# 5.1.1 Cloud security policy



## 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.

## 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.

## Responsibilities

The Responsibility for cloud security lies with IT Manufactory SecOps and our cloud service provider. We are responsible for ensuring that the cloud security policy is regularly reviewed and adhered to.

## 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 data in the cloud services, there is further documentation in Non-Organizational IT Services.

## Information Security

Our IMS 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 (DSGVO) 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.

## Datasecurity 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.

## 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.

## Cryptographic measures

The employee shall primarily use the encrypted Internet access of IT Manufactory GmbH. For teleworking (home office / mobile working), the teleworking guidelines apply.
The use of encryption procedures and optional encryption is mandatory.

## Separation of development-, test- and production environments

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

## Data storage

When using cloud services must the data volumes be limited to the minimum necessary. The primary storage location for data remains the Microsoft SharePoint document management system of IT Manufactory GmbH. Cloud provider back-ups are configured as far as possible and relevant.
Further documentation on the backup of information can be found in the data security policy.

## Data deletion

Cloud storage providers usually use storage techniques that efficiently utilize 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 when the delete command is sent, the data is merely hidden for the user but not deleted. For this reason is data that is subject to a legal obligation to delete unsuitable for storage in the cloud.

## Event logging

Logging of accesses and all types of changes will be as far as possible and relevant to view at any time. Log information is used only for authorized purposes and authorized employees. The data is regularly deleted after the expiry of reasonable and documented periods.

## Confidentiality or non-disclosure agreements

Every employee of IT Manufactory GmbH has the obligation of secrecy within the scope of his employment contract.

## Reporting of violations

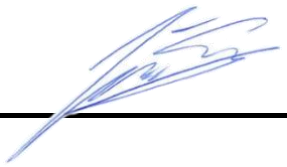
Procedure for breaches of the cloud security policy:
If personal data, trade secrets are breached or such a breach is imminent (e.g. loss of work equipment or documents, hacker attacks, attacks by malware, etc.), the employee must immediately inform the management, supervisor or data protection officer.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