Higher Education Information Security Programme – HEISP

“The universities know their information security risks and create trust through information security management!”

Information Security Unit of the Bavarian State Universities

Version 1.0 – final

Table of contents

1 Role and mission

The Ministerial Council Decision on the IT strategy of Bavarian universities of 19th January 2011 confirmed that the universities shall continue to be responsible for the further development of their IT infrastructure. This places the responsibility for ensuring information security with the universities and their management.

To fulfil this responsibility, *Universität Bayern e.V.*, association of the Bavarian research universities, and *Hochschule Bayern e.V.*, association of the Bavarian universities of applied sciences, have jointly adopted the *Grundsatzpapier zur Informationssicherheit an bayerischen Hochschulen* (policy document on information security at Bavarian universities). Given the special importance of research data and information, this document describes the risks specific to universities and the organisational and technical measures that are generally necessary to prevent or minimise damage in the event of an attack. Furthermore, the universities are also urged to implement an information security management system (ISMS).

The establishment of an ISMS should ideally be based on the recognised standards of the ISO 2700X series. For various areas of responsibility, these standards describe how to analyse and deal with risks and give very specific instructions for organisational and technical measures. An ISMS supports the sustainable maintenance of an adequate level of information security by encouraging the definition of measures to strengthen information security based on a risk analysis, the implementation of these measures, regular monitoring of their effectiveness and the performance of any necessary adjustments. As the standard is technology-neutral, the concepts prescribed, when implemented, need to be adapted to the specific situation of the respective university, depending on their organisational, operational and technical circumstances. This brings with it, in particular, a substantial organisational effort.

The Information Security Unit was created to support universities in introducing an ISMS and implementing specific measures to ensure information security. To enable it to fulfil its tasks in a structured manner and at minimal cost to the universities, the creation of a general Higher Education Information Security Programme (HISP) is suggested; the universities can then use this as a blueprint for their own ISMS.

The Higher Education Information Security Programme (HISP) describes steps towards the implementation of an ISMS at universities and is intended to monitor the status and implementation level at the individual universities.

The structure of the HISP follows the phases that the introduction of an ISMS typically entails. The universities can choose to start following this ideal process from any point onwards, depending on the specific circumstances prevailing at each university. The HISP ensures that all phases will be completed by all universities within a reasonable time-scale, which in turn ensures that the local university-specific ISMS will be completed.

This programme is not intended to offer an alternative to steps already taken by individual universities, but rather offers options for continuing and adding detail to these steps in the complex environment of universities with their partly very high needs for protection.

2 HISP – programme steps

2.1 Overview

Security is defined as an individually experienced state of trust, and so cannot be defined in general terms. There are, however, best practice approaches to strengthen this trust that we are doing what is right.

The most efficient way for university management to follow this security programme for the Bavarian universities is to consistently complete all defined steps. Completing only the first steps, or a selection of easily achievable goals, will lead to partial improvements in the short term but will not create a holistic process to ensure information security.

Advice on introducing the ISMS and active support in the form of model documents and model processes are available from the central Information Security Unit. This support is intended to help with the process but does not replace the need to create information security approaches and manage information security locally.

The programme is divided into several steps, which are detailed in the following.

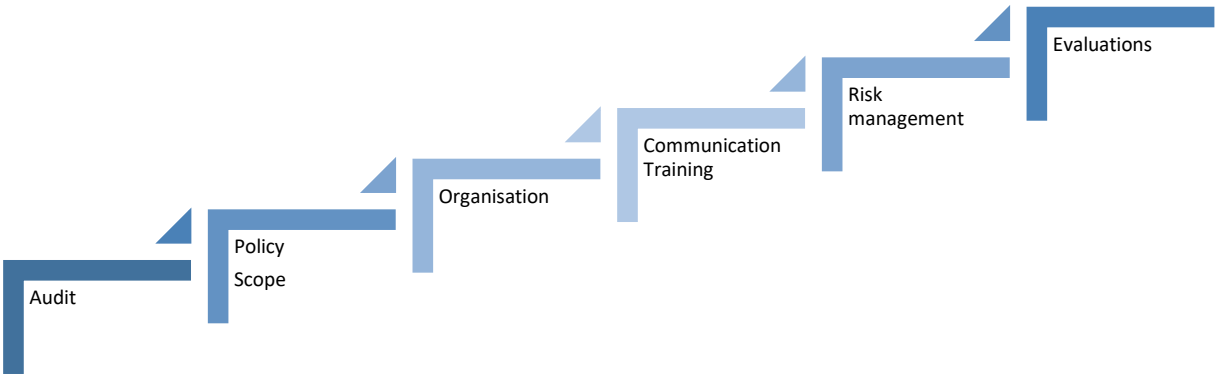

Figure 1: Steps in HISP

2.2 Survey of the status quo (audits)

At the beginning of the process of introducing an information security management system we recommend completing an optional audit (initial survey of the status quo). The resulting insights on which structures need improvement or are already well developed can inform the university of issues to be prioritised and help create an understanding of the perspective of the standard. Since 2017 the Information Security Unit has performed information security audits at one third of all Bavarian universities.

Later audits should be obligatory and take place every two to three years, in order to guarantee an independent review of the status of information security. Ideally, these audits are carried out not only by the information security unit, but additionally alternating audits are carried out by internal ISO 27001 auditors at the university (this is currently the case at the *LRZ* (Leibniz Supercomputing Centre of the Bavarian Academy of Sciences and Humanities) and the University of Bayreuth).

2.3 Policy

The Information/IT Security Officers in the information security working group have developed a model policy document. Even if there is already a policy, it should be checked against the model policy, to ensure it is up-to-date.

At the same time, a project needs to be set up with the aim of developing an information security management system (ISMS) that is adapted to the needs of the individual university. The overall project plan can be based on the steps in the HISP programme.

The policy is supposed to cover the whole university and all members of the university. This very broad scope can be an impediment to the introduction of an ISMS with resulting implementation measures. The Information Security Unit therefore recommends starting with necessary, established and centralised IT services or processes (such as central user administration, network management and campus management) and initially introducing the ISMS for a limited, manageable area.

2.4 Organisation

Pre-requisites and cornerstones need to be defined for the level of security to be attained, as security measures depend on the value or need for protection of information. These tasks may be delegated by university management to an existing or newly established organisational structure. This structure with functions (such as Information Security Officer), committees and tasks needs to be documented and formally approved in the form of a regulation.

A model regulation is provided by the Information Security Unit, which needs to be revised and adapted locally.

2.5 Communication / training

Security is achieved through technical and organisational measures. Training courses and communication channels about the information security measures need to be established to encourage security-conscious operation by those involved.

The Information Security Unit provides a training and data protection plan. This can be integrated into existing learning programmes (e.g. on Moodle). The universities need to establish to what extent participation in such training courses should be mandatory for staff.

2.6 Risk management

Risk management is introduced relatively late compared to the ISO standard; this is based on the insight from the survey of the status quo in 2017 that all participating universities already have approaches to risk management, and the topic is generally handled informally and at the discretion of those responsible.

The local ISMS is based on identifying, recording, assessing and dealing with risks at the respective university. The starting point for this has to be a previously performed analysis of need for protection as well as documented threat scenarios.

Experience with different risk management tools is collected and made available by the Information Security Unit, and if desired a framework agreement can be negotiated for all or participating universities in Bavaria.

2.7 Reports, improvement

Possible reporting items are already to be taken into consideration while developing the ISMS. Sensible effectiveness checks for the different processes and measures are to be selected and performed regularly. The Information Security Unit provides help in selecting suitable performance indicators. Alternatively, ISO Standard 27004 can help you to develop appropriate key performance indicators (KPIs).

For independent internal audits, building a pool of ISO 27001 auditors within the Bavarian universities is recommended. Auditors can then help each other with outsider perspectives. A general capability maturity model (see 3.1 Capability maturity model) is used to assess the level of implementation at each university, and also to be able to compare the Bavarian universities to each other (‘security map’).

2.8 Gradual development of a university-wide ISMS

An existing ISMS can be expanded gradually to include the whole university by expanding successfully developed elements of the system from the initial/reference institutions to other areas.

Furthermore, a healthy continual improvement process ensures that the ISMS focusses on the most urgent issues when it is introduced and that it then progressively improves security levels.

When new requirements arise, these need to be assessed and necessary changes implemented, first in the reference area, then in all other areas. Any necessary divergence from information security approaches is to be assessed and documented according to the provisions for risk assessment.

3 Framework conditions for monitoring progress

3.1 Capability maturity model

In 2017, mini-audits were conducted at one third of all Bavarian universities, to survey the status quo. The following conclusions can be drawn:

The universities offer central services and support for operating IT systems in teaching and research as well as administration. There are hardly any systematic procedures or procedures that are organised in the same way for the entire university. It is currently the responsibility of individual Information/IT Security Officers (or heads of computer centres) to achieve organisational changes or to structure processes according to information security aspects and to document these processes. Technical improvements and progress occur within the scope of the respective possibilities (budget) and dependent on the individual level of knowledge of the respective administrators. Many technically convincing solutions have been developed in this way, but these are mainly based on the knowledge of individuals. The same is true for IT security solutions.

Now, the need to start a continual and above all comprehensive improvement process has become urgent; this process should not be based on a collection of isolated solutions developed by individuals but should (eventually) be applied throughout the entire university. Such a structured procedure can only be ensured by the introduction of an information security management system (ISMS).

Future audits to regularly survey the status quo (external or self-assessment) will then be evaluated according to the capability maturity model stipulated in ISO/IEC 21827 and made available in the CIO meetings ('security map'). This procedure will make it possible to compare the current status quo across universities, and also give a clear and detailed status irrespective of which standard is implemented.

Based on ISO/IEC 21827:2008 (System Security Engineering – Capability Maturity Model, SSE-CMM for short), the capability maturity model is structured as follows:

Capability level	**Meaning as defined in ISO 21827**
Non-existent	There are no security measures or plans.
Performed informally	Basic security measures ('base practices') exist and are implemented **on an ad hoc basis**. There are general regulations on how to perform certain tasks. There is no monitoring, adaptation or reporting for these regulations.
Planned and tracked	Basic security measures are planned, introduced and are **repeatable**.
Well-defined	In addition to planning and tracking, processes are **documented**, **approved** and implemented **throughout the university**.
Quantitatively controlled	In addition to documentation, there are **measurable** goals and performance is **reviewed** (e.g. audit).
Continuously improving	Processes are **regularly reviewed** and **adapted**. Improvements occur in response to identified impacts of weaknesses.

Figure 2: Overview of the capability levels as defined in SSE-CMM (ISO21827:2008)

3.2 Milestones

The HISP is based on recognised standards and divided into several steps. Based on the insights from the survey of the status quo in 2017, the following milestones have been defined (note: the years given are a rough guideline for the Information Security Unit). Every university can take additional or different measures or apply different timings. As the current status differs considerably between universities, there is little to be gained from binding rules/agreements.

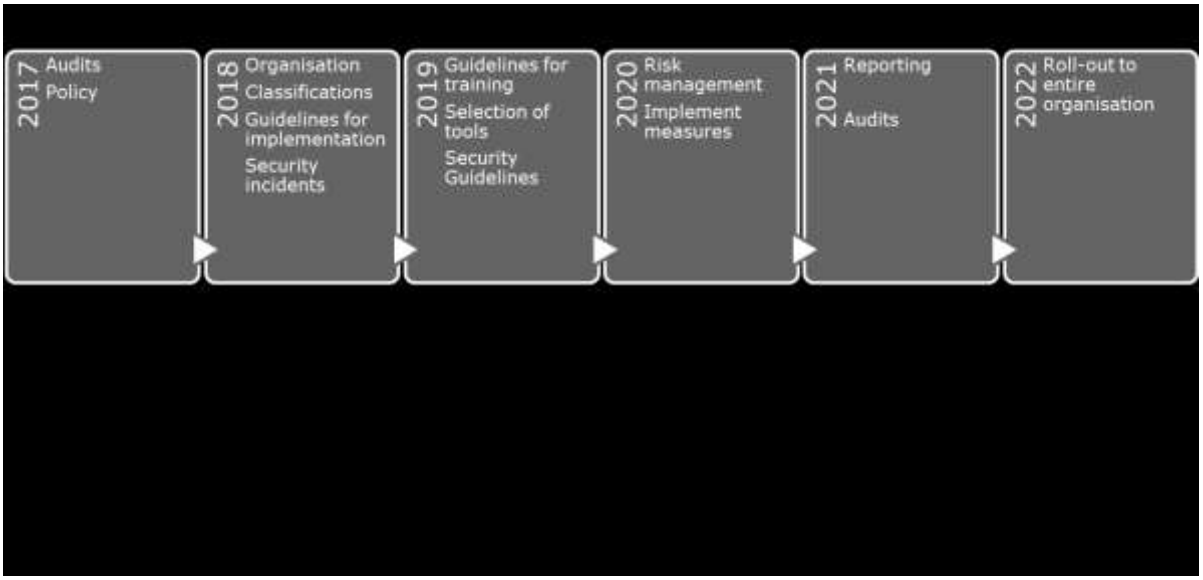

Figure 3: HISP milestones

3.3 Improvement

As the HISP is a medium-term project, it is to be expected that there will be changes or joint projects or tenders developed by several universities, with the aim of encouraging synergies. Agreeing to this programme allows the universities to participate in any such implementation projects or to buy relevant products, but there is no obligation whatsoever to do so. Specific needs for such cooperative projects or tenders, and whether to participate, need to be clarified as part of the project planning of each university, and should not impede continuation at individual universities. The programme needs to be adapted to new goals and requirements if the framework conditions change (for example changes in the standards it is based on). This should be reviewed based on the yearly summary report to the CIOs.

4 Further steps, governance

An ISMS should be seen as a procedure for continual improvement of information security at universities. In order to develop an adequate ISMS at a university, it is indispensable that the respective university management establish assessment, steering and monitoring procedures.

This means that information security governance procedures can be established in connection with the IT strategy, in order to allocate resources effectively (see ISO27014:2013 standard).

In doing so, the following principles need to be considered:

- Should be scalable to the entire university
- Risk-based approach
- Steering resource allocation
- Conformity with internal and external requirements
- Encourage a security-conscious environment
- Review effectiveness in relation to requirements

The Information Security Unit offers services targeted specifically at supporting universities with the introduction and implementation of an ISMS and with implementing measures resulting from it. Services include providing model documents, ensuring a consensus is reached in assessing risks with a view to stipulating appropriate security measures, or coordinating the selection of software tools. Also, audits to survey the achieved information security status can be implemented or supervised. It is the responsibility of the Information Security Unit to continue and update these services.