5.1.1 Data Backup Policy

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.

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.

Responsibilities

The Responsibility for cloud security lies with IT Manufactory SecOps and with our SaaS-Providers. We are responsible for ensuring that data is backed up on a regular basis and that backups are kept in a secure, encrypted location.

Data backup

IT Manufactory GmbH is responsible for ensuring that all data is backed up on a regular basis to minimize loss of data due to accidental deletion, hardware failures, security incidents or other causes. We perform regular backups to ensure that all data is protected and losses due to accidental deletion, hardware failures, security incidents or other causes are minimized. We perform daily incremental backups as well as weekly full backups. These backups are backed up to an encrypted internal location.

Access control

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

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 that all integrity and availability is restored. 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 a server failure, the maximum data loss is prevented until the last backup, which is always less than 24 hours ago.

Cryptographic measures

IT Manufactory GmbH ensures that all secured information remains confidential.
We use strong encryption protocols to ensure that all secured data is protected.

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.

Separation of development-, test- and production environments

IT Manufactory GmbH must also consider the data protection measures including risk assessment for situations in which test data is used.

Data deletion

The backups are automatically deleted as soon as they are older than 35 days. We pay attention to the compliance with the usual data storage and store the data on the database only as long as it is necessary for the smooth operation. Upon request, it is also possible to delete all user data. However, SaaS providers of cloud storage usually use storage techniques to make efficient use of physical storage capacity. Due to these techniques, it may take some time before the data can be completely deleted.

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 autjhhorized employees of IT Manufactory GmbH. All logs are regularly deleted after the expiration of reasonable and documented periods of time.

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 technical, 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.

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.

Reporting of violations

Procedure for breaches of the cloud security policy:
If personal data, trade secrets are breached or such a breach is imminent (e.g. loss of work equipment or documents, hacker attacks, attacks by malware, etc.), the employee must immediately inform the management, supervisor or data protection officer. In the event of IT breaches, the IT department must also be informed immediately.

Important contact details

IT emergencies: ISMS officers (see emergency contacts)

Location, Date

Passau, 14.03.2023

Management