Recommendation by the
25th General Assembly of
the German Rectors'
Conference (HRK)
on 6 November 2018
in Lüneburg

Information security as a strategic task for leaders of universities

HRK German Rectors' Conference

The Voice of the Universities

Leipziger Platz 11
10117 Berlin
Tel.: +49 (0) 30 206292-0
Fax: +49 (0) 30 206292-15
post@hrk.de
www.hrk.de

Ahrstraße 39
53175 Bonn
Tel.: +49 (0) 228 887-0
Fax: +49 (0) 228 887-110
post@hrk.de
www.hrk.de

Table of Contents

Preamble

This paper consists of two parts. The first comprises a recommendation for the leaders of universities, and the second provides guidelines that are also directed at middle management. The sum of these two parts aims to help convey both the relevance of the topic of information security and starting points for implementation measures.

Part A: Summary for leaders of universities

I. Information security as a challenge facing universities

Universities, like other organisations, are increasingly exposed to dangers and risks to information and knowledge. These dangers and risks specifically affect the core functions of teaching, research and knowledge transfer, particularly in terms of

- loss of integrity and availability of **research data**
- the compromising of **personal data**, particularly student and patient data
- loss of confidentiality of **data within cooperative arrangements**, for example due to espionage.

Universities are especially vulnerable in this regard. Freedom of research and teaching, global cooperation based on the exchange of ideas between experts, the large degree of autonomy of sub-units, the common project format, high personnel turnover, the various status groups with their different roles and rights and the rapid development cycles of information technology all contribute to this. For this reason, information security is a significant challenge for universities.

Universities have made impressive efforts in recent years to protect their information processing[1]. In a current survey by the AKIF, the German Research Institutions' Information Security working group[2], over one hundred universities provided information about the current status of their activities in the area of information security. Both the fact that this topic is highly relevant and the growing need for action in the face of increasing digitalisation are acknowledged. Accordingly, many universities are dedicating themselves to the task of further developing their security strategy, starting with a more narrowly defined IT security concept and moving towards a broader understanding of information security appropriate to academia and research.

II. The strategic task of leaders of universities

In the academic environment, the concept of information security mainly focuses on the aspects of integrity, confidentiality as well as the availability and

[1] See also HRK Rundschreiben (circular) no. 24/2014 "IT-Sicherheit an Hochschulen und Forschungseinrichtungen" (IT security at universities and research institutions) with the annex "Bedeutung der IT-Sicherheit an wissenschaftlichen Einrichtungen" (Importance of IT security at scientific institutions) by the Alliance of Science Organisations in Germany (available only in German).

[2] The German Research Institutions' Information Security working group is a working group of the Alliance of Science Organisations in Germany, see also https://www.ak-if.de/ (available only in German).

exchange of information. Information security differs from IT security in that the asset of information to be protected and the associated information-processing tasks are given priority in risk assessment and management.

Integrating information security as an aspect of process quality at universities is not only required by law, it is also an organisational task within the framework of the governance structure and institutional awareness. Leaders of universities must actively address these aspects, which also concern the research and teaching culture. These organisational and cultural dimensions can only be brought together, evaluated and addressed in their entirety by the leaders of universities. Information security is thus a primary strategic task of leaders of universities and needs to be integrated into all higher education processes. In doing so, protection measures must always be seen in the context of the security gains made and the value of the assets to be protected because in the long term this is the only way that the need for security and freedom of research, teaching and creative development projects can be reconciled.

The responsibility of leaders of universities for information security extends, in particular, to the creation of functional structures for the planning, implementation, review and improvement of information security. The department in question and the operators of the information infrastructure must cooperate within these structures, and the relationships to and between data protection, IT security, the legal department, Executive Board, press and communications office and incident reporting points must be regulated. In order to achieve the envisaged level of security, adequate resources must be made available.

As with the issue of data protection, outwardly the exercise of responsibility for information security is primarily demonstrated by

- appointed persons responsible for the process
- defined notification channels and the presence of a response team
- a regulated risk management system
- the documentation of security strategy and measures in the form of guidelines and an information security concept
- an ongoing improvement process.

Notification, response and documentation obligations as well as risk management are fulfilled in a coordinated manner for information security, IT security and data protection for logical reasons. The security level actually achieved depends very much on the awareness of information security within the university, the existing expertise in IT security and successful interactions between the structures detailed above.

III. Guiding principles for information security processes

The following guidelines provide generally applicable guiding principles in the form of dos and don'ts:

	Dos	Don'ts
Relevance	⊕ Regard information security as a comprehensive organisational and cultural asset.	⊖ Regard information security as a mere technical challenge.
Protective measures	⊕ Always assess the effort involved in protective measures in relation to the increase in security achieved and the value of the assets to be protected.	⊖ Maximise security measures without context.
Mandates	⊕ Appoint information security officers officially and formally.	⊖ Informally nominate information security officers.
Dual functions	⊕ Information security officers and computer centre management as well as data protection and information security officers should be able to resolve conflicting goals using dialogue.	⊖ Appoint the same person to act as information security officer and head of computer centre, as well as data protection and information security officer.
Legal framework	⊕ Consider legal terms within the context of technical development and the interests of universities.	⊖ Consider and follow legal guidelines without context.
Information security concept	⊕ Information security concept is a tool for risk assessment and management.	⊖ Rush to create an information security concept that only documents target states that differ widely from the actual status.
Process goals	⊕ Formulate goals that are achievable in the short term and put them into effect incrementally.	⊖ Implement idealistic master plan non-incrementally.
Handling of incidents	⊕ Aim for the highest degree of resilience possible.	⊖ Strive for absolute security.
Communication in event of incidents	⊕ Comply with notification obligations, consult with the press and communications office.	⊖ Withhold information.
Support	⊕ Make use of support from institutional service providers (e.g. German National Research and Education Network (DFN)).	⊖ Only rely on internal expertise.
Resources	⊕ Assess resources in relation to the envisaged scope and complexity.	⊖ Regard resources as an indispensable prerequisite for achieving any goal whatsoever.
Cooperative arrangements	⊕ Take advantage of synergies, while maintaining your responsibility.	⊖ Understand cooperation structures as relieving you of responsibility.
Certifications	⊕ Aim for certifications with a view to possible added value for the institution.	⊖ Pursue certifications as a goal in themselves.

Part B: Guidelines

Preliminary remarks

These guidelines are intended to provide guidance to those persons entrusted with the implementation of the relevant processes. With this in mind, the guidelines include explanations as well as suggestions and action points.

Given the complexity of the topic of information security and the heterogeneity of universities, it is inherently impossible to outline a uniform model solution. However, the guidelines are based on the guiding principle of an incremental approach. Generally, there is no such thing as absolute security and the handling of incidents must therefore be regulated and practised, and the implementation of measures must be prioritised on the basis of risk.

I. Information security as a challenge facing universities

Science requires trust. This applies to research and teaching as well as, building on this, transfer to society, which are core functions of the universities. Information security is therefore an indispensable requirement for academic work and trust in science, especially in light of digitalisation.

Universities, like other institutions, are increasingly exposed to dangers and risks to information and knowledge. These dangers and risks specifically affect the core functions of teaching, research and knowledge transfer, particularly in terms of

- loss of integrity and availability of **research data**
- the compromising of **personal data**, particularly student and patient data
- loss of confidentiality of **data within cooperation arrangements**, for example due to espionage.

For example, gateways exist for current attempts to access personal data via fake websites, e-mails or text messages (phishing). Access data for research purposes, student examinations or even administrative management tools can be the targets of such phishing attacks. Phishing is also a genuine danger in the context of espionage activities. Another threat scenario is the infection and locking of computers in order to demand money for unlocking them (ransomware). If the infection or locking of a central university computer is successful, research, study and administrative activities may be brought to an abrupt halt and sensitive data could also be lost. There could be similar consequences in the event that external parties use the university infrastructure for botnets.

Universities are particularly vulnerable. Freedom of research and teaching, global cooperation based on the exchange of ideas between experts, the large degree of autonomy of sub-units, the common project format, high personnel turnover, the various status groups with their different roles and rights and the rapid development cycles of information technology all contribute to this. For this reason, information security is a significant challenge for universities.

In a current survey by the AKIF, the German Research Institutions’ Information Security working group, over one hundred universities provided information about the current status of their activities in the area of information security. Both the fact that this topic is highly relevant and the growing need for action in the face of increasing digitalisation are acknowledged. Accordingly, many universities are dedicating themselves to this issue, starting from a more narrowly defined IT security concept and moving towards a broader understanding of information security appropriate to academia and research.

These challenges have been given a more concrete form, particularly with respect to the protection of personal data and associated documentation obligations, with the advent of the EU General Data Protection Regulation (GDPR), which came into force on 25 May 2018. The GDPR introduces more extensive documentation and notification obligations, in particular. Synergies can be exploited for data protection and information security. However, the differing orientations must be taken into account.

II. The task of leaders of universities

1. Information security involves more than IT security

The term 'information security' is defined by various standards organisations (see the definition below according to ISO/EC/DIN); however these definitions mostly focus on a general corporate environment. For science and its operating methods – and in particular for universities – an interpretation oriented towards these activities is necessary in relation to goal-setting and management.

Definition of information security according to DIN/ISO/IEC 27000:2015

2.33 Information security

Preservation of confidentiality (2.12), integrity (2.40) and availability (2.9) of information;

A note regarding the concept: Other qualities such as authenticity (2.8), accountability, non-repudiation (2.54) and reliability (2.62) can also be included.

Information security covers three main aspects: confidentiality, availability and integrity. Information security requires the application and management of appropriate security measures, taking into account a broad range of threats, with the goal of ensuring sustained business success and business continuity and minimising damage due to information security incidents. Information security is achieved by implementing a suitable set of measures that are selected during the specified risk management process and controlled with the help of an ISMS[3], which covers guidelines, processes, procedures, organisational structures, software and hardware for the protection of identified information values. These measures must be determined, implemented, monitored, reviewed and, where necessary, improved in order to ensure that the specific information security and business goals of the organisation are achieved. It is expected that relevant information security measures will be integrated seamlessly into the business processes of the organisation.

The criterion of quality and the associated quality assurance play a prominent role in science. Reliable data must therefore fulfil the requirements of both quality assurance and information security. In addition, universities are active in a global context and engage in open dialogue with society. This gives rise to conflicting priorities for universities that necessitate the balancing of protection goals.

- On the one hand, the postulate of openness, of digital research processes, methods and results (open access, open science, open data) and of teaching materials (open educational resources) implies that the protection goals of integrity and availability have a particularly significant value.
- On the other hand, there is also the desire for confidentiality deriving from the need for protected areas for academic cooperation and not least from academic competition.

The weighing up required in relation to the creation of protection goals and risk assessment can only be performed by academia itself – within the framework of the existing laws of course. Information security thus differs from IT security in that the asset of "information" to be protected and the associated information-processing tasks in research, teaching and knowledge transfer are given priority in risk assessment and management.

[3] Information Security Management System.

Hence, the complex issue of information security can only be approached on the basis of collaboration between the departments in question (research, teaching, knowledge transfer, administration) and the IT area. The development of framework conditions for process transparency and codes of conduct in the form of principles and guidelines must be guided and overseen by the university and cannot be the task of the operational IT service provider alone. In this process, responsibility for making decisions on risks must be integrated into university processes. The task of anchoring information security as an aspect of process quality in the university as an organisation is therefore not restricted to creating IT security in the narrower sense. Information security is not only a legal requirement, but rather part of an overarching organisational task in the context of institutional awareness and governance structures and processes.

2. Information security as an overarching organisational task

In creating institutional awareness for information security, the primary aim is to sensitise and train staff members of universities. It is important to convey the fact that every person can make their own contribution in the area of information security. This institutional awareness can only be successful where it is not simply conceived and implemented, but also practised – that is, continually tested and improved. To advance information security in the long term, it is imperative that the topic of information security also be understood as a function of education and be addressed in teaching accordingly.

Measures to promote awareness

Measures to promote awareness should address both employees and students as their target group. Possibilities include competitions for ideas, lectures and information stands with posters, flyers, personalised password cards and giveaways. The relevant information can also be distributed on the website of the university and its newsletters or student magazines. As regards phishing, options include online self-assessment tests and phishing advice.

Leaders of universities must actively address the topic of awareness and its diverse aspects, which also include the culture of research and teaching. These organisational and cultural dimensions can only be brought together, evaluated and addressed in their entirety by the leaders of universities. Information security is hence a primary strategic task for leaders of universities. Information security must not be viewed as a mere technical challenge; it should rather be seen as an overarching task of organisational development.

For the university as a whole, as well as for its sub-units, the key processes of the respective units must serve as points of reference for information security. Protection measures should not be maximised out of context. The effort involved in protection measures must always be assessed in relation to the increase in security achieved and the value of the assets to be protected because in the long term this is the only way that the need for security and freedom of research, teaching and creative development can be reconciled. To determine the accepted risks, there needs to be an organisation and governance capable of decision-making.

3. Responsibility for administration and governance

Above all, the responsibility of leaders of universities for information security includes the creation and maintenance of effective structures and the provision of adequate resources for achieving the envisaged security level.

While leaders of universities bear responsibility for information security, the administration and implementation of information security management are delegated to a subordinate with responsibility for the procedure or an officer such as Chief Information Security Officers (CISOs) or Information Security Officers (ISOs), who may be based in a unit reporting to the leaders of the university. In this context, it is important for the legitimation of the position that the leadership of the university grants the appropriate mandate officially and formally, instead of informally nominating someone. Persons responsible for the procedure should be able to resolve any conflicts between goals with the heads of internal higher education units through dialogue. For this reason, appointing the same person as the information security officer and head of a computer centre does not appear advisable. Likewise, one person should not perform the role of both data protection officer and information security officer. A CISO/ISO is responsible in particular for the so-called information security concept, that is, for the documentation of information security risks and the associated implemented and planned measures.

Interactions between information security, data protection and operational IT security and with university leadership, the legal department, emergency centre and press office must be regulated, described and communicable. There are naturally overlapping areas here that promote a collaborative approach at universities in favourable circumstances. The fact that information security, viewed as a process, can be identified in all processes of the university also constitutes a challenge. Firstly, the entire organisational structure is affected and, secondly, clear decision-making channels and assumption of responsibility are vital to the capacity to act in terms of information security.

Despite the heterogeneity in the higher education landscape with regard to governance in general and governance of information processing and supply in particular, it is possible to adapt general principles to local conditions. However, it is evident that clarity needs to be established with regard to the assumption of rights/obligations and responsibility, particularly in respect of decentralised and centralised responsibilities as well as with regard to risk assessment and decisions on risk acceptance.

Approach to clarifying responsibilities:
RACI charts

Differentiated role models can be supported by RACI charts and the variations derived from these. RACI (Responsible, Accountable, Consulted, Informed) distinguishes, for example, between responsibility for implementation and accountability/overall responsibility. Numerous variations of this exist in the literature. This clarification of differentiated responsibilities in terms of information security in core and support processes of teaching, research, knowledge transfer and administration also facilitates an incremental approach, which deals with processes according to their priority.

Furthermore, a fundamental decision can be made about the extent to which particular status groups must commit themselves in writing to comply with the regulations on information security and to undergo training in information security when commencing work at the university. The onboarding process also presents opportunities for awareness measures.

4. Legal framework

From a legal perspective, information security and data protection must always be viewed as a whole, but in dialogue. While risks to the university as an organisation are evaluated from the perspective of information security, data protection focuses its attention on the risks of breaching the right of determination of disclosure and use of personal data of the natural persons, such as students, researchers, employees and test subjects, working at the higher university institution and its environs. Data protection risks can comprise information risks, just as information risks can result in data protection risks. However, the types of classification and what risk responses are derived may vary due to the differing perspectives. Leaving processes relevant to data protection aside, there are information security requirements, particular relating to confidentiality, for example with respect to copyright law and protection of patents, as well as confidentiality obligations in the context of cooperation agreements.

The relevant legal standards are the German IT Security Act amended on the basis of the EU Directive to ensure a high level of Network and Information Security (NIS) for information security and the aforementioned EU General Data Protection Regulation (EU GDPR) for data protection. Further applicable legal standards include the Act on the German Federal Office for Information Security, BSI, the Telemedia Act and the Telecommunications Act, state data protection legislation, criminal law as well as non-legislative and, where applicable, state-specific rules and standards.

At the heart of these legal standards are concepts such as 'state of the art', and the assessment criteria of 'reasonableness', 'necessity', 'appropriateness' and 'adequacy'. Given the dynamic nature of technical developments, these legal concepts must be continuously aligned with the interests of the respective university and implemented by the persons responsible. Thus, legal requirements should not be viewed or pursued out of context.

5. Preparing and updating an information security concept

The goal of every university is to achieve and maintain an adequate level of information security. Information risks must be assessed and managed for this purpose. As a tool for the associated planning and implementation, the risks identified as well as the implemented and planned measures are recorded (and updated) in an information security concept.

The planning and implementation of information security and thus the process for preparing and updating an information security concept are inherently complex and resource-intensive. For this reason, the focus should not be on achieving 'completeness' as quickly as possible. Information security concepts that have been hastily prepared or updated run the risk of only documenting target states that differ widely from the actual status. Instead, it is advisable to formulate goals that are achievable in the short term and put them into effect in succession. This means rejecting the notion of implementing an ideal master plan non-incrementally.

The following key questions have proven especially beneficial for an incremental approach:

a) Can risks which must be dealt with as a matter of urgency be identified?
b) How can the importance of the different types of data be captured?
c) How can the assessment and management of information security risks be integrated into the processes of the organisation?

On a) For universities, the particular need to protect student and patient data is obvious. In this case, priorities can be determined using a top-down approach – such risks do not first need to be laboriously identified. Basic protection of IT systems, e.g. of audit offices, is also required. Approaches such as IT baseline protection methodology (Version 200-2) or ISIS12 also offer easily accessible basic and core protection or a simplified entry point.

On b) A multi-stage approach is particularly promising in the context of risk management. A classification of data must first be performed. In the course of such a risk management approach, relevant processes can be recorded and the corresponding risk assessments can be carried out in each unit. Proposals for centralised and decentralised measures can be derived from this. The recorded points and proposals should then be evaluated centrally. On the basis of this evaluation, a central unit can then delegate model standards or prescribed minimum measures to the decentralised units for further elaboration. The solutions prepared in this way offer a high degree of uniformity and comparability as well as acceptance.

Proposal: data classification
In terms of both awareness and bottom-up participation, the process could begin with all personnel classifying information in particular need of protection in their units. This classification should be comprehensive. The starting point could be the broad classification of 'public', 'internal', 'confidential' and 'secret'. In the process, it is necessary to review whether a differentiation should be made with regards to the university groups 'researchers', 'teachers' and 'students' and 'administration'. This initial impetus could subsequently be used for the preparation of

the corresponding FAQs. In this way, awareness of information security issues could be raised in specialist areas not closely related to IT.

On c) Ongoing assessment and management of information risks results from integration into processes in teaching, research, knowledge transfer and administration. For example, information security should be included in considerations when preparing data management plans.

Proposal: preparation of data management plans
Data management plans are already being called for within the framework of the guidelines of some research funding organisations. A data management plan describes which data is collected and generated in the course of work and what happens to this data during its life cycle (storage, publication, citation, long-term availability, anonymity, deletion, etc.). The goal of a data management plan is to meet the requirements of good scientific practice and to ensure the traceability of research results in the long term.
(Source: Library of ETH Zurich: https://library.ethz.ch/en/news-and-courses/news/news-articles/2021/12/data-management-plan-instructions.html
(link updated 8 February 2023)))

Aspects of risk assessment and management can easily be integrated into this documentation process. Likewise, the corresponding documentation obligation can be alleviated by means of referral to central services with known commitments to information security.

6. Handling of incidents

The basis for dealing with incidents should be recognition that absolute security cannot be created in any information security system. The goal must therefore be to achieve the highest possible degree of resilience, in other words, to return to a functional system status as quickly as possible after an attack.

Clear-cut responsibilities should be defined, e.g. for incident response teams[4], for operational measures in the case of incidents. This also includes procedures for the internal and external communication of incidents. Due to legal requirements, notification obligations also exist with particular regard to data protection incidents. It is advisable to consult with the press and communications office. The reported incidents also create a foundation for drawing up the situation report on information security at the university. To prevent reports from being withheld, careful management must be ensured and there must be understanding for the occurrence of incidents.

7. Resources

The proposed approach of proceeding incrementally is consistent with the aim of using resources efficiently. Nevertheless, leadership of universities must make sufficient resources available so that the targeted security level can be

[4] Groups prepared to respond rapidly; other possible designations are 'incident response task forces' and 'incident protection teams'.

reached. The resources required for the establishment of an information security management system mainly arise from the preparation of the strategy, implementation and operation. In principle, it is advisable to rely not only on internal expertise, but to also make use of external support.

Proposal: make use of use external support
Universities can access support in all phases from the following institutions

- DFN-CERT Services GmbH
- AKIF, the German Research Institutions' Information Security working group
- German Federal Office for Information Security (BSI)

The German Initiative for Network Information (DINI) also has expertise at its disposal. In proposals submitted to the DFG, funds can also be obtained for preparing data generated in a DFG-funded project. There are also other service providers in the marketplace.

When preparing a concept, various expenses for internal and external consultants should not be underestimated. The personnel costs required for the establishment and operation of information security processes are also often underestimated. Naturally, the exact resource requirement depends on the scope and complexity of the information security management system to be established. In order to operate the information security management system, staff resources must also be made available, e.g. for awareness and training measures. The funding agencies must make additional resources available within the framework of basic funding.

8. Cooperative arrangements for information security

Given the intense use of resources mentioned, cooperative arrangements are worthy of consideration. In the case of consortium structures, it should be noted that not only the consortium leadership but also the respective university are responsible for information security. Local cooperative arrangements are particularly beneficial for smaller universities that, given their facilities, are not able to come up with the critical mass of resources required for information security processes by themselves. In any event, the recommendations of the German Council of Science and Humanities on regional cooperative arrangements between scientific institutions should be taken into account.

Cooperative arrangements can be extended to the following areas, for example: development of state and group concepts, communications concepts for incidents, training measures, exchange of experiences and purchasing cooperatives as well as peer audits or peer penetration tests[5].

In order to achieve synergies, standardisation and comparability as well as clear policies are required, especially in administration. Certifications or uniform Business Continuity Management (BCM) concepts can also help lay the

[5] Comprehensive mutual security tests of individual computers or networks.

groundwork for comparable structures. In addition, the community – consisting of universities and service providers – can establish cooperative platforms, good pseudonymisation or anonymisation tools, and open, easy-to-use encryption tools.

Standardisation and comparability are limited by the heterogeneity of universities. This means that it is not always possible to have a uniform model for all participating universities. For this reason, graded solutions must be an option for both scopes of application and security levels with regard to adequacy. These scopes of application and security levels must be negotiated between the cooperating universities. In addition, it would seem advisable not to set the number of participating universities too high, so that the structures developed do not become overly complex. Cooperative opportunities can be limited by competition between universities.

In principle, cooperative structures should not be seen as relieving individual responsibility. Instead, the persons responsible at the university ought to focus on the potential synergies arising from cooperation, while being aware of their own responsibility at all times.

9. Certifications and audits

The necessity of certifications generally results from external professional guidelines of authorities and funding agencies or from cooperation with industry. Certifications as well as internal and external audits form the third line in the Three Lines of Defence[6] model (the first line comprises the operational level, the second line the owner of the information security process). Reputable institutions (e.g. BSI-certified auditors, TÜV) can be considered as potential certifiers. In this context, it should be noted that there is currently no general certification obligation for universities. Self-audits, peer audits and other external audits are also conceivable. Audits and self-audits are associated with increasing requirements in this area.

The critical decision on certifications comes down to clarification of which certification should be sought in the first place (e.g. pursuant to ISO 27001, BSI basic protection). At the same time, it is important to consider which procedures are or will be required for industrial cooperation. Certifications and audits or processes based on these may also become competitive advantages. Certifications should therefore not be pursued as a goal in themselves, but rather always from the perspective of adding value to the institution.

[6] The model for a systematic approach to risks that can occur in businesses and organisations originated from the European Confederation of Institutes of Internal Auditing (ECIIA).

Annex

Definition of information security protection goals according to DIN/ISO/IEC 27000:

Authenticity: An entity's property of being what it claims to be

Confidentiality: Property that information is not made available or disclosed to unauthorised persons, entities or processes

Integrity: Property of safeguarding the accuracy and completeness of assets

Availability: Property of being accessible and usable by an authorised entity on demand

Accountability: Responsibility of an entity for its actions and decisions

Non-repudiation: Ability to evidence that an alleged event or an action occurred and the responsible entities in order to resolve disputes regarding the occurrence or non-occurrence of the event or the action and the involvement of entities in the event

Reliability: Property of consistent intended behaviour and results

About the creation of the guidelines

These guidelines were prepared by the HRK Standing Committee on Digital Infrastructures. The Committee is headed by the HRK Vice-President for Digital Infrastructures, Professor Dr Monika Gross. The standing members of the Committee are Mr Malte Dreyer, Professor Dr Petra Gehring, Professor Dr Gudrun Gersmann, Professor Dr Hannes Hartenstein, Professor Dr Wolfram Horstmann, Dr Antje Kellersohn, Professor Dr Norbert Lossau, Mr Jens Andreas Meinen, Professor Dr Joachim Schachtner, Professor André Stärk, Professor Dr Gudrun Stockmanns and Dr Beate Tröger. The Committee is supported by Dr Elmar Schultz at the HRK Head Office.

A hearing on 11 October 2017 laid the foundations for the paper. The following persons were consulted at the hearing: Mr Alexandros Gougousoudis (Head of Service Center IT, Berlin), Mr Klaus Keus (Federal Office of Information Security), Dr Jan K. Köcher (Team Leader CAT in DFN-CERT), Professor Dr Gudrun Oeval (Head of IMT, University of Paderborn), Dr Hans Pongratz (Vice-President and CIO, TU Munich), Dr Helfried Broer (Deputy Chief Information Security Officer, FhG) and Professor Dr Sebastian Schinzel (Information Technology, University of Applied Sciences, Münster).

The HRK would like to thank everyone involved for their contributions.