ISMS purpose, components, and Statements for the Overall security policy

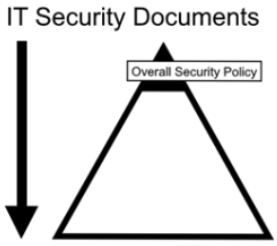
By Jonas Blocher

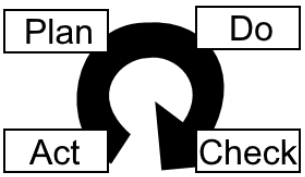
The main business goals of the University of Applied Science Ulm (THU) are **educating** students to be able to quickly adapt to new problems and get a deep understanding of their fields, to certify their graduation in a fair and comparable way and contributing to the **technical** and **ecological development** of the region by driving forward **research** projects in cooperation with partners from business and science.

To achieve these goals an **I**nformation **S**ecurity **M**anagement **S**ystem (ISMS) is crucial:
An ISMS helps managing and thus improving the security of information in any organization by providing a standardized framework to address any risks related to information security.
In fact, an ISMS helps the THU to maintain high **availability** of material and systems required for **education**, must secure the **integrity & confidentiality** of student's personal data (according to the **EGDPR**), grants the **integrity** of student certificates and ensures **confidentiality & integrity** of the THU's **research findings**.

An ISMS must assign responsibilities for managing security to specific roles in the organization:
The **C**hief **I**nformation **S**ecurity **O**fficial (CISO) as head of management and multiple **I**nformation **S**ecurity **O**fficials (ISO) for the specific topics.
To minimize risks, they must first be identified. A useful tool to identify the security requirements of all information assets is performing an analysis regarding **C**onfidentiality, **I**ntegrity and **A**vailability (CIA Analysis).

The **documentation** of an ISMS is structured **hierarchically** in a pyramid following a top-down scheme with short general documents like the general security policies at the top and a way larger amount of specific low-level documents like instructions & manuals at the bottom of the pyramid.

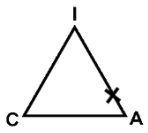




Any ISMS must have a process to continuously improve it (CIP). A good way is to follow the PDCA cycle: Start **p**lanning (by identifying risks & measurements), continue **d**oing (implementing the measurements), **c**heck if they were successful (in reducing the risks), **a**ct (extend measurements) and keep repeating this cycle.

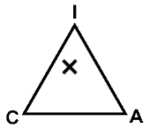
Definition & Objectives

The objective of information security is to enable the University of Applied Science Ulm to ensure that high levels of education, certification and research are maintained and to minimize the risk of security threads. Therefore, security incidents should be prevented, and their potential impact should be reduced.



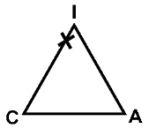
Education:

High availability must be maintained to make sure continuous lessons can be held without interruption, integrity of materials is also required



Research:

Integrity of research findings is the highest priority. Confidentiality of research papers must be ensured if findings are under non-disclosure.



Certification:

Integrity must be ensured with high priority to prevent loss or changes in certificates under any circumstances, also they must be confidential

Principles

- **Need to do:** Permissions & information should only be given if required to fulfill tasks
- **Clean Desk:** When leaving the workplace, no data should be left accessible
- A **C**ontinuous **I**mprovement **P**rocess should be established
- **Segregation of** Educational & Administrative **networks** must be ensured

Roles

In order to achieve an appropriate level of information security, a security organization will be implemented, headed by the **C**hief **I**nformation **S**ecurity **O**fficial (CISO) with multiple **I**nformation **S**ecurity **O**fficials (ISO) for specific topics. The CISO is responsible for maintaining the policy. All ISO's should provide support and advice for implementing it.

The rectorate must enforce the policy and ensure staff and students comply.

Processes

All security breaches must be reported to the CISO.

The CISO is in charge to implement a Business Continuity Management (**BCM**) plan. This plan provides processes to identify potential threats, the impact of those threats and what needs to be done to recover after a disruption.

Topic specific policies

Topic specific policies should be written by the ISO's. These topics include:

- Access control
- information classification (and handling)
- physical and environmental security
- end user oriented topics
- backup
- information transfer
- protections from malware
- management of technical vulnerabilities
- cryptographic controls
- communication security
- privacy and protection of personally identifiable information
- supplier relationships

Additional topics & policies not included in this list might also be added if desired.

This document is approved by the CISO (Chief Information Security Official):

_____	25.10.2021
Signature	Date