Protec since 1976 HighRel Components

Europe's Leading Distributor for HighRel Components

INFORMATION & CYBER SECURITY POLICY

Protection of Information, Systems and Digital Infrastructure

Issued by	PROTEC GmbH
Applicable for	On-Premise Office Infrastructure
Version	1.0
Effective Date	01.05.2026

1. Purpose

PROTEC GmbH is committed to protecting company information, customer data, IT systems and digital infrastructure against unauthorized access, misuse, loss, disclosure, disruption and cyber threats.

2. On-Premise Infrastructure

Most applications and data are stored locally in the office on on-premise infrastructure. Critical data is not stored in cloud services. AI/KI services are operated only in isolated on-premise environments where applicable.

3. Approved Systems and Software

PROTEC GmbH uses authorized, licensed and certified systems or software where required by law, customer requirements or operational standards. Employees must not install unauthorized software or connect unauthorized devices without approval.

4. Access Control

System access is limited to authorized users with a business need. Controls include individual accounts, strong passwords, restricted administrative access and prompt adjustment of access rights when roles change.

5. Cybersecurity Measures

Reasonable security measures include firewall and network protection, endpoint protection, security updates, backups, monitoring and protection against phishing and malware.

6. Remote Access and Devices

Where remote access is permitted, secure methods must be used. Lost or stolen devices and suspected unauthorized access must be reported immediately.

7. Incident Reporting

Employees must immediately report suspected cybersecurity incidents, unauthorized access attempts, phishing, data breaches or accidental disclosures.