IT Security Guideline

Motivation

This Security Guideline describes the positioning of information security (IT Security) at HOCHTIEF. The guideline relates to own activities but also clearly shows what expectations HOCHTIEF places on business partners.

The Group strategy is based on comprehensive risk management. Information technology (IT) is an integral part of support for HOCHTIEF's business tasks. Consequently, great value is placed on the security of IT systems and data.

1. Security targets

Achieving an appropriate security level with the use of IT security through technical and organizational **security measures** is not only determined by legal regulations but is part of obligations toward HOCHTIEF's clients and business partners and is designed to protect own interests. Security with regard to the use of information technology is hence in the interest of all parties and is consequently an important target for HOCHTIEF.

The targets to be achieved are in particular the following:

- complying with statutory and contractual regulations
- compliance with internal and external regulations (Compliance)
- protection against access by non-authorized persons
- protection against manipulation of data
- appropriate availability of data and systems

Statutory regulations pursuant to Section 91 (2) of the German Stock Corporations Act (AktG):
"The Executive Board must implement suitable measures, in particular establishing a monitoring system, so that developments which could jeopardize the continuation of the company can be recognized at an early stage."

2. Security measures

The following measures are implemented to achieve the defined security targets:

- establishing and maintaining an **IT security management system**
- defined approach for conception, implementation and updating of an **IT security policy** that is suitable for dealing with risks and economically appropriate
- communicated processes on **risk evaluations for applications for exceptions**

2.1. IT security management

The planning, implementation and maintenance of IT security is ensured by the IT security organization, which supports the Executive Board. The IT security organization consists of

- the Chief Information Security Officer (CISO) of HOCHTIEF Aktiengesellschaft and
- the CISOs of the divisions (CISO Divisions).

Sufficient financial resources and time are invested in the IT security organization, to enable it to properly perform its information security tasks.

To ensure that all places within the organization promote the issue of IT security in the sense of the Executive Board, the Executive Board delegates responsibility for implementation to the divisions (IT Security Policy part of the IT Directive).

Within the divisions, IT Security is part of the individual IT Steering Committees. The IT Steering Committees are composed of representatives of the management boards and the operational IT.

2.2. IT Security Policy

The CISO prepares an IT Security Policy, which describes appropriate and effective security measures. On the basis of statutory and business framework conditions, the risk situation and the latest technical possibilities, the CISO updates the IT Security Policy according to requirements. The **measures** defined in the IT Security Policy are in each case allocated to one of the two levels “normal“ and “high”.

The divisions ensure that the IT Security Policy is specified, communicated and implemented within their division. Furthermore, **security incidents** must be reported to the CISO, respectively the CISO Division.

All employees are obliged to comply with the Directives at HOCHTIEF in accordance with their employment contract. The managerial staff ensure compliance and implementation.

On the basis of a questionnaire, the specialist areas of HOCHTIEF Aktiengesellschaft and the Divisions determine the protection requirement (“normal” or “high”) for the information available in their sphere of responsibility. The specialist areas implement security measures from the IT Security Policy on the basis of the protection requirement.

Intentional or grossly negligent actions which jeopardize the security of data, information, applications, IT systems or networks are pursued as violations and can be punished by disciplinary measures or measures under labor law.

Should tasks allocated by the company result in requirements which contradict applicable IT Security Policy, these are not allowed to be implemented without previous assessment and require a **risk evaluation** in the form of an application for exemption.

2.2.1. Measures

The latest applicable measures are described in detail in the IT Security Policy, respectively presented in a documentation of the IT security concepts.

2.2.2. Reporting security incidents

Security incidents must be immediately reported via the envisaged notification channels and immediately investigated. If necessary, the resulting findings are taken into consideration in the security targets or the IT Security Policy.

2.2.3. Risk evaluation

Via an application for exemption, the specialist department can apply for deviations from the IT Security Policy. On the basis of the specialist department’s information and a technical description, the CISO or CISO Division performs an evaluation of risks and occurrence probabilities. An implementation is only allowed after a positive authorization of the application for exemption by the CISO or CISO Division.