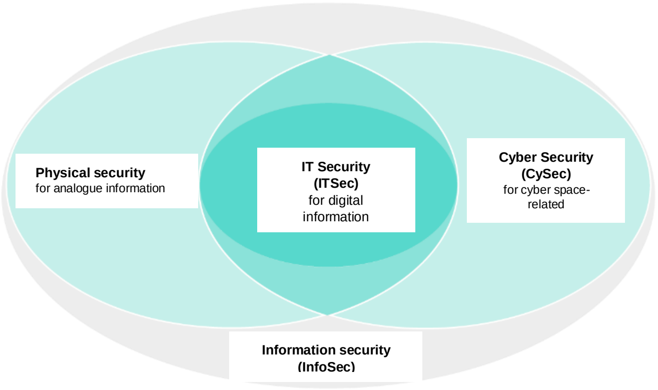
Information Security Report

Zug, 6 January 2025

1 Background

The Zug Estates Group operates a number of initiatives relating to information security, which are always geared to statutory requirements, industry best practice and the size of the company.

With the support of IT experts, high security standards are set for the whole of the Zug Estates Group, which are continuously adapted to current circumstances and which cover all relevant systems.



1.1 Information security

Information security protects all data necessary for business processes and the technical data processing systems with appropriate and effective measures both in the technical and non-technical (organisational) environment. Here, the measures aimed at minimising risk follow the requirements of the protection targets confidentiality, integrity and availability

1.2 Cyber security (IT security)

The topics of overarching cyber security are assessed periodically and implemented in specific recommended actions. The stipulated principles apply for all areas of the Group and are prioritised on the basis of a risk assessment.

An emergency manual exists for the event of a cyber emergency (IT Service Continuity Management). It sets out detailed specifications, precautionary measures, emergency management, organisation and communication.

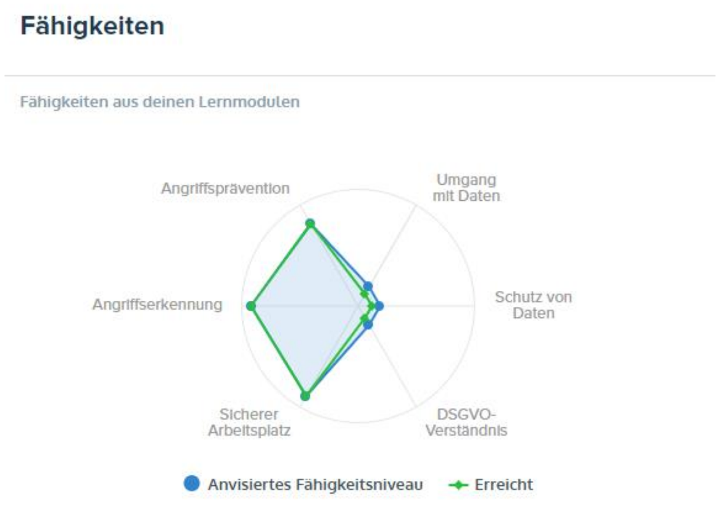
1.3 Data protection

Data protection is very important and is dealt with periodically as well as during current operation by a panel of responsible specialist units. Implementation of data protection is geared to statutory requirements in Switzerland and abroad and is implemented together with experts.

2 Employee training

As part of the "Cyber Security Awareness" programme, all employees must develop a basic knowledge of IT security and compliance. This also applies to new employees, who are required to achieve a certain level of learning within three months.

All learning content is grouped in modules and is available on a learning platform. All learning modules include a case study and the necessary theory. A module is deemed to have been completed as soon as a brief test has been successfully passed. The Digitalisation & IT Services department monitors the learning activities and ensures that they are completed. Content is updated each year in the form of refresher courses.



An ability matrix (see example above) shows employees the status of their learning progress.

In addition to basic knowledge, employees are tested regularly with phishing simulations. Refreshers are conducted to maintain the level of knowledge. Once a year, employees are presented with a current case in order to increase their awareness of the topics.

3 Organisation

The Head of Digitalisation is responsible for information security. The Group Management is informed several times a year and the Board of Directors once per year about the current status of information security.

In the Cyber Security Advisory Trust, a quarterly exchange with suppliers takes place, where current cyber security topics, among other things, are discussed.

Regular external security audits, ongoing in-house training programmes and the conclusion of cyber insurance ensure that the necessary organisational measures have been taken.

4 Security-related incidents

To date there have been no breaches of information security. The last security-related incident – which did not involve any data outflow – was in 2019. Zug Estates is not aware of any data outflow or security-critical incidents at its suppliers or business partners (third parties).

5 Assessments and audits

In 2023, Zug Estates conducted an assessment of the US-based National Institute of Standards and Technology (NIST) in the field of cyber security[1]. The assessment was performed in accordance with the requirements of the NIST and Switzerland's ICT minimum standards[2], which apply to critical infrastructures. This industry-independent and technology-neutral framework serves to identify action fields. It highlights strengths and weaknesses of proprietary IT and derives specific measures.

As part of the regular audit for the 2023 financial year, an IT audit was conducted – based on the voluntary IT audit of 2021 – that again checked the measures taken.

[1] https://www.bithawk.ch/services/cyber-security-nist-assessment

[2] https://www.bwl.admin.ch/bwl/en/home/bereiche/ikt/ikt_minimalstandard.html