeable	Critical	Catastrophic
Frequently	🟨	🟥	🟥	🟥	🟥
Possible	🟩	🟨	🟥	🟥	🟥
Rarely	🟩	🟨	🟨	🟥	🟥
Very rare	🟩	🟩	🟨	🟨	🟥
Unlikely	🟩	🟩	🟩	🟩	🟨

Effects of the damage

🟩 acceptable risks
🟨 conditionally acceptable risks
🟥 unacceptable risks

3.4 Risk treatment

Risk identification and risk assessment must be followed by risk treatment. The following procedures are generally possible for dealing with risks:

- **Risk avoidance** : Risk avoidance means that the causes of risk are excluded, for example by not using certain processes or systems.
- **Risk reduction** : Risk reduction means that risks are reduced through appropriate measures that reduce the impact of damage or the likelihood of damage occurring.
- **Risk transfer** : Risk transfer means sharing risks with another party, for example by taking out insurance or outsourcing.
- **Risk acceptance** : Risk acceptance means that risks are consciously accepted because, for example, the opportunities presented by an activity should be seized, and other risk treatments cannot be used or cannot be used sensibly or the risks are below the risk acceptance threshold .

Risk transfer is generally only applicable to a limited extent in the area of critical infrastructures and therefore also for the critical infrastructure operated by the UMG, i.e. to cover against residual risks (see and [11]ANF-RM 27 in [10]).

4 Operational structure

4.1 Determination of information assets (risk objects) and risk owners

The Göttingen Foundation University is active in teaching, research and health care. The processes that enable these areas of activity and all information that is used to maintain the processes represent the primary values of the Göttingen Foundation University. The primary values are dependent on supporting processes and IT systems (secondary values). The decentralization and heterogeneity of teaching, research and (partial) health care requires an identification of the values in decentralized units of the Göttingen Foundation University.

The management in charge as risk owners for these risk objects is responsible for identifying information assets as risk objects within their area of responsibility. The specialists responsible and information security coordinators support the management in charge in determining information values and the further steps of the risk analysis.

4.2 Determination of protection requirements and criticality

As part of the creation of operational concepts, the specialists responsible determine the protection requirements for information assets, taking into account the protection objectives of confidentiality, integrity, availability and, where necessary (e.g. when considering the critical infrastructure operated by the UMG), authenticity.

The need for protection results from the consideration of the damage scenarios in accordance with Section 3.2.1and the classification of effects of the damage in accordance with Section 3.2.3. The basis for this is the consideration of threats in accordance with Section 3.2.5.

The probabilities of occurrence and thus the determination of risks are not taken into account when determining protection requirements.

The criticality in accordance with Section 3.3.2be considered for the critical infrastructure in the healthcare system operated by the UMG .

Results of determining the protection requirements and criticality must be documented as part of the operational concepts.

4.3 Risk analysis

For information assets with normal protection requirements, it is assumed that the implementation of the measures of basic IT protection in accordance with the Information Security Policy will achieve a sufficient level of information security.

For information assets with higher protection requirements, a risk analysis must be carried out and documented as part of the creation of an operational concept. A higher protection requirement must be assumed for all information assets in health care, so a risk analysis must be carried out for this area.

For the risk analysis, the steps of risk identification (see Section 3.2), risk assessment (see Section 3.3) and risk treatment (see Section 3.4) must be carried out by the specialists responsible. The risk treatment must be implemented and documented by the specialists responsible and the responsible IT staff, with the specialist responsible being responsible for controlling.

The effects of the damage and probabilities of occurrence determined in this way result in 3.3.3

If the risk reduction procedure is used in the risk treatment plan, a new risk identification must be carried out with a view to reducing the impact of damage and the probability of occurrence and, based on this, a risk assessment must be carried out on the basis of measures that have already been implemented or specifically planned. The reduction effects must be documented in terms of effects of the damage and probability of occurrence as well as the resulting assignment to a risk class.

After the risk treatment has been implemented, the risk analysis must be repeated until the remaining risks have been completely treated, i.e. all remaining risks have been accepted.

4.4 Monitoring

4.4.1 Monitoring implementation

When monitoring the implementation of the risk reduction measures defined as part of risk treatment plans by those responsible and, above all, by the responsible ISM, the effectiveness and appropriateness of the measures must also be checked in addition to conformity to the treatment plan.

The results of the test must be documented as appendices to the operational concepts.

4.4.2 Monitoring policies and concepts

The information security policy, the overarching information security concepts and operational concepts must be regularly reviewed and updated. All changes to information values, threats, vulnerabilities, effects of the damage, probabilities of occurrence, risks and risk treatment options must be considered.

The information security policy and overarching information security concepts must be reviewed annually. The review is carried out by the information security officer in collaboration with the data protection and information security advisory board. The results of the audit must be presented to the Presidential Board and the Management Board as a report. Based on the report, the Presidential Board and the Management Board decide whether to maintain or change the information security policy and the overarching information security concepts.

Reviewed by those responsible at the intervals specified in these concepts and revised if necessary. The operating concepts based on test results and revised ones are submitted to the responsible management for decision and to the information security officer for approval.

4.5 Communication and consultation

The Presidium and Board of Directors are informed about risks as part of the annual report of the ISB in accordance with § 11Paragraph **Fehler! Verweisquelle konnte nicht gefunden werden.**Letter **Fehler! Verweisquelle konnte nicht gefunden werden.**.

The report in accordance with § 11Paragraph **Fehler! Verweisquelle konnte nicht gefunden werden.**Letter **Fehler! Verweisquelle konnte nicht gefunden werden.**lists the information security risks assumed. The focus is on risks that, according to this appendix, can be assigned to risk class n “conditionally acceptable” and “unacceptable”. The change in the risk situation and the results of monitoring the risks, the monitoring of measures with regard to the effectiveness of the measures and the need for decisions must be listed in the report.

The report is based on the operating concepts adopted by the responsible management and the results of their updating.

In the area of critical infrastructure operated by UMG, an additional half-yearly report must be prepared by the ISB to the Board of Directors on material risks.

In the university area (excluding UMG), comprehensive risk management takes place, which is described in the university's risk management concept. If information security risks in the university area exceed the threshold values for recording risks set out in this risk management concept, these risks will be reported by the risk officers responsible in accordance with this risk management concept for inclusion in the risk report.

5 additional information

5.1 List of threats

The following list of threats is taken from the BSI's guide “Protection of Critical Infrastructures: Hospital IT Risk Analysis” [12]or the associated appendix “Protection of Critical Infrastructures: Hospital IT Risk Analysis – Aids” [13]. The numbering has been added. The threats B 4.2.6, B 4.3.1and B 4.4.1were based on the threats A1.4, A1.11 and A1.10 of the “Guidance on content and requirements for industry-specific security standards (B3S) in accordance with Section 8a (2) BSIG Version 1.0" [14]supplemented by the BSI.

B 1 Natural events
B 1.1 Natural events (lightning, fire, water, dust, climate, wind)
B 2 Technical failure
B 2.1 Technical failure of IT systems
B 2.1.1 Malfunction of IT systems

B 2.1.2 Malfunction or failure of IT systems
B 2.2 Technical failure of data storage
B 2.2.1 Wear and tear of storage media
B 2.2.2 Data loss
B 2.3 Technical failure of networks
B 2.3.1 Interference or failure of communication networks
B 2.4 Technical failure of the supply
B 2.4.1 Malfunction or failure of the power supply
B 2.4.2 Disruption or failure of supply networks
B 3 Human wrongdoing
B 3.1 Human errors in IT systems
B 3.1.1 Incorrect use or administration of IT systems
B 3.2 Human errors in software
B 3.2.1 Software vulnerabilities or errors
B 3.3 Human mishandling of data
B 3.3.1 Unintentional disclosure of sensitive information
B 4 Intentional actions
B 4.1 Intentional actions on IT systems
B 4.1.1 Hardware manipulation
B 4.1.2 Theft and loss of systems, data carriers and documents
B 4.1.3 Unauthorized entry into premises
B 4.1.4 Unauthorized intrusion into IT systems
B 4.1.5 Unauthorized use or administration of IT systems
B 4.1.6 Destruction of IT systems
B 4.2 Intentional acts on software, data and information
B 4.2.1 Denial of actions
B 4.2.2 Spying on information/data
B 4.2.3 Manipulation of software and information/data
B 4.2.4 Misuse of personal data (e.g. persons worthy of protection)
B 4.2.5 Abuse of permissions
B 4.2.6 Identity abuse
B 4.2.7 Destruction of data carriers
B 4.3 Intentional actions on data networks
B 4.3.1 (Distributed) denial-of-service attacks (DoS, DDoS)
B 4.4 Intentional actions in interpersonal communication
B 4.4.1 Social engineering
B 5 Organizational influences
B 5.1 Internal organizational influences
B 5.1.1 Lack of resources (poor planning)
B 5.2 External organizational influences
B 5.2.1 Disruption or failure of service providers

When considering human error and intentional actions, internal and external perpetrators must be taken into account, and people with physical access as well as those with only network access must also be taken into account.

5.2 List of vulnerabilities

The following list of vulnerabilities is taken from the BSI's guide “Protection of Critical Infrastructures: Hospital IT Risk Analysis” [12]or the associated appendix “Protection of Critical Infrastructures: Hospital IT Risk Analysis – Aids” [13]. The numbering has been added. S 3.4.5supplemented based on vulnerability A 2.7 of the “Guidance on content and requirements for industry-specific security standards (B3S) in accordance with Section 8a (2) BSIG Version 1.0” .[14]

S 1 Hardware

S 1.1 Improper disposal

S 1.2 Inadequate environmental conditions

S 1.2.1 The system is not resistant to moisture, dust or contamination

S 1.2.2 The system is not resistant to heat or cold

S 1.2.3 The system is placed in an inappropriate location

S 1.3 Inadequate maintenance

S 1.4 Insecure and/or incomprehensible hardware configuration

S 1.4.1 Incomplete and/or incorrect hardware configuration documentation

S 1.4.2 Changes to the hardware are not adequately documented

S 1.4.3 Hardware changes are not monitored

S 2 software

S 2.1 Lack of malware protection

S 2.2 Known software bugs

S 2.3 Lack of security functionality

S 2.3.1 Inadequate password protection

S 2.3.2 Inadequate encryption

S 2.3.3 Lack of access protection

S 2.4 Insecure software configuration

S 2.4.1 Lack of patch management

S 2.4.2 Insufficient default configuration

S 3 network

S 3.1 Missing encryption

S 3.1.1 Unprotected connections to public networks (especially unprotected WLAN access)

S 3.1.2 Unprotected communication connections

S 3.1.3 Transmission of passwords in plain text

S 3.2 Physical defects

S 3.2.1 Poor cabling

S 3.2.2 Unprotected network connections

S 3.3 Improper network management

S 3.3.1 Routing resilience to interference

S 3.3.2 Poor network configuration management

S 3.4 Insecure network architecture

S 3.4.1 Single point of failure

S 3.4.2 Unknown IT systems

S 3.4.3 Known compromised IT systems

S 3.4.4 Lack of mechanisms for identification and authentication

S 3.4.5 Coupling of services and lack of separation to prevent and isolate faults

S 4 staff
S 4.1 Inadequate staffing of critical human resources
S 4.2 Inadequate user training
S 4.3 Lack of care in personnel selection
S 5 Infrastructure
S 5.1 IT systems are freely accessible
S 5.2 Poor building security
S 5.2.1 Lack of access protection
S 5.2.2 Lack of protection against water damage
S 5.2.3 Lack of fire protection
S 5.2.4 Unfavorable building location
S 5.3 Insufficiently secure power supply
S 5.3.1 Voltage and frequency fluctuations
S 5.3.2 Dependence on a single energy supplier
S 5.3.3 Lack of emergency power capacity
S 6 organization
S 6.1 Inadequate processes
S 6.1.1 Lack of service provider management
S 6.1.2 Inadequate processes for security and risk management
S 6.1.3 irregular backups
S 6.1.4 Lack of end device management
S 6.1.5 Inadequate emergency planning
S 6.1.6 Lack of logging and monitoring
S 6.1.7 Lack of hardware and software configuration management
S 6.1.8 No consistent management of hardware or software inventory
S 6.2 Inadequate responsibilities
S 6.2.1 There is no one responsible
S 6.2.2 There is no clearly named responsible person
S 6.3 Insufficient role definition
S 6.3.1 Incomplete job description of roles
S 6.3.2 Lack of Identity and Access Management (IAM)

5.3 Lists of hazards

5.3.1 Elementary threats to BSI basic protection

The following list of elementary hazards is taken from BSI standard 200-3. The basic value column notes which basic value/information security objectives can be affected by the threat (C=Confidentiality, I=Integrity, A=Availability).

number	Danger	Core value
G 0.1	Fire	A
G 0.2	Unfavorable climatic conditions	I, A
G 0.3	Water	I, A
G 0.4	Pollution, dust, corrosion	I, A
G 0.5	Natural disasters	A
G 0.6	Disasters in the area	A
G 0.7	Major events in the area	C, I, A
G 0.8	Failure or malfunction of the power supply	I, A

G 0.9	Failure or disruption of communication networks	I, A
G 0.10	Failure or disruption of supply networks	A
G 0.11	Failure or disruption of service providers	C, I, A
G 0.12	Electromagnetic interference radiation	I, A
G 0.13	Intercepting compromising radiation	C
G 0.14	Spying for information/espionage	C
G 0.15	Eavesdropping	C
G 0.16	Theft of devices, data carriers and documents	C, A
G 0.17	Loss of devices, data carriers and documents	C, A
G 0.18	Poor planning or lack of adjustment	C, I, A
G 0.19	Disclosure of sensitive information	C
G 0.20	Information from unreliable source	C, I, A
G 0.21	Manipulation of hardware and software	C, I, A
G 0.22	Manipulation of information	I
G 0.23	Unauthorized intrusion into IT systems	C, I
G 0.24	Destruction of devices or data carriers	A
G 0.25	Failure of devices or systems	A
G 0.26	Equipment or system malfunction	C, I, A
G 0.27	Lack of resources	A
G 0.28	Software vulnerabilities or errors	C, I, A
G 0.29	Violation of laws or regulations	C, I, A
G 0.30	Unauthorized use or administration of devices and systems	C, I, A
G 0.31	Incorrect use or administration of devices and systems	C, I, A
G 0.32	Abuse of permissions	C, I, A
G 0.33	Loss of staff	A
G 0.34	attack	C, I, A
G 0.35	Coercion, extortion or corruption	C, I, A
G 0.36	Identity theft	C, I, A
G 0.37	Denial of actions	C, I
G 0.38	Misuse of personal data	C
G 0.39	Malicious programs	C, I, A
G 0.40	Denial of Service	A
G 0.41	sabotage	A
G 0.42	Social engineering	C, I
G 0.43	Importing messages	C, I
G 0.44	Unauthorized entry into premises	C, I, A
G 0.45	Data loss	A
G 0.46	Loss of integrity of information worthy of protection	I
G 0.47	Harmful side effects of IT-based attacks	C, I, A

5.3.2 Threats to the B3S

The following hazards are taken from the DKG industry-specific safety standard for healthcare in hospitals [10]. These threats must also be considered for information assets in the critical healthcare infrastructure operated by UMG.

GEF 1 Unavailability of important, medically relevant data in the diagnostic process
GEF 2 Unavailability of important medically relevant data in the therapy process

GEF 3 Unavailability of important medically relevant data in the nursing care process

GEF 4 Unavailability of important medically relevant data in the discharge process

GEF 5 Non-availability of process and release information important for the treatment process

GEF 6 Unavailability of IT systems relevant to the treatment process

GEF 7 Unavailability of treatment-relevant logistics chains

GEF 8 Inconsistencies in data sets relevant to the treatment process

GEF 9 Inconsistencies in the transfer of data relevant to the treatment process

GEF 10 Manipulation of medically relevant data in the diagnostic process

GEF 11 Manipulation of medically relevant data in the therapy process

GEF 12 Manipulation of medically relevant data in the care process

GEF 13 Manipulation of medically relevant data in the discharge process

GEF 14 Interruption of treatment-relevant communication processes.

GEF 15 Loss of confidentiality for particularly sensitive patient and treatment information.

GEF 16 Loss of data authenticity

GEF 17 External control/manipulation of medically relevant IT systems

GEF 18 External control/manipulation of network-connected medical devices

GEF 19 External control/manipulation of relevant infrastructure components

5.4 Criteria for assignment to damage impact categories and protection needs

The assignment to the five categories of is carried out according to the criteria in the table below:

Level	Personal integrity	Task fulfillment	Negative internal or external impact	Financial impact	Right to informational self-determination	Violation of laws, ordinances, regulations, contracts	Need for protection
Insignificant	Incident, but without consequences (critical incident, near miss).	stays untouched.	The reputation is hardly affected. There is a need for clarification internally.	The financial damage is hardly noticeable in the annual result (university up to €100,000, UMG up to €200,000).	Unauthorized access to data that has been made freely accessible elsewhere by those affected.	Without violations of regulations and laws, no or only minor claims for damages	normal
small amount	Minor health damage with temporary discomfort/pain up to 3 days of hospitalization or, in the case of UMG patients, extended hospitalization.	remains unaffected, there will be short-term disruptions in operations and additional costs.	Inquiries from interested people outside the university, the media are interested. The external need for clarification does not yet have any lasting consequences.	The financial damage leads to small deviations in the annual result (university up to €300,000, UMG up to €500,000).	Unauthorized access to data whose improper handling is not expected to cause any particular impairment, but which has not been made freely accessible by those affected.	Violations of regulations and laws with minor consequences, minor claims for damages up to €300,000; Fines of up to €10,000	high
noticeable	Serious damage to health without lasting consequences. More than 3 days (extended) hospitalization.	Temporarily diminished. Additional costs arise from the treatment and/or from additional disruptions to the processes.	Reputation is affected by negative reports, investigations and local media reports.	The financial damage has a negative impact on the annual result. Both income and liquidity are visibly affected (university up to €1,000,000, UMG up to €3,000,000).	Unauthorized access to data, the improper handling of which could adversely affect the person concerned's social status or economic circumstances ("reputation").	Violations of regulations and laws with significant consequences, over €1,000,000; Fines of up to €100,000; Criminal liability	
critical	Serious damage to health with permanent consequences, without the need for long-term care, but with occupational restrictions.	constantly impaired. The range of services is limited.	The reputation is damaged regionally over a long period of time through negative media reports, criminal and liability lawsuits and investigations. If possible, students, research partners or patients prefer other universities or clinics.	The financial result is sustainably influenced. The damage increases to the amount of an annual result. Liquidity is tightened (university up to €3,000,000, UMG up to €5,000,000).	Unauthorized access to data, the improper handling of which could significantly affect the person concerned's social position or economic circumstances ("existence").	Serious violations of regulations and laws with significant consequences, claims for damages in excess of €1,000,000; Fines over €100,000; significant criminal liability	Very high
catastrophic	Serious damage to health with long-term consequences and long-term need for care. Death.	The continuation of an institution (institute, clinic, department, area) with its previous range of services is threatened.	The reputation is irreparably damaged nationwide, e.g. B. through criminal law suits and negative reporting. Confidence in the leadership has been shaken and capacity utilization is no longer guaranteed.	The financial damage threatens the company's existence and has a serious impact on the annual result. There is a risk of insolvency (university over €3,000,000, UMG over €5,000,000)	Unauthorized access to data, the improper handling of which could harm the health, life or freedom of the person concerned.	Fundamental violation of regulations and laws, claims for damages over €3,000,000; Fines over €1,000,000; Criminal liability up to and including crimes	

6 Bibliography

[1] Georg-August-Universität Göttingen, “Risk management concept of the Georg-August-Universität Göttingen,” https://www.uni-goettingen.de/de/document/download/c4666b41203f78adb6d0a510c4908639.pdf/Risk management_konzept.pdf, 2020.

[2] ISO/IEC, “ISO/IEC 27005:2011(E): Information technology — Security techniques — Information security risk management,” ISO/IEC, Geneva, 2011.

[3] Austrian Standards Institute, “ONR 49000, Risk management for organizations and systems, terms and principles,” Austrian Standards plus GmbH, Vienna, 2014.

[4] Austrian Standards Institute, “ONR 49001, Risk management for organizations and systems, risk management,” Austrian Standards plus GmbH, Vienna, 2014.

[5] Austrian Standards Institute, “ONR 49002-1, Risk management for organizations and systems, Part 1: Guide for embedding risk management in the management system,” Austrian Standards plus GmbH, Vienna, 2014.

[6] Austrian Standards Institute, “ONR 49002-2, Risk management for organizations and systems, Part 2: Guide to risk assessment methods,” Austrian Standards plus GmbH, Vienna, 2014.

[7] Federal Office for Information Security, “BSI Standard 200-3 Risk Analysis based on IT-Grundschutz,” Bonn, 2017.

[8th] DIN, “DIN EN 80001-1:2011-11: Application of risk management for IT networks containing medical devices,” 2011.

[9] Federal Office for Information Security, “BSI Standard 200-1 Management Systems for Information Security (ISMS),” Bonn, 2017.

[10] German Hospital Society, “Industry-specific safety standard for healthcare in hospitals,” Berlin, 2019.

[11] BSI, “www.bsi.bund.de,” Federal Office for Information Security, [Online]. Available: https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/FAQ/FAQ_8aBSIG_general/faq_bsi_8a_general_node.html#faq10523112. [Accessed January 25, 2020].

[12] Federal Office for Information Security, “Guidelines for the Protection of Critical Infrastructures: Risk Analysis of Hospital IT,” Bonn, 2013.

[13] Federal Office for Information Security, “Aids for protecting critical infrastructures: Risk analysis of hospital IT,” Bonn, 2015.

[14] Federal Office for Information Security, “Orientation aid on content and requirements for industry-specific security standards (B3S) in accordance with Section 8a (2) BSIG Version 1.0,” Bonn, 2017.

[15] Georg-August University of Göttingen, “Information Security Guidelines of the Georg-August University of Göttingen,” *Official Notices of the Georg-August University of Göttingen,* open 2019.

Addendum 4: 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.

Increased need for protection

Summary term for high or very high protection needs in contrast 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.