Information Security Policy

Digital Automotive

Version: 1.1.0

Date: 08.01.2025

Confidentiality: low

Availability: high

Integrity: high

Author: Jürgen Sterr / CTO

Contributors:

- Tobias Kellner / ISB

Interested Parties:

- Employees
- Customers

Version history

Version	Date	Updated by	Approved by	Changes
1.0.0	17.7.2023	Jürgen Sterr	Erik Reiter	Document was created initially.
1.1.0	08.01.2025	Tobias Kellner	Jürgen Sterr	Styling and minor mistakes.

1 Content

2 Information security policy

2.1 Goals

This Information Security Policy of IT Manufactory GmbH establishes confidentiality, integrity, and availability, as well as ensuring compliance within the company.

2.2 Area of Effect

This Information Security Policy applies to IT Manufactory GmbH and its employees. The policy extends to all areas of the company.

2.3 Project management

Information security is taken into account in project management, regardless of the type of project. For projects classified as security-critical, a security check in the sense of the ISMS is required. This check is performed and evaluated by the project manager, the DevSecOps and, if necessary, the information security officer.

Amon other things, the focus is on:

- Availability of systems,
- integrity, confidentiality, and availability,
- Time frame,
- Financial resources,
- Personnel expenditure,
- Project organization,
- Information security risk requirements,
- Steering committee,
- Internal / external customers,
- Project management / project team,
- Involved experts,
- Contracting,
- Interested parties,
- Goals / milestones,
- Process and schedule planning,
- Risk management in the project,
- reporting,
- monitoring,
- presentation of results,
- decisions,
- Takeover / handover and,
- action plans.

Furthermore, changes in the project are made traceable through documented change management & re-release management.

2.4 Mobile devices and teleworking

A policy and supporting security measures have been implemented to manage the risks associated with the use of mobile devices. A corresponding policy is implemented and enforced.

2.5 Guideline on teleworking

A policy and supporting security measures to protect information accessed, processed or stored from telework places have been implemented. Teleworking (home office / mobile working) is generally permitted. Security measures are implemented both technically and organizationally. Approval is process controlled. A corresponding guideline has been established.

2.6 Shared roles and responsibilities within a cloud computing environment

Our information security controls are based on the ISO/IEC 27002 for cloud services. IT Manufactory GmbH provides Cloud Service customers with practical guidance and information regarding their expectations of our Cloud Service. Information security features, roles and responsibilities for the use of its cloud service are the responsibility of the customer, as only it manages the data itself. IT Manufactory GmbH and customers are aware of the shared responsibility in the cloud.

2.7 Reprimand process

A formally defined and announced disciplinary process is in place to take action against employees who have committed an information security breach. The disciplinary process is implemented and documented.

2.8 Termination or change of employment

Responsibilities and duties in the area of information security, which continue to exist even after termination or change of employment, are defined, communicated to the employee or contractor and enforced. Through off boarding and change of employment, the tasks to be performed with regard to information security are processed and their fulfilment is checked when employees leave (off boarding) or change of employment (change of employment).

2.9 Value management

Values are the foundation of any corporate culture. Values in our company are:

- Inventory,
- Business processes,
- Intangible assets such as
  - reputation of the company and
  - its image,
  - credibility,
  - reliability
- Product information such as
  - source code,
- IT systems with:
  - software,
  - licenses,
  - hardware,
  - network plan,
- Buildings & Rooms as well as:
  - Facilities,
  - Vehicles,
- Employees with

    - software architecture,
    - documentation o protocols,
    - checklists,
    - training manuals,
    - process descriptions,
    - instructions,
    - productivity,
    - customer data,
    - quality objectives,
    - progress,
    - safety,
    - contracts,
    - results,
- Data carriers,
- Documents,
    - respect,
    - diversity,
    - integrity,
    - sincerity,
    - openness,
    - community,
    - teamwork,
    - communication,
    - collegiality,
    - creativity,
    - qualifications and experience,
    - responsibility,
    - appreciation
- Computing and communication services,
- Equipment / utilities and
- Assets.

These values must be protected by all parties involved. If they can be compromised or lost, the ISMS officer(s) or management must be informed immediately. These values may be used to the extent specified.

2.10 Return of valuables

2.10.1 Regulated procedure for the departure of employees

All employees and other users, external parties shall, upon termination of the employment, contract or agreement employment, contract, or agreement, shall return all assets in their possession that their possession that belong to the organization. In off boarding, upon leaving, a task, in the form of a checklist for the return of assets is processed and reviewed.

2.10.2 Regulated procedure when a customer terminates a contract

IT Manufactory has implemented a contract termination policy to ensure that customers are treated fairly and transparently, and that the company complies with all relevant legal requirements and standards. To terminate a contract with a customer, we first review the contract to ensure that all conditions have been met. If all conditions have been met, we send the customer a written notification of the termination of the contract. In this notice, we state the reason for the termination and the date on which the termination is effective.

We require Customer to return all property and documents provided by us to ensure that all of our intellectual property rights remain protected. Verify that we have received back all property provided by us. We ensure that all payments or refunds due have been cleared and we set a deadline for repayment or collection of items still with us.

We document the termination of the contract and ensure that we have all relevant documents and information in case we are later asked to provide evidence of the contract termination. We ensure that the customer is satisfied and address their concerns when we terminate the contract. If possible, we discuss possible alternatives or solutions to enable future collaboration.

By following this procedure for contract terminations, we can ensure that we are professional and respectful to our customers and maintain our business relationships. We pride ourselves on

providing a high standard of quality to our customers and maintaining this standard during contract terminations, giving our customers the assurance that they will be treated fairly and transparently at all times and that a contract termination will proceed smoothly and without unforeseen difficulties.

2.10.3 Regulated procedure for return and secure removal of information assets

IT Manufactory has implemented a regulated procedure for the return and secure removal of information assets to ensure that customers are treated fairly and transparently, and that the complies with all relevant legal requirements and standards. The organization uses only established IT services that have policies for the return, transfer, and/or deletion of information assets as well as deletion of information assets and are accessible at all times. A contractual arrangement between the organization and the cloud services exists and is reviewed regularly. We also support our customers with requests for data return or deletion of information assets.

2.10.4 Orderly termination of a cloud usage relationship

IT Manufactory has implemented an orderly termination of cloud usage relationships to ensure that customers are treated fairly and transparently, and that the company complies with all relevant legal requirements and standards.

First, we review the contractual notice period to ensure that all conditions have been met. We want to ensure that both parties are comfortable with the termination of the relationship and that no unexpected issues arise. The organization submits the notice of termination to the cloud service and determines the desired termination date. The cloud service acknowledges receipt of the notice, and the organization schedules the return of the information assets. The organization begins repatriating the information assets to a secure environment, such as an on-premises backup or another cloud platform. The organization verifies the completeness of the data, tests all expected functionality in the new environment, and then gives the cloud service the go-ahead to delete the data from the old environment. The cloud service disables access to the services and deletes all data that is not part of the organization's information assets. The cloud service provides the organization with a final invoice for the services used. The termination process is completed, and the cloud service and the organization sever their business relationship. By following this procedure, we can ensure that the termination of the cloud usage relationship is handled in a professional and respectful manner and that all relevant steps have been executed to ensure a smooth transition. IT Manufactory's orderly termination of cloud usage relationships provides our customers with peace of mind that their data and information is safe and secure at all times, and that the termination of the relationship will proceed smoothly and without unforeseen difficulties.

2.11 Handling of data carriers

2.11.1 Handling of removable media

Procedures for handling removable media are implemented according to the information classification scheme used by the organization.

The handling of removable media is defined internally:
Data remains in its context whenever possible and is not copied to removable media.

If data does have to be transferred/saved to mobile data media, the following applies:
Data that is stored on mobile data media (especially that contains internal, confidential, or highly

confidential information) must be encrypted and secured using appropriate techniques (e.g., BitLocker).

2.11.2 Disposal of data carriers

Data carriers that are no longer required are disposed of securely by our specialists (SecOps Team) using formal procedures and techniques.

2.11.3 Transport of data carriers

Data carriers containing information are protected against unauthorized access, misuse, or falsification during transport.

The handling of data carriers and their transport is defined internally:
Data that is stored on mobile data carriers and may contain internal, confidential, or strictly confidential information must be encrypted and secured using appropriate techniques (e.g., BitLocker) to minimize unauthorized access, misuse, or falsification of the data.

2.12 Access Control Policy

An access control policy is established, documented, and reviewed based on business and security requirements. Access control is defined via role-based groups and corresponding group memberships. The required rights are assigned via the respective roles.

It apply the principals:

- Need-to-Know-Principle
- As much access as necessary, as little as possible.

Both the policy, compliance with access control, and the roles and their rights are regularly reviewed at least once a year.

2.13 User access management

2.13.1 Registration / Deregistration

A formal process for registering and deregistering users has been implemented to enable the assignment of access rights.

We create and manage two types of user accounts for different environments:

- User accounts for internal use of applications.
- User accounts for Digital Automotive Platform customers.

For both types of user accounts, processes are defined and implemented to ensure the correct registration and deregistration of users. For example, employee accounts are created during the On-Boarding-procedure when they join the company and deactivated and deleted when they leave Off Boarding. The administration is done e.g., via Microsoft Entra ID, Azure, etc.

IT Manufactory GmbH carries out checks for unused access data at regular intervals. After a compromise becomes known, the reset of affected accounts is regulated via an organizational process.

For cloud operation, the following also applies:

The configuration guide in Atlassian Confluence is also dedicated to the Digital Automotive Platform (Keycloak) on the topic of setting up users.

2.13.2 Privileged access rights management

The management is responsible for these roles. The allocation and use of privileged access rights is restricted and controlled by management. Users with special administrative or privileged rights are grouped in suitable role groups and are subject to the corresponding approvals by management. For particularly privileged rights (e.g., firewall access, admin portals, etc.), the user must use a special personalized administrator account; his "normal" user account does not get these rights / cannot be assigned to the appropriate roles.

2.13.3 Management of secret authentication information of users

The assignment of secret authentication information is controlled in IT Manufactory GmbH via a formal process. This information is only stored in encrypted form in IT Manufactory GmbH. All employees use an appropriate password tool. IT Manufactory GmbH uses the password tool Bitwarden. The obligation to use the password tools in all cases is defined by corresponding guidelines.

2.13.4 Withdrawal or adjustment of access rights

The access rights of all employees and users belonging to external parties to information and information-processing facilities shall be withdrawn upon termination of the employment relationship, contract or agreement, or adjusted in the event of a change. Access rights and roles are revoked upon resignation. This is initiated via the personnel administration. Upon termination of a partnership, the partner manager regulates the closure of accesses.

2.13.5 Information access restriction

Access to information and application system functions is restricted accordingly via permissions and access control policy. Access control is defined and restricted via role-based groups and corresponding group memberships. The required rights are assigned on a need basis via the respective roles.

It applies the principals:

- Need-to-Know-Principle
- As much access as necessary, as little as possible.

Both the policy, compliance with access control, and the roles and their rights are regularly reviewed at least once a year.

For cloud operation, the following also applies:

We make sure that when we (re)allocate storage space, it does not contain legacy data.

2.14 Cryptography

All necessary data is encrypted using cryptographic services. All users are instructed in the cryptographic services. Data that is not cryptographically encrypted is communicated to the ISMS officer. A root service is installed on the client computers to ensure encryption. The ISMS officer checks the regulations on a quarterly basis.

More detailed information on the cryptographic systems used can be found in the corresponding policy.

2.14.1 Key management

A policy on the use, protection, and lifetime of cryptographic keys is developed and implemented throughout their lifecycle. Guidelines for the use, protection, and lifetime of cryptographic keys exist and are implemented throughout their lifecycle.

SSH key validity areas:

The scope defines the users, systems, and applications to which the SSH key applies:

- Users: IT Manufacture development team, DevSecOps team.
- Systems: Access to all servers (internal and external) is managed via SSH keys. DevSecOps is responsible for managing access to these systems for each user. Users are only granted access to the systems when needed.
- Applications: Developers are required to access IT Manufactory Gitlab via their SSH keys.

Inventory of assets:

The collection of all SSH keys and their access usage is stored in a Git repository. With that we make sure that revoked keys and the date of removal is also documented.

SSH Key Generation Policy:

The developer's setup defines the proper way to generate an SSH key pair that is compatible with all internal configurations while adhering to standard security practices. All SSH key pairs are created using the ECDH ED25519 curve algorithm.

Access Granting and Withdrawal:

Timely or scheduled access to keys is managed by the DevSecOps teams. A user can create a standard Jira ticket to grant access to specific systems. The user's request is then evaluated, their active key is retrieved, and access is granted to the user. The duration of access depends on the task at hand and the user's requirements.

2.15 Physical and environmental safety

2.15.1 Physical safety perimeter

Security perimeters are defined and used to protect areas where either sensitive or critical information or information-processing equipment is located.

- The Passau headquarters is secured by electronic access control system.
- Only authorized persons have access.

- Areas are separated by locked areas.
- Further documentation can be found in the corresponding policy.

2.15.2 Physical access control

Secure areas are protected by appropriate traceable access control to ensure that only authorized personnel are granted access.

- There are two areas: non-public area and special areas. All access points are secured and equipped with locks with AirKey.
- The issuance, handover and return of keys is documented.
- The issuance, transfer, return, and destruction of AirKey is documented and validity periods are established as needed.
- Employees are made aware of how to deal with guests as part of their security briefing.
- In the event of loss, the ISMS representative must be informed immediately.

2.15.3 Safe disposal or reuse of equipment and operating materials

All types of equipment and supplies containing storage media are reviewed to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or reuse. Paper, storage media, and other devices containing information are securely destroyed.

Disposal of data media is designed to assume that it contains personnel-related data. The DevSecOps department experts collect them, destroy them securely on site. The destruction process is described in DIN 66399:

- Security level: confidential (DIN 66399-1)
- Security level: hard disks and similar: H-4 (DIN 66399-2), paper: P-4 (DIN 66399-2)

This also applies to cloud operations.

2.16 Unattended user equipment

Users ensure that unattended devices and resources are adequately protected. The policy for re-authentication prompts after inactivity varies by device:

- For local PC, or laptops, notebooks after 5 min.
- For mobile devices (smartphones, tablets, etc.) PIN (or password, min. 4 characters) and spear time of 3 min.
- Removable data carriers and mobile devices must be kept locked.

See also the occupational safety guideline as a further document.

2.17 Tidy work environment policy and screen locks

IT Manufactory GmbH lives the clean desk policy. Guidelines for a tidy working environment with regard to documents and removable data carriers and for screen locks for information processing equipment are applied.

No documents or data carriers containing sensitive data may be left unattended and unlocked at the workplace. Outside working hours, all documents containing sensitive data and mobile devices belonging to employees must be kept locked away. Access data (such as username/password) must

not be left in writing at the workplace (e.g., attached to the screen, under the keyboard or desk pad - with the exception of central administration accounts that are managed in appropriate tools). Confidential documents and documents containing personal data do NOT belong in the wastebasket but must either be shredded or placed in paper disposal garbage cans. Screen, mail and filing bins must be placed in such a way that no visitor can look at them in passing or pocket documents without attracting attention. In the case of short absences, it must be ensured by logging off from all systems or by locking the screen (with renewed password entry) that no one gains unauthorized access to confidential data.

When leaving a meeting room all working documents, presentations, flipcharts, removable media, etc. must be taken away. Also, for hygienic reasons, all coffee cups and mugs, glasses, empty bottles, dishes and garbage must be disposed of properly and the table must be left Table is to be left clean. Printouts at the community printer are to be picked up immediately. Remain at the printer or copier during the printing and copying process. printer or copier. As a matter of principle, work is done paperless and only in special cases should printouts and copies be made.

See also the Work Safety Guideline as a further document.

2.18 Change management

Changes to the organization, business processes, information processing equipment and systems are controlled and communicated in a timely manner. All changes are subject to the change management process, and this controls the respective change. If necessary, briefings are carried out or information is produced.

2.19 Capacity control

Resource utilization/usage is monitored and reconciled, and forecasts of future capacity requirements are made to ensure the required system performance. All resources (IT infrastructure, such as network, computing power, storage) are regularly audited. Forecasts of system utilization and utilization trends are presented and analysed via appropriate tools and graphics. Planning of new systems, system expansions and line upgrades are carried out within the framework of projects and in a controlled change management, which in turn results in corresponding measures for capacity expansion. As a matter of principle, planning is carried out with a forward-looking buffer that is appropriate to the dynamics of the last few years and adapted to the forecasts of further developments.

2.20 Separation of environments

Operating environments are kept strictly separate from each other to reduce the risk of unauthorized access to or changes to the operating environment. Separate operating environments are used for this purpose and role-based access data is provided. Separation for the following operating environments:

- Development,
- Testing,
- Review,
- Staging,
- Demo,
- Trail,

- Production.

This is ensured by appropriate processes. Customers' productive systems are implemented according to Service Level Agreements (SLA).

This concerns in particular:

- Measures against cyber-attacks,
- Early detection of emergencies,
- prevention and recovery measures, and
- the sensitization of the processing personnel.

See further documentation of the data protection policy and SLAs maintenance contracts.

Where IT Manufactory GmbH is not responsible for development (3rd party systems), development systems may not exist. Nevertheless, staging/trial/production systems are strictly separated here as well.

For cloud operation, the following also applies: IT Manufactory GmbH also takes into account the data protection measures including risk assessment for situations in which test data should be used.

2.21 Logging and monitoring

2.21.1 Event logging

Logs are kept of all incidents and events are monitored. This covers:

- Event logs,
- activities of users and administrators,
- exceptions,
- incidents,
- information security incidents.

Monitoring, alerting and logging are performed in a controlled manner. They are anchored in the application management. The associated guidelines are defined by IT Manufactory GmbH in the internal Atlassian Jira Confluence Operation.

The following also applies to cloud operation:

Upon request, we offer our customers the option of handing over relevant log data. The regularity and depth of the audit is the responsibility of the customer.

2.22 Information transmission

2.22.1 Information transmission policies and procedures

Formal transmission policies, procedures and measures are in place to protect the transmission of information for all types of communication equipment. IT Manufactory GmbH has issued rules on how to handle the transmission of data (data on the move).

Appropriate procedures and measures have been implemented and are being applied. This also applies to cloud operation.

2.22.2 Information transfer agreements

Agreements cover the secure transfer of business information between the organization and external parties. The handling of the transfer of data (data on the move) is agreed with external partners.

These agreements can be found in the corresponding contracts:

- among other things, in Non Disclosure Agreements (NDA),
- license agreements for system access (DA),
- the corresponding service descriptions (which are part of the contract) or individual service level agreements (SLA) with customers.

2.22.3 Electronic messaging

Information in electronic messaging is adequately protected. All data that is transmitted (Data on the Move) is encrypted at the latest when it makes a zone change. The encryption is at least TLS 1.2 (with AES 256 bit).

2.22.4 Confidentiality or non-disclosure agreements

Requirements for confidentiality or non-disclosure agreements that reflect the organization's need to protect information are identified, regularly reviewed and documented. Confidentiality agreements are in place for both internal and external use. Responsible parties (from legal, data protection and human resources) are responsible for the content and maintain it regularly. Sources for changes may include audits, legislation, requirements in the exchange with business partners (suppliers, customers) and changes in the inventory of assets requiring protection.

Content of non-disclosure agreements (NDA), even if they are created by the other party:

- persons/organizations involved,
- the nature of the information covered by the agreement,
- the subject matter of the agreement,
- the period of validity of the agreement,
- the responsibilities of the obligor(s).
- Non-disclosure agreements contain provisions for handling the information requiring protection beyond the contractual relationship. A process by which the validity period of temporary non-disclosure
- The process for monitoring the validity of temporary non-disclosure agreements and for initiating an extension of non-disclosure agreements in good time has been defined and implemented.

For cloud operation, the following additionally applies:

- Customers and partners sign standard contracts at the beginning of the contract with a corresponding obligation to maintain secrecy, also in data processing.
- Employees of IT Manufactory GmbH are obligated to maintain secrecy as part of their employment contract and are regularly trained in this regard.
- These contracts contain earmarking in accordance with the obligation to follow instructions within the scope of the present order processing.
- The obligation to maintain secrecy extends beyond the duration of the agreement.

2.23 Safety in development and support processes beyond

2.23.1 Guideline for safe development

Rules for the development of software and systems are defined and applied to developments within the organization. As part of the SCRUM process, the consideration of security interests in the development and maintenance of software and systems is regulated and defined in the form of processes and HowTos. Topic owners are designated for specific processes in software development. See the Agile Manifesto and the corresponding policy for further information.

2.23.2 Procedure for managing system changes

The implementation of changes must be subject to a formal change control procedure. The implementation of changes is carried out as part of a change management process by subject matter experts who coordinate release planning and communication with the customer and evaluate software changes with noticeable effects for customers.

2.23.3 Restriction of changes to software packages

Changes to software packages are not encouraged, are limited to what is required, and all changes are subject to strict governance. As part of the SCRUM process, it is regulated in the form of HowTos, how software changes are to be evaluated before release. The changes are controlled by the product managers responsible for the topic. In the case of customized systems, changes are made at the request of the customer.

2.23.4 Principles for the analysis, development and maintenance of systems

Principles for the analysis, development and maintenance of secure systems are defined, documented, kept up to date and applied to every implementation project of an information system. Rules that ensure principles for the analysis, development and maintenance of secure systems are integrated in the corresponding processes, in the associated instructions (HowTos), as well as across the board through the specifications of the Security Guide and the provision of the framework.

2.23.5 Secure development environment

Organizations create secure development environments for system development and system integration projects throughout the entire development cycle and protect them appropriately. The provision, operation, and maintenance of a secure development environment is ensured by appropriate subject managers. The security and up-to-dateness of the development environment and the entire application landscape are regularly checked as part of application management.

2.23.6 Outsourced development

The organization oversees and monitors the activities of outsourced system development. Within the framework of quality management, it is regulated and defined in the form of processes and HowTos how activities relating to outsourced system development are integrated and monitored or driven. The main responsibility for this lies with the respective partner manager of the respective development partner.

2.23.7 Testing the system security

Security functionality is tested during development. As part of quality assurance, new developments are tested manually against the defined requirements and for data protection and security requirements before release. For this purpose, there are test managers who take over the test management. In addition, automatic tests continuously safeguard against unintended side effects of the development.

2.23.8 System acceptance test

Acceptance test programs and associated criteria are defined for new information systems, updates and new versions. Within the framework of quality, change and release management, processes and HowTos are defined which specify that, prior to the release of new information systems, updates or new versions, corresponding acceptance tests are to be carried out, planned and controlled by the persons responsible for the subject. Regular maintenance work (software maintenance) is planned well in advance and documented together with irregular maintenance.

2.24 Information security incident handling and improvements

2.24.1 Responsibilities and procedures

Handling responsibilities and procedures are established to ensure a rapid, effective and orderly response to information security incidents. The security incident notification process is organized and communicated regularly. For this purpose, the notification allows several options for triggering and is processed with tool support. Possible recipients (e.g., for IT security incidents, data breaches, emergencies) are anchored and trained by roles.

The following also applies to cloud operation:

IT Manufactory GmbH has set up an internal process for reporting and handling security incidents. Among other things, the criticality is analysed according to the security criteria and taken into account in the further procedure. If necessary, the process provides for cooperation with the affected customers as agreed.

2.24.2 Reporting information security events

Information security events are reported to the Information Security Officer and Data Protection Officer as soon as possible. IT Manufactory GmbH has implemented security incident processes to ensure that information security events are reported and handled as quickly as possible through appropriate, known channels for handling them. This includes processes for both regular operations (the security incident and incident management) and exceptional situations (processes in emergency management as well as availability management or data breaches in the data protection area). Customers can contact IT Manufactory GmbH Service Management with all security concerns and reports through the channels available to them. From here, initial reactions as well as escalations are controlled. IT Manufactory GmbH immediately contacts the affected customers in the event of its own security incidents.

2.24.3 Assessment of and decision on information security events

Information security events are assessed, and a decision is made as to whether they should be classified as information security incidents.

Elementary security incidents, events and threats:

- Communication network failure or malfunction
- Failure or malfunction of service providers
- Misplanning or lack of adaptation
- Disclosure of sensitive information
- Information or products from unreliable source
- Manipulation of hardware or software
- Manipulation of information
- Unauthorized intrusion into IT systems
- Failure of equipment or systems
- Malfunction of equipment or systems
- Lack of resources
- Software vulnerabilities or errors
- Violation of laws or regulations
- Unauthorized use or administration of devices and systems
- Incorrect use or administration of devices and systems
- Misuse of authorizations
- Personnel failure
- Denial of actions
- Misuse of personal data
- Malicious programs
- Prevention of services (Denial of Service)
- Sabotage
- Loss of integrity of information worthy of protection

2.24.4 Response to information security incidents

Information security incidents are responded to in accordance with documented procedures. IT Manufactory GmbH has implemented security incident processes to ensure that information security events are reported and handled as quickly as possible through appropriate, known channels for handling them. This includes processes for regular operations (the security incident and incident management) as well as for exceptional situations (processes in emergency management as well as in availability management or for data breaches in the data protection area).

2.24.5 Insights from information security incidents

Insights gained from the analysis and resolution of information security incidents are used to reduce the probability of occurrence or impact of future incidents. IT Manufactory GmbH has established a process for security incidents as well as an incident process. This also includes taking care of the findings from security incidents and dealing with them in the long term. The same applies to emergency management as well as availability management or the processing of data breakdowns. Regular meetings ensure that findings are evaluated and dealt with. These are also input for the ISMS

(for example, with regard to correcting probabilities of occurrence, risk assessment and risk treatment).

2.25 Collection of evidence

The organization determines and applies the identification, collection, recording and retention of information that may serve as evidence. Evidence is condensed and processed by the ISMS officer(s). Management decides whether to initiate a criminal investigation.

Evidence:

- System logs,
- Log files,
- notes,
- photos of screen contents
- Data media,
- Digital information,
- People
- Activities
- Facts

2.26 Compliance

2.26.1 Compliance with legal and contractual requirements

The risk of non-compliance with legal, regulatory, self-imposed or contractual obligations with regard to information security is considered.

2.26.2 Privacy and protection of personal information

Privacy and protection of personal information are ensured, where applicable, in accordance with the requirements of the relevant laws and regulations. An data protection officer has been appointed to ensure compliance with the relevant data protection laws. Training and continuing education measures on these topics and on ensuring awareness have been set up for employees. For external employees, contact can be established via our Trust Center.

2.26.3 Information security reviews

Information security is regularly audited across the company. All departments additionally audit information security in their own areas. The results are incorporated into the information security assessment.

2.26.4 Independent review of information security

The organization's approach to managing information security and its implementation is independently reviewed at scheduled intervals or whenever significant changes occur.

We undergo regular external certification audits according to:

- Independent audit by the certifiers QM ISO 9001,
- Independent audit by the certifiers ISMS ISO 27001,

- Independent audit by the certifiers TISAX.

Verified are:

- Measure Objectives,
- Measures,
- Policies,
- Processes
- Procedures

The results are condensed in an audit report. We currently consider an annual audit to be sufficient. In addition, specially scheduled audits are carried out by the ISMS officer(s) with the departments in the event of events and incidents relating to information security.

Further audits are carried out by third parties, for example to check data security:

- Review by customers in the context of software integration and implementation,
- Review by customers in the context of security self-assessments questions

In some cases, the audits of the technical and organizational measures (TOMs) in accordance with Article 28 of the GDPR by our business partners can also be evaluated in the course of audits for order processing.

For cloud operation, the following additionally applies:

- IT Manufactory GmbH offers its customers a wide range of information to assure themselves of proper operation.
- IT Manufactory GmbH allows itself to be audited by independent, accredited bodies and provides suitable evidence such as certificates.

2.26.5 Compliance with security policies and standards

Senior executives regularly review compliance with applicable security policies, standards and any other security requirements for information processing and procedures within their areas of responsibility.

We have a multi-stage concept for this:

- Permanent responsibility and audit through the role of security officer.
- Regular meetings information security and technical debt.
- Regular internal audits; with cross-checking of relevant security policies and sample testing.
- Regular reminder and refresher training.
- Project driven ensuring necessary activities are running.
- Strategic meetings such as roadmap.

2.26.6 Review of technical compliance

Information systems are regularly reviewed for compliance with the organization's information security policies and standards.

For this we have several situations:

- Regular testing as part of change management by IT Operations.

- Permanent responsibility and testing by those responsible for the guidelines and the role of the security officer.
- Regular review from a data protection perspective by the data protection officer.
- Regular internal and external audits for ISO 9001, ISO 27001, TISAX.
- Regular appointments in the information security and technical debt meeting.
- Regular control and maintenance of controls.

IT Manufactory GmbH
Brunngasse 4, 94032 Passau / Germany
Phone: +49 (0) 800 14 14 14 7
Email: info@digital-automotive-supplier.com
Web: https://digital-automotive-supplier.com