techem

Overview of the Security Organization and Architecture

1 Introduction

The security architecture of the Techem Group follows a defense-in-depth strategy and extends across the various security layers in line with best-practice approaches. The frameworks used for the security organization and architecture are primarily the ISO 27000 series of standards, the National Institute of Standards and Technology (NIST), and the German Federal Office for Information Security (BSI).

2 Organizational Security

2.1. Certification according to ISO 27001 and ISMS

The information security management system (ISMS) of the Techem Group is certified according to ISO 27001 in certain areas. The scope of the certification is defined in the respective certificate (currently: core IT systems and related support processes, including Techem Solutions). Initial certification was obtained in 2022 in accordance with DIN EN ISO 27001:2017. Recertification took place in 2025, including the transition to the new standard version DIN EN ISO 27001:2022 and the extension of the scope of application to Techem Solutions.
The ISMS comprises the Information Security Policy, the Information Security Management Policy, the Information Security Management Manual, and the subordinate relevant policies. Risk management is a core component of the ISMS and is monitored by the security organization.

2.2. Security Organization

Techem's security organization is a group function and is responsible for all Techem companies. It consists of the Head of Information Security and their team, as well as the Head of IT Security and their team. The Head of Information Security has overall responsibility for all security-related matters and has the right to report directly to the management and the Advisory Board at any time. Where security matters are concerned, the Information Security department has authority to issue instructions. The IT Security team is reachable 24/7 through on-call duty.

2.3. Audits

The teams regularly conduct audits covering Techem's foreign subsidiaries as well as strategically critical service providers. The audits usually take place at a defined cadence and are planned anew by the teams each fiscal year. In addition, event-driven audits may be conducted at any time.

2.4. Training, Education and Awareness

Regular training, education and awareness measures are conducted in various formats. The primary e-learning module on information security is rolled out annually to all employees via the central Human Resources (HR) system; participation is mandatory and is tracked by HR up to management level. It is also mandatory for external staff and subcontractors. Regular live phishing simulations are carried out by a specialized service provider. In addition, training on specific topics is conducted regularly and selected and carried out based on the relevant occasion. This also applies to the security teams themselves with regard to specialist training.

2.5. Advisory Support for Business Departments

Techem's security organization advises business departments, employees and projects, thereby ensuring that security-by-design principles are observed.

2.6. Outsourcing and Service Providers

In the area of security, service providers are used for various areas, including:

- Managed Security Services
- Incident Management and Security Operations
- Penetration testing, red teaming and advisory services
- Phishing simulations, e-learning modules and specialized training

3 Physical Security

Access to buildings and office areas is restricted by card readers and company ID cards. Guests must register, receive visitor badges and may not move around internal office areas unattended. Particularly sensitive areas have dedicated access authorizations that are granted only after a multi-level approval process. The buildings are partially monitored by video and motion detectors.

Techem's IT is fully outsourced, meaning that no server rooms, data centers or similar facilities are located in Techem buildings.

4 Technical Security

4.1. User & Access control

User management is performed centrally and covers both on-premises systems and cloud applications. Multi-factor authentication (MFA) is used across the board; authentication via single sign-on (SSO) is preferred. Administrator rights are assigned to separate user accounts that cannot be used for everyday work and are granted only according to a defined process involving several approval instances. As a general rule, these rights are time-limited and are audited regularly. The password policy requires long and complex passwords that do not have to be changed periodically. User accounts for external users are generally time-limited. All user rights are assigned according to the principle of least privilege. Rights and roles are managed centrally in user management; rights and roles within specialist applications are the responsibility of the respective system owner.

4.2. End Devices

Centrally managed laptops are used throughout. In addition, access to the Techem IT environment is possible via virtual applications. After successful authentication, the laptop automatically establishes a VPN tunnel. Without this tunnel, the laptop can only be used offline and there is no access to internal or cloud-based systems. When the VPN connection is established, the status of the device is checked; the connection is established only if the device is classified as compliant. Patch management is ensured centrally by the IT service provider.

Access via mobile devices (smartphones, tablets) can only be provided through managed devices. Mobile Device Management (MDM) is used for this purpose. The app store is highly restricted and only previously reviewed and approved apps may be used. Bring-your-own-device (BYOD) is possible only for smartphones or tablets and is likewise handled exclusively through MDM. The hard drives of end devices are encrypted.

4.3. Network and Internet

The internal network is divided into several logical network zones that are separated from each other by firewalls. The production environment and non-production systems are segmented into different environments. External access is possible only via a demilitarized zone (DMZ) or via site-to-site VPN; access via clients is possible exclusively through a Virtual Private Network (VPN). The networks at the sites are secured by Network Access Control (NAC).

The central cloud environment is located in the EU and is configured redundantly; the security policies are managed centrally by the security organization.

All internet access is routed through a central cloud proxy, which ensures security during browsing by means including SSL inspection, blacklists/whitelists and sandboxing. A Cloud Access Security Broker (CASB) ensures that unknown cloud applications cannot be used and additionally prevents uncontrolled data leakage.

4.4. Servers and Databases

Servers and databases are almost fully virtualized and distributed across two data centers, each of which can take over the work of the other (active/passive configuration). They are located in different network zones and, with the exception of development machines, can be reached only via jump servers in the internal network. All servers use hardened standard images and are subject to standardized patch groups. Changes to systems are approved only through a change process in which the security organization is involved.

4.5. Storage, Backup and Archive

Storage is primarily provided via cloud storage. Backups and the archive are kept in a dedicated third data center; an additional backup in the cloud is performed regularly.

4.6. Communication

The primary means of communication are e-mail and instant messaging. Protective mechanisms for e-mails include spam and phishing protection, link and attachment protection, and sandboxing. Encryption using TLS 1.2 is enforced; the use of S/MIME is possible.

4.7. Applications

Standard software is rolled out and kept up to date via central software distribution. Individual software must be requested and is reviewed by several instances before approval; these applications are also packaged and rolled out. Own installations using local admin rights are the exception and are mainly limited to users with IT knowledge who require these rights for their daily work.

Company-wide applications are reviewed and approved as part of the purchasing processes before implementation; this also applies to pure SaaS applications.

4.8. Certificate Management

Techem uses its own Public Key Infrastructure (PKI) to create certificates for various purposes. Two strands exist (RSA and ECC); the certification policy and certificate revocation lists are published at ca-rsa.techem.de and ca-ecc.techem.de, respectively.

4.9. Penetration Testing and Security Reviews

Techem's security organization regularly conducts penetration tests and security reviews. These are defined and planned in line with the audit plan. Penetration tests are largely carried out by external, specialized service providers. Projects with significant impact on day-to-day operations (e.g., new customer portals, interfaces for automated data exchange, remote reading infrastructure, etc.) are also reviewed after a risk assessment and before commissioning; go-live takes place only after a successful review by an external service provider.

4.10. Data Leak Prevention (DLP) and Information Classification

Techem has introduced information classification; labeling documents before electronic storage in Office applications is mandatory. E-mails must also be classified. Publicly available AI systems have been blocked to prevent the leakage of sensitive data. Outside the secured Techem environment, files cannot be downloaded and stored in order to avoid uncontrolled information leakage.

5 Security Operations

5.1. Security Operations Center

Techem uses an external Security Operations Center (SOC), which is operated 24/7 as a managed security service. It is based on Security Information and Event Management (SIEM), where system log files are collected and analyzed. A team is available on call to provide support for incident response and forensics as needed.

5.2. Vulnerability Management

All systems are regularly checked for vulnerabilities as part of vulnerability management. The internal network areas are scanned regularly, and end devices transmit their data via an installed agent. The security organization analyzes and evaluates the incoming data and defines risk mitigation measures in coordination with the IT departments.

5.3. Threat Intelligence

A specialized system is used to collect information in the form of threat intelligence. This includes clear and dark web scans, the identification of attack trends, and the detection of potential phishing domains or social media profiles used to prepare social engineering attacks.

5.4. Incident Management

Security Incident Management is performed and ensured by the security organization. For this purpose, an Incident Response Plan is in place that governs the structured response to security incidents.

In the event of a critical incident, Techem's crisis team can be activated; the decision is made by the Head of Information Security.

Eschborn, 14.07.2026

Contact:

Information Security
Techem Energy Services GmbH
Hauptstr. 89
65760 Eschborn

Web: www.techem.de