**Data backup policy**

# Purpose

The data backup policy provides comprehensive documentation of the applicable regulations in the company and measures taken for data backup. It also serves as evidence to third parties that the legally required availability control is carried out correctly.

# Responsibilities in the company

* Companies have to provide for IT security and data backup.
* Corporate management is directly responsible for this and is personally liable where applicable.

# General legal conditions

* The law requires certain controls via technical and organisational measures, both with processing data for one’s own purposes and with commissioned data processing; in this context, an availability control applies in particular.
* Verification of the controls or technical and organisational measures is, inter alia, to be provided to customers within the scope of commissioned data processing.

# Risks

* Human error: incorrect operation/accident, sabotage, attack
* Technical disruptions: technical malfunction, hardware failure, line disturbance
* Force majeure, accidents, catastrophes: water, fire, etc.
* Significant to existentially threatening effects on companies possible

# Data backup procedures, options

* Complete backup
* Incremental backup
* Differential backup

# Minimum technical and organisational regulations

## General regulations

* Data backup must be performed responsibly and competently
* No accidental bypassing of authorisation models by data backup measures
* Confidentiality and obligation to data protection
* Nomination of people responsible for each task area
* Determine need for confidentiality, integrity and availability

## Technical implementation

* Create data backup plan
* Determine retention period and number of generations
* Coordination with the emergency-prevention policy
* Sufficient documentation and logging: especially backup data, backup scope, backup parameters
* Arrange the recovery procedure
* Create inventory directory
* Ensure the evaluation of logs
* Tests on data reconstruction/restoration and emergency drills
* Set up necessary controls, especially access control
* Implement the protection requirements for confidentiality, integrity and availability
* Specify and secure transport routes
* Allocate capacities: throughput, volume, quantity of data-storage devices
* Implement requirements for seamless backup (mobile computers, PDA/MDA, databases, open files, system data, log data, etc.)
* Especially ensure access control, access-permission control, transmission control, input control and separation control, also with regard to data backup sets.