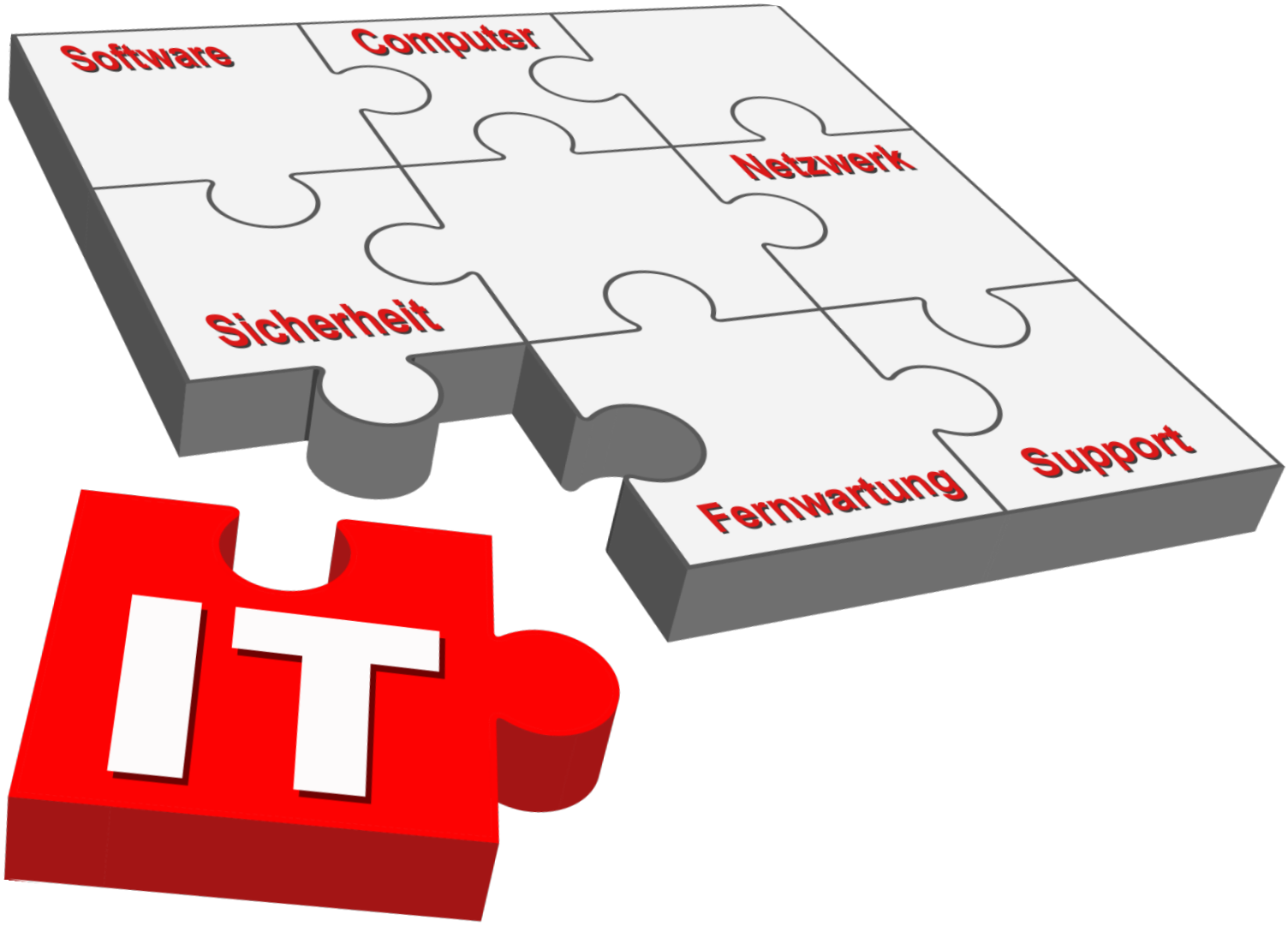
HYDAC INTERNATIONAL

IT Security Directive – External Service Providers

Status: February 2016



1. Scope and purpose

This safety directive is obligatory for all external service providers who work for a HYDAC affiliate. The stipulations are to be understood as minimum requirements for the provision of services within HYDAC.

If these minimum requirements cannot be satisfied by the external service provider, HYDAC will not cooperate with this external service provider.

The most recently approved version of this IT Security Directive - External Service Providers stored at http://hyd.ac/itsicherheit applies.

2. Responsibilities

The external service provider must ensure that the services provided comply with this directive.

- The service provider commissioned must ensure at all times that their actions, and the actions of their employees, do not adversely affect the availability, integrity or confidentiality of the IT systems of HYDAC affiliates.
- Copyrights and patent rights, as well as license agreements, must be observed.
- The access data provided must not be passed on to third parties.

3. Access to buildings and production sites

The external service provider must inform their employees that they must report to their contact person in a HYDAC affiliate company. The external service provider must also inform their employees who are not in possession of a personalised visitor's permit that they will be issued a visitor's permit and the "Security information for visitors" form, and that they must wear this permit so it is clearly visible at all times.

4. Utilisation of HYDAC IT systems and IT infrastructures

Basis and rights of utilisation

The hardware and software used with the HYDAC infrastructure must not adversely affect the security and performance of the infrastructure. Consequently, the service provider may only use products and devices that have been approved by the Central IT Department.

Use of the Internet and the communication infrastructure

All access is protocolled by the Central IT Department for diagnostic and security purposes.

The external service provider must inform their employees that any access to Internet resources or HYDAC email accounts provided may only be used for business purposes.

IT systems in the production environment must not include Internet access.

The use of "cloud solutions" is forbidden.

Hardware and software management

The external service provider may only provide, install or incorporate IT components that have been checked and approved by the Central IT Department prior to their connection to the HYDAC network.

Written documentation must be provided for the approval of hardware and software. As a minimum requirement, this documentation must include the following points:

- Configuration of the network components and functions
- Function of the software
- Interfaces
- Required rights
- Access data

The IT components used by the service provider must support the IT security solutions selected by HYDAC. The external service provider must request these from the Central IT Department.

Modifications to the hardware or software of a terminal (for example, installation of hard disks, memory expansion, WLAN cards) must be coordinated with the Central IT Department. Disposal of IT components must be agreed with the Central IT Department.

When using external storage media (e.g. USB memory stick, external hard disk, USB devices, etc.), please note that only media approved for use by HYDAC may be used.

In addition, the requirement of the document *General IT minimum requirements in the field of HYDAC production* must be observed for IT systems in production, accessible at http://hyd.ac/itstandardproduction.

Network

The HYDAC network infrastructure is operated only by the offices authorised to use it. All modifications that are not authorised by the Central IT Department are forbidden.

Unrestricted network access is permitted only for HYDAC proprietary terminals approved and administered by the Central IT Department.

WLAN components may only be used and operated after consultation with the Central IT Department.

5. Minimum safety requirements

The external service provider must ensure that the hardware he provides has the current version of an anti-virus system with current virus signature database installed.

This anti-virus system must include the following components:

- On-access scanner
- On-demand scanner
- Email scan
- Host intrusion prevention system
- Local firewall

At least one weekly full scan of the system is mandatory.

The current updates for the operating system and the software used must be installed and checked for validity at least once per quarter.

Furthermore, the external service provider must ensure their employees receive instructions on IT security. If personal data are required to provide the service and/or access to personal data cannot be ruled out, the external service provider must ensure that their employees are instructed and obligated in accordance with § 5 BDSG (German Federal Data Protection Act).

The transfer of data from HYDAC affiliates to third parties is not permitted, unless special approval is granted.

All email traffic between HYDAC and the external service provider must be treated confidentially.

The non-encrypted storage of HYDAC data on mobile data media (e.g. USB sticks) is not permitted. Exceptions shall require special authorisation from the Central IT Department.

Data of all types generated in the course of job processing for HYDAC affiliates are the property of the HYDAC company that commissioned the work.
After completion of the work, all data produced must be returned to the HYDAC company that commissioned the work, and no copies, excerpts or other full or partial reproductions retained.

6. Handling of technical faults

The external service provider must inform their employees that any faults which occur during operation or any IT security issue that arises must be notified immediately to the HYDAC contact person.

7. Regulations for user accounts provided

The access rights assigned and use of personal or other corporate data shall apply only for fulfillment of the subject of the contract.

The external service provider must ensure that every employee engaged can log in using the user account assigned. The user account and password must no be divulged to third parties. The password must comply with HYDAC regulations.

On termination of the service contract, the external service provider must ensure that their employees return all ID cards and issued data carriers to HYDAC. User accounts of the external service provider that are no longer required must be notified immediately to the Central IT Department for deactivation.

8. Remote maintenance / remote access

Local access to the HYDAC network must always be preferred to remote access. Remote access is possible only after consultation with the Central IT Department and in compliance with the regulations stated below.

- The remote access for remote maintenance is provided only via the HYDAC SSL Gateway, no other options are supported.
- The external service provider must ensure that the in-house employee network does not allow uncontrolled access to the HYDAC network.
- Only connections and/or software approved by the Central IT Department may be used for remote access.
- No IT system may establish a VPN connection autonomously.
- The external service provider is obliged to test the remote-access functionality at least once per quarter.

9. Performance

Software

If the external service provider provides services in the field of software development, the following regulations shall apply in the order stated:

- General Terms and Conditions for Purchasing and
- Special Terms and Conditions for Purchasing Software Products and/or
- Special Terms and Conditions for Purchasing Machinery and Installations.

It must be ensured that the source code is available for developed software products. The following options are available here:

- Handover of the source code and the development environment.
- Deposit of the source code and the development environment with a notary.

Hardware

The hardware must be designed in compliance with internal regulations as agreed with the contact person at HYDAC.