intech
an Infosys company

Information Security

"White Paper"

Contents

Foreword

"The Purpose of Politics"

Our corporate policy on information security and cybersecurity outlines our guidelines and regulations for safeguarding the security of our data, assets, and our technical infrastructure.

The more we rely on technology to collect, store, and manage information, the more vulnerable we become to serious security breaches.
Human error, cyberattacks, and system malfunctions could cause significant financial damage and jeopardize our company's reputation.

For this reason, we have implemented a number of security measures. In addition, we have developed guidelines that can help mitigate security risks.

"Scope of Application"

The scope of this policy covers all divisions, subsidiaries, and affiliate companies of the in-tech Group, as well as all locations and premises in all their forms.

Furthermore, our guidelines have a ripple effect that extends beyond their immediate scope: Our suppliers are required to comply with the applicable guidelines. Employees who work on-site at client locations are also subject to in-tech's policies.

1. Conformity Certification and Assurance

To ensure a structured and strategic approach to information security, we implement our information security management system in accordance with a number of well-known industry standards. We know that these certifications and labels are particularly important because they demonstrate to our customers that we maintain a high standard of information security and also provide independent assurance.

STANDARD	BASIS	STATUS
ISO/IEC 27001	**ISO/IEC** International Organization for Standardization / International Electrotechnical Commission	Certified Areas: Services for the development and validation of electrical and electronic systems in the automotive, Industry 4.0, and transportation sectors; conducting vehicle inspections and tests; conducting inspections and tests for quality assurance; development Development of conversion kits for the electrification of diesel vehicles Development and production of charging communication control units, software consulting and services, and development for car-sharing and fleet management providers ISO/IEC 27001 also draws on the comprehensive security measures described in detail in ISO/IEC 27002. The basis for this certification is the implementation of an information security management system (ISMS).
TISAX®	**ENX Association** is an association of automakers, suppliers, and four national automotive associations	Information Security Assessment (ISA) by the German Association of the Automotive Industry (VDA). Verified Labels: Assessment Level **= AL3** ✔ Information with Very High Security ✔ Very High Availability ✔ Data Protection Regarding Special Categories of Personal Data ✔ Protection of Prototype Parts, Components, and Prototypes

2. Information Security Management

2.1 Information Classification

The in-tech Group applies information classification to all information assets used within the organization. For these identified assets (primary, supported, or business application assets), the protection requirements are determined and classified accordingly based on the CIA model (**Confidentiality**, **Integrity**, and **Availability**). This is carried out through centralized asset management.

Level	Protection Needs	Classification
0	not relevant	Public
1	normal	Internal
2	high	Confidential
3	critical	Secret

2.2 Information Security Risk Management

The in-tech Group applies information security risk management in accordance with ISO 27005, which involves the systematic identification and management of risks when they are associated with the loss of or impact on the confidentiality, integrity, and/or availability of information assets.

Our approach to risk management includes:

- Risk Management for Information Security in the Enterprise - Significant changes to the organization, business processes, or information processing facilities that affect information security are managed through a risk management process.
- Risk Management in Product Development - Information security risk management is implemented as part of our product development framework.
- Risk Assessment in Project Management – When planning and executing projects, risk analysis and mitigation based on the FMEA model are standard practice.
- Risk Management for IT Services/Systems and Suppliers - Information security requirements and the risks associated with new IT systems/services and suppliers are managed through a risk management process within the change management framework.
- Risk Management and DPIA — If the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons, a Data Protection Impact Assessment (DPIA) is conducted to ensure adequate protection of personal data.

2.3 Information Security Audit

The in-tech Group conducts audits on an ongoing basis to ensure compliance with standards, guidelines, controls, best practices, laws, and regulations. Another important aspect for us is to achieve this through continuous improvement in performance and maturity.

The audits are conducted by both internal and external independent auditors.
External audits are conducted exclusively by accredited audit service providers.
The core internal audit team has completed relevant training and holds certifications in the applicable management systems:

- Internal Information Security Audit (annual)
- Management Reporting and Evaluation (Annual)
- External ISO 27001 Certification Audit (annual)
- External TISAX® Compliance Audit (in the event of changes at the site or every 3 years)

2.4 Incident Management

All information security and data protection incidents are handled by the information security and data protection organization in accordance with established policies and procedures.

The reporting system has been defined and is reviewed and explained each year during our information security training.

2.5 Supplier Management

To ensure compliance with information security and data protection laws and to maintain the quality of the service, appropriate agreements (GHV) are entered into and subsequently monitored on an ongoing basis (supplier audit).

Contractual provisions with suppliers ensure that the integrity, confidentiality, and availability of the accessible information are maintained. The storage, processing, disclosure, and deletion of data are carried out exclusively in accordance with the contractual provisions.
Supplier audits are conducted to verify compliance with these requirements. There are reporting requirements for security incidents. Access controls and behavioral guidelines are communicated to suppliers and are an integral part of the agreements.

In addition, we maintain a “**Business Partner Code of Conduct**” with our partner companies (suppliers) to ensure their adherence to our code of conduct.

2.6 Guidelines, Policies, and Requirements

Our ISMS is structured and designed to cover all aspects of the ISO standard and other regulatory requirements to which we adhere. Our ISMS and policy management are designed to ensure that all requirements are met as follows:

- is accessible to all relevant stakeholders
- has been communicated to all employees
- was approved by management
- It is well-documented and readily available
- complies with the definition of security objectives
- Demonstrate our commitment to fulfilling our regulatory obligations
- is focused on continuous improvement
- The following is reviewed annually:

2.7 Business Conduct

Our mission statement describes the values we share and how we want to work together—today and in the future. It sets a clear goal for us that we must achieve in order to ensure our long-term success.

We can only achieve this goal by working together. In this context, our values—such as personal responsibility, openness, and transparency—as well as conduct that is always in compliance with the law and ethically sound play a particularly important role.

2.8 Information Security Awareness

Each year, the in-tech Group educates, trains, and tests all employees on the applicable policies, procedures, and measures for ensuring information security.

After completing mandatory training courses and passing the exams for “**Information Security Training**,” “**Data Protection**,” “**Training on Handling Prototypes**,” “**Ransomware Awareness**,” “**Phishing Email Awareness**,” or “**Information Security & “Data Protection in the Use of AI”**—employees receive a training certificate.

2.9 GHV/NDA Employee

All of our employees are subject to a contractual agreement regarding information security and confidentiality.

2.10 Prevention of Data Leaks (Data Loss Prevention (DLP))

To protect the confidentiality of our information—particularly customer and personal data—the in-tech Group implements a comprehensive set of measures to prevent data leaks and loss.

From an organizational standpoint, all employees are bound by confidentiality agreements and IT usage policies that are incorporated into their employment contracts. Annual mandatory training sessions on information security, data protection, and compliance raise awareness of risks and promote the proper handling of sensitive data.

From a technical standpoint, measures are implemented based on the security requirements of the systems and business applications.

2.11 Dealing with Artificial Intelligence (AI)

At in-tech, the use of AI systems is subject to a centralized risk assessment. Every business application with AI functionality is recorded, evaluated, and documented as an asset—including the models, functions, and operating environments used.

All employees complete mandatory annual training on the safe and legally compliant use of AI. The use of AI systems is subject to a binding terms of use agreement
(Code of Conduct).

A company-wide AI hub supports the responsible and quality-assured use of AI through regular training sessions and open forums for discussion.

2.12 Security Screening of Applicants

As part of the recruiting and onboarding process, various security screenings are conducted depending on the location and local requirements. The goal is to identify potential threats early on and ensure the protection of confidential information.

These measures include, among other things, identity verification, a photograph, diplomas, a driver's license, health and occupational safety tests, etc.

3. Safety in Use

3.1 Access Control

Access controls are role-based and restricted according to the need-to-know principle. Each of our users is assigned a unique user ID to ensure integrity. The unique user ID applies to all employees, including system administrators and system accounts.

in-tech GmbH has processes in place to modify or revoke access rights immediately after a change in an employee's employment status or position. In addition, access control authorization reviews are conducted.

3.2 Multi-Factor Authentication

"Strong authentication" (or multi-factor authentication) is required to access internal services.

3.3 Password Policy

All employees or system users of the in-tech Group have individual user accounts and must authenticate themselves using at least a username and password. In addition, we have a password policy whose requirements are implemented technically on a one-to-one basis to ensure complex and secure passwords.

The password policy can be customized to meet specific customer requirements.

Passwords are reset only in accordance with the dual-control principle, requiring authentication by an additional manager.

3.4 Clean Desk and Clear Screen

With our company-wide Clear Desk/Clear Screen Policy, we reduce the risk of unauthorized access, loss of information, and damage to information both during and outside of working hours.

Procedures for handling paper documents and storage media, as well as secure data destruction (certified document shredding and data erasure procedures in accordance with BSI recommendations), are defined and regulated.

The use of paper printouts is regulated and is only possible with Print2me.

The automatic locking of screens and automatic logout from systems have been technically implemented.

3.5 Handling Information Values

The customer's data is logically separated for each client to ensure confidentiality and integrity across clients.

This data is classified in accordance with our information classification system. This ensures that all relevant values are recorded and classified, and that rules for handling them are established and followed. To determine the specific protection requirements based on the criteria of confidentiality, integrity, and availability, an assessment framework is included in our asset template.

Access to sensitive information is granted only on a need-to-know basis.
Access to confidential information is part of the quarterly review of role-based permissions.

3.6 Event logs

To the extent technically feasible, all relevant activities within business applications are logged. These logs may contain information about the user, the time and date, user activities, and critical security events (such as authentication attempts that violate authentication policies).

To protect the integrity of these logs from tampering, access rights to the
source logs are strictly limited. In addition, relevant logs are also stored on a Syslog server
.

The system and application time are synchronized using the Network Time Protocol (NTP).

3.7 Encryption

Communication between end users and the in-tech servers is encrypted using industry-standard best practices. In addition, all mobile devices (OS) are encrypted.

In addition, further technical measures have been implemented in accordance with the information classification level. This includes, for example, content encryption, S/MIME, SSL, and much more.

4. IT Operations Security

4.1 Access Control

Privileged access to IT infrastructure assets such as servers, switches, firewalls, etc., is further protected by restricted network segments and multi-factor authentication.

4.2 Mobile devices

Mobile devices, such as laptops, smartphones, and tablets, sometimes play an important role in achieving our business goals. However, they also pose significant security risks: For example, loss or theft could allow unauthorized individuals to gain access to in-tech GmbH's IT infrastructure via these mobile devices.

For this reason, this policy deserves special attention in order to protect our information assets, secure customer data and access, and safeguard our reputation.

That's why our devices...

- centrally managed
- whose storage media are encrypted
- Assigned to a specific individual (no additional employees can be registered)
- protected by strong authentication
- the handling and disposal of the material are regulated and described

4.3 IT Infrastructure - Event Logs

Event logs from these IT infrastructure assets are also backed up on a syslog management platform that is centrally managed by the in-tech Group's IT team. The platform is used to collect, index, and analyze syslog data at a central location.

The system and application time are synchronized using the Network Time Protocol (NTP).

4.4 Backup

The in-tech Group has a backup strategy in place that backs up and monitors both internal data and the client's respective project data in accordance with the required level of protection.

The design takes into account all server systems, firewalls, and switch configurations. Daily backups are available for restoration for at least two weeks. In addition, both monthly and annual backups are available.
The current backup data is stored in a second fire compartment.
Backup recovery tests are scheduled.
Recovery Time Objectives and Recovery Point Objectives are defined and documented.

An offline backup is used as an additional measure to protect against ransomware.

4.5 Vulnerability Management

The in-tech Group has a documented vulnerability management policy. This document specifies potential sources of information and reporting channels. In addition, a software and patch management system is in place,
which defines the process for identifying vulnerabilities and patches and ensures they are classified, applied, and resolved in accordance with internal policies and procedures.
The systems are monitored using automated tools and report to designated monitoring points.

4.6 Development Environment

The in-tech Group has separate environments for application development (Test / Integration / Production).

4.7 Monitoring and Incident Detection

All production-critical systems send their syslogs to a central platform (syslog server).
This platform is permanently available for analyzing the logs, particularly in cases of suspected incidents or to investigate the causes of security incidents.

In the event of an emergency, there are defined processes and immediate measures in place for handling information security and emergency incidents.

4.8 Business Impact Analysis and Emergency Management

A Business Impact Analysis (BIA) is conducted annually for all locations and subsidiaries.
This process involves identifying and evaluating the most important core processes at each location. The necessary IT systems, Recovery Point Objectives (RPO), and Recovery Time Objectives (RTO) are identified and coordinated with management.

The central BCM manual contains all relevant guidelines, responsibilities, and crisis response checklists. Emergency and recovery plans are documented and tested regularly. Emergency simulations, including tabletop exercises simulating cyberattacks, are being conducted or are planned.

4.9 Problem Management and Ticket System

The in-tech Group uses several ticket systems to manage incidents and issues. These are specifically used for relevant areas. The processes are documented and ensure structured tracking and processing.

4.10 Performance and Capacity Management

Processes for collecting and analyzing performance and capacity metrics (KPIs) have been established for all relevant systems. The results are reported annually to senior management as part of the management review.

5. Communications and Network Security

5.1 Access Control and Authentication

Login and authentication to corporate networks that provide access to internal resources and information are permitted only via a VPN connection with multi-factor authentication.
Web-based services that provide access to internal or confidential data are also accessible only via multi-factor authentication. In addition, login is only possible from an approved geographic location.
Access to networks and network services is granted only to authorized employees or users.

5.2 Redundancy

The in-tech Group has redundant network connections and the ability to route or redirect communication accordingly in the unlikely event of a network outage.

5.3 Network Encryption

All site-to-site communication within the in-tech Group is encrypted via VPN tunnels.
All VPN traffic from external sources into the in-tech infrastructure is encrypted.
Internal traffic from in-tech clients to production services is encrypted.

5.4 Protection Against Malware

To protect our information (values, customer data, and personal data) and our information-processing systems from malware, we implement various security measures at the in-tech Group.

In our approach, we focus on prevention as well as on the technical detection of malware during operations. Finally, we have also defined procedures for protecting and restoring our information and information-processing systems in the event of an emergency (BCM).

5.5 Network Isolation / Segmentation

To ensure a sufficiently high level of security on our internal network, we have implemented a company-wide network segmentation policy. These include server systems, VOIP, client networks, management, and many others, which are either separate from one another or divided into respective areas.
These are only partially interconnected and are still separated by respective firewalls.

5.6 Firewalls

Each node in our company-wide network is protected by firewalls.
Central systems are protected against outages by hot-standby clusters.

The firewalls we use all offer the latest next-generation firewall security features.

5.7 Network Access Control (NAC)

To ensure that only authorized devices have access to the corporate network, the in-tech Group uses the IEEE 802.1x protocol for both its wired network and its Wi-Fi network.

6. Physical Security

6.1 Security in the Data Center

The central IT systems are located in the primary data center. It features a range of different physical security controls and security standards, such as:

- Strict physical multi-factor access control
- Access Logs
- Dedicated and Locked Server Cabinets
- Security Alarms
- Fire Detection and Prevention Measures
- Climate Control Systems and Alarms
- Uninterruptible Power Supply
- Lightning Protection
- Redundant Networks
- Video Surveillance

6.2 Server Room Security

In addition to our primary data center, we have appropriately secured server rooms at various locations for IT systems that process sensitive information. These are secured by multiple access control points and a burglar alarm system.
They are also equipped with an uninterruptible power supply (UPS) and air conditioning.

This allows us to establish a high level of geographic redundancy, which contributes significantly to our reliability.

6.3 Security in the project office or common areas

The in-tech Group’s various project and office spaces are protected by access controls as well as by an EMA / security and fire alarm system. Access permissions have been established.

Security at the in-tech Group's physical locations is managed in accordance with ISO 27001, TISAX® VDA guidelines for physical security, and the workplace security policy.

Documented site risk assessments and safety plans are available.

7. Privacy Policy

The goal of in-tech’s data protection management system is to protect the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data.

To ensure that the processing of personal data complies with applicable laws and the company’s self-imposed obligations, the in-tech Group maintains a company-wide data protection management system and has designated a Data Protection Officer within the company for this purpose.

This data protection management system also includes a policy on the handling and retention of personal data within the in-tech environment. The purpose of this policy is to ensure the compliance of internal processes, IT systems, and applications through design and standards, as well as through the principles of data minimization and storage limitation.

The foundation for this is our asset management of information-processing (including pbDaten) IT systems, in which the security requirements regarding confidentiality, integrity, and availability are defined.

The measures necessary to ensure an appropriate level of protection for personal data are defined, implemented, and monitored in conjunction with information security.