Data Backup Policy

Digital Automotive

Version: 1.2.0

Date: 23.05.2025

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	18.07.2023	Jürgen Sterr	Erik Reiter	Document created initially
1.1.0	07.01.2025	Tobias Kellner	Jürgen Sterr	Added styling, declarations concretized
1.2.0	23.05.2025	Tobias Kellner	Jürgen Sterr	Updated backup plan for Kubernetes migration

1 Content

2 Data Backup Policy

2.1 Goal

The goal of this policy is to ensure that all information collected, stored, or processed by IT Manufactory GmbH and our customers through our Digital Automotive SaaS application is secured in a reliable, secure, and complete manner. We ensure that all secured data remains confidential and that we comply with all applicable laws and regulations.

2.2 Area of Effect

This policy applies to all employees of IT Manufactory GmbH when they set up, maintain, or perform data backups as part of their official duties.

2.3 Responsibilities

Responsibility for data backup lies with the DevSecOps department of IT Manufactory GmbH and our cloud service providers. We are responsible for ensuring that the data backup policy is regularly reviewed and adhered to. We are responsible for ensuring that data is backed up on a regular basis and that backups are kept in a secure, encrypted location.

2.4 Identification and classification

A determination must be made regarding which data are considered official records and therefore need to be specially protected. This determination is made by classifying the records into different categories based on their sensitivity and importance.

Further information can be found in the classification policy.

2.5 Data backup

IT Manufactory GmbH is responsible for ensuring that all data is regularly backed up to minimize the loss of data due to accidental deletion, hardware failures, security incidents, or other causes. Regular backups ensure that, in the event of an incident, data availability can be restored, and downtime is reduced.

2.5.1 Backup environments and systems

2.5.1.1 Production/Trial systems

The production and trial systems are provided via the infrastructure from Microsoft Azure Cloud and are connected to Azure's backup services which also apply encryption and integrity to the backups. If not stated differently the hosting location is *North Europe*. The following backup policies are applied:

- **Database:**
  The databases are provided by the "Azure Database for PostgreSQL - Flexible Server" service. Automated full backups of the databases are performed daily. The backups are retained for 30 days and are stored geo redundantly.

In addition to the cloud backup, daily full backups of all databases are created on a selfhosted NAS system. These daily backups are retained for 30 days before being automatically deleted. A monthly backup from the 1st of each month is kept for at least 6 months. The customer can request early deletion of data (e.g., in case of termination of the business relationship). This NAS system is equipped with RAID protection to provide additional security against hardware failures. The backups are also encrypted to protect against unauthorized access.

- **Documents & Images:**
  The file resources are provided by the "Azure Storage Account – File shares" service. Automated full backups of the file share are performed daily. The daily backups are retained for 30 days. A monthly backup from the 1st Sunday of each month is kept for 6 months. All backups are stored geo redundantly.
  In addition to the cloud backup, daily full backups of all file resources are created on a selfhosted NAS system. These daily backups are retained for 30 days before being automatically deleted. A monthly backup from the 1st of each month is kept for at least 6 months. The customer can request early deletion of data (e.g., in case of termination of the business relationship). This NAS system is equipped with RAID protection to provide additional security against hardware failures. The backups are also encrypted to protect against unauthorized access.

2.5.1.2 Staging systems

The staging systems are provided via the infrastructure from Digital Ocean. If not stated differently the hosting location is *FRA1*. The following backup policies are applied:

- **Database:**
  We perform daily full backups of all databases on a selfhosted NAS system. These daily backups are retained for 30 days before being automatically deleted. A monthly backup from the 1st of each month is kept for at least 6 months. The customer can request early deletion of data (e.g., in case of termination of the business relationship). This NAS system is equipped with RAID protection to provide additional security against hardware failures. The backups are also encrypted to protect against unauthorized access.
- **Documents & Images:**
  We perform daily full backups of all file resources on a selfhosted NAS system. These daily backups are retained for 30 days before being automatically deleted. A monthly backup from the 1st of each month is kept for at least 6 months. The customer can request early deletion of data (e.g., in case of termination of the business relationship). This NAS system is equipped with RAID protection to provide additional security against hardware failures. The backups are also encrypted to protect against unauthorized access.

2.6 Access control

IT Manufactory GmbH controls the registration and deregistration of users in such a way that only authorized personnel are allowed to access the systems for data backup purposes.

2.7 Physical protection

Use of secure physical locations for storing records, such as lockable cabinets, secure data centers, and secured in-house server rooms. Implementation of monitoring systems such as cameras, alarm systems, and access control systems to control and monitor physical access to the records.

2.8 Data Recovery

In the event of data loss, IT Manufactory GmbH ensures that information is restored and made available as quickly as possible. We use backups to restore lost or damaged data and ensure the integrity of the data. The goal is to prevent any data loss. Regular data backups and recovery procedures are in place to ensure that in the event of data loss, only minimal data loss occurs. However, the exact extent of a possible data loss depends on various factors, such as the frequency of data backups and the amount of data that has been created since the last backup. However, we strive to reduce potential data loss to an absolute minimum. In the event of failure, the maximum data loss is prevented until the last backup, which is always less than 24 hours ago.

2.9 Cryptographic measures

IT Manufactory GmbH ensures that all secured information remains confidential. The created backups are stored on an encrypted location which is under the control of IT Manufactory GmbH.

2.10 Review and testing

IT Manufactory GmbH ensures that all backups are regularly checked for integrity and completeness to ensure that they can be restored if necessary. We also perform regular testing to ensure that our backup and restore processes are working properly.

2.11 Separation of environments

IT Manufactory GmbH has taken data protection measures, including risk assessments, into account for situations where test data is used.

Further information on the separation of operational environments can be found in section A 12.1.4.

2.12 Data deletion

The retention periods for backups are defined taking into account legal and operational requirements. The exact retention periods have already been mentioned in the data backup section. Expired backups are securely and completely deleted according to established deletion policies. We store data only as long as it is necessary for smooth operations, contractual obligations, or legal requirements. An example of a legal requirement is the General Data Protection Regulation (GDPR). Therefore, all customer data will be deleted when, for example, the business relationship ends, as the purpose of data processing no longer applies. Any exceptions due to other legal regulations should be noted. The deletion of individual records (e.g., user records) is also possible upon request. IT Manufactory GmbH commits to performing data deletion within one week of being notified.

Additionally, it is worth mentioning that our cloud providers use storage techniques that ensure the physical storage capacity is used efficiently. Therefore, the final physical deletion of data may take some time. IT Manufactory GmbH has no control over this process.

2.13 RTO & RPO

2.13.1 Recovery Time Objective

The Recovery Time Objective (RTO) defines the maximum allowable downtime for restoring services after a disruption, ensuring minimal impact on operations. For all services, the RTO is set at 4 hours if the failure is noticed during working hours. The working hours are defined as Monday to Friday from 8:00 AM to 5:00 PM CET/CEST (excluding national holidays). Backup systems and recovery processes are designed to meet this target, with regular testing to verify adherence. In the event of an incident, restoration efforts will prioritize achieving service availability within the defined RTO to maintain operational continuity and reduce the risk of prolonged outages.

2.13.2 Recovery Point Objective

The Recovery Point Objective (RPO) establishes the maximum allowable data loss in terms of time during a disruption, defining the point in time to which data must be restored to resume operations. For all services, the RPO is set at 24 hours, ensuring that backups capture data frequently enough to meet operational requirements. Backup schedules and replication processes are configured to align with this objective, minimizing potential data loss. Regular reviews and testing are conducted to ensure that backup systems meet the defined RPO, safeguarding data integrity and reliability.

2.14 Side services

All side services, including but not limited to the authentication service and the messaging service, are subject to the same backup policies and procedures as the main service. These services are critical to the overall functionality and security of the system and must maintain consistent data integrity and availability. Regular backups of configuration files, logs, databases, and other critical data associated with these side services will be performed following the same schedule and retention periods as the main service. In addition, recovery processes will be tested periodically to ensure seamless restoration in case of failure, adhering to the defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for the main service.

2.15 Event logging

Logging of backups and all types of data backups are visible at any time as far as possible. Log information is used only for authorized purposes and authorized employees of IT Manufactory GmbH. All logs are regularly deleted after the expiration of reasonable and documented periods of time.

2.16 Compliance

IT Manufactory GmbH ensures that we comply with all applicable legal regulations and contractual requirements that relate to data backup.

We ensure that all backed up information is handled in a secure and lawful manner.

The organization's approach to handling data protection and its implementation are independently reviewed at scheduled intervals or whenever significant changes occur.

To this end, we subject our ISMS to regular independent audits by external auditors in accordance with ISO 27001.

2.17 Changes

IT Manufactory GmbH reserves the right to change this data backup policy at any time. We will inform our customers of any changes and ensure that they are up to date with our data backup policy.

2.18 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.

2.19 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