Cloud Security Policy

Digital Automotive

Version: 1.1.0

Date: 07.01.2025

Confidentiality: low

Availability: high

Integrity: high

Author: Jürgen Sterr / CTO

Contributors:

- Tobias Kellner / ISB

Interested Parties:

- Sales/DevSecOps/CX
- Customers

Version history

Version	Date	Updated by	Approved by	Changes
1.0.0	14.03.2023	Jürgen Sterr	Erik Reiter	Document was created initially.
1.1.0	07.01.2025	Tobias Kellner	Jürgen Sterr	Added further statements and increased accuracy.

1 Content

2 Cloud Security Policy

2.1 Goal

Especially in the IT environment, this security guideline is intended to help raise awareness of the potential risks and provide appropriate instructions for action. When data is collected, stored, or processed with the help of cloud services, there are special risks. In particular, the dynamic distribution of storage capacities across different locations, which are usually not known to the user, require specific precautions with regards to information security and the protection of information.

2.2 Area of effect

This policy applies to all employees of IT Manufactory GmbH when they collect, store or process data in the cloud as part of their official activities.

2.3 Responsibilities

Responsibility for cloud security lies with the DevSecOps department of IT Manufactory GmbH and our cloud service providers. We are responsible for ensuring that the cloud security policy is regularly reviewed and adhered to.

2.4 Cloud security

IT Manufactory GmbH exclusively uses cloud services in all areas of the company. Every employee whose official activities are directly or indirectly affected, is obliged to always comply with the relevant instructions of the IT Manufactory GmbH.

- The storage and processing of official data in third-party cloud services, such as pCloud, Strato HiDrive, Dropbox, Luckycloud, Google Drive or similar services, is generally not permitted.
- The retrieval of chargeable information for private use is prohibited; for service use, this is only permitted with the approval of the management.
- Private uploads and downloads that are not urgently required for official use are not permitted.
- Passing on passwords and access data to cloud services is prohibited.
- Access to cloud services by other persons is prohibited.
- Changes to the configuration without the clear consent and instruction of the supervisor are prohibited.

When deciding in which applications data is collected, stored, or processed in the cloud, there are clear segregations of duties and responsibilities. If there are any uncertainties regarding the data in the cloud services, further documents are available in the ISMS documentation.

2.5 Information security

Our ISMS and the information security guidelines of IT Manufactory GmbH make it clear, that the provisions of the Data Protection Act (BDSG) as well as the General Data Protection Regulation (GDPR) apply to the processing of personal data in the cloud. It requires either the consent of the data subjects (in the case of data processing outside the EU), or the application of the regulations for commissioned data processing (data processing within the EU).

In addition, business secrets as defined by the German Act on the Protection of Business Secrets (GeschGehG) also constitute data requiring protection. In principle, business secrets may only be disclosed if the respective contractor or business partner has previously been obligated to maintain confidentiality and the security level to be maintained for the protection of the data is guaranteed at the recipient of the data.

2.6 Data security education and training

Every employee of IT Manufactory GmbH must regularly attend training sessions on the procedure to be followed in the event of security incidents, data breaches and on the significance and possible consequences of breaches or must obtain information on this from the ISMS Officer of IT Manufactory GmbH.

2.7 Access management

IT Manufactory GmbH controls the registration and deregistration of users in such a way that the allocation of user access, as well as information access restriction, is only permitted to an authorized group of persons within the scope of official activities.

2.8 Cryptographic measures

The employee shall primarily use encrypted networking channels. For teleworking (home office / mobile working), the teleworking guidelines apply. The use of encryption procedures and optional encryption is mandatory.

2.9 Separation of environments

Each employee must comply with the data protection measures, including risk assessment, even in situations where test data is used.

2.10 Data storage

When using cloud services, the data volume must be kept to the necessary minimum. The primary storage location for data is the Microsoft SharePoint document management system of the IT Manufactory GmbH. Cloud provider backups are configured as far as possible. Further documentation on backing up information can be found in the data security policy.

2.11 Data deletion

Cloud storage providers generally use storage technologies that make efficient use of physical storage capacities. Due to this storage technology, data can often only be deleted after a certain period of time. In principle, it cannot be ruled out that the data is only hidden from the user when the deletion command is transmitted, but not deleted. For this reason, the physical deletion of data cannot be influenced by the IT Manufactory GmbH. Nevertheless, our cloud storage providers take care of this process, and it is guaranteed that the data will be deleted within an acceptable time frame.

2.12 Event logging

Access and changes of all kinds are logged at all times as far as possible and reasonable. Logged information is only used for authorized purposes and by authorized employees. The data will be deleted regularly after appropriate and documented periods have expired.

2.13 Non-disclosure agreements

Every employee of IT Manufactory GmbH is obliged to maintain confidentiality as part of their employment contract.

2.14 Reporting of violations

If personal data or business secrets are breached or such a breach is imminent (e.g., loss of work equipment or documents, hacker attacks, etc.), the employee must inform the management or supervisor immediately. If necessary, the IT department must also be informed immediately.

2.15 Important contact details

The mentioned persons can be found in the **emergency contacts** list in the ISMS documentation.

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