



Number:

Title:

Title (EN):

Type:

Scope:

Area:

Country:

Previous Number:

Document Information

Revision:

Status:

Effective Date:

1 OBJECTIVE

This Standard Operation Procedure defines processes for backup and restore of data and applications at Grünenthal, applied at a Global level, including all sites and subsidiaries.

The Backup and restore processes defined in the present procedure protects Grünenthal digital assets. Data, records and software can be restored in case of failure, loss of integrity, unexpected modification during operation or damage of the original.

2 SCOPE

This document applies to data, records and application hosted on Grünenthal Headquarters and locations/subsidiaries premises and supported by GIT.

Global IT offers a default backup and restore service for systems and server applications as described in Chapter 5.1.

Backup or restore of end user devices are out of scope, they are under users/System Owners responsibility.

Standalone systems (not connected to the network) and non-server operating system are not covered by this procedure.

Backup and restore process executed by cloud suppliers for SaaS applications is not in scope of this procedure.

3 RESPONSIBILITIES

The responsibilities of roles listed in this document are as follows:

Role	Responsibility
Business Process Owner (BPO)	The BPO is the owner of the process and the related associated Data / records. The BPO defines the business requirements for protection of the application and the application data.
System Owner (SO)	The SO has the technical responsibility of the computerized system, including availability, support, maintenance security and integrity of the data. SO can be also called Service Owner. SO is in direct contact with the AM.
Application Manager (AM)	The AM is responsible for the administration of an IT application. The AM can use the centralized backup services to protect data of applications within her / his responsibility if necessary. The development of recovery procedures and processes to rebuild the running application belongs to the AM's responsibility.
Application Manager Backup (AM Backup) GIT	The AM Backup (and his deputy) is responsible for administration and maintenance of backup tools and media. He / She will schedule backups according to the definitions given by the BPO / AM. In addition, the AM backup will restore data on request of the BPO / AM or according to pre-defined test schedules.

4 TERMS AND DEFINITIONS

Term	Definition / Explanation
Backup	Backup is the process of copying records, data and software to protect against loss of integrity or availability of the original. In the context of this document "backup definition" will also refer to the scheduling of backups in backup tools.

Term	Definition / Explanation
Backup definitions	It is composed by "backup jobs" or "backup policies" where the configurations and settings are defined.
Backup generation	Backed-up data must be kept for well-defined time. The definition of a backup includes a decision how many backup generations to retain (may vary per system / application). The retained backups (corresponding to multiple points in time for restore) represent backup generations. Backup generations are subject to aging (i.e. they will be automatically deleted at the end of the retention period).
Backup media	Backup media are mass storage media (e.g. clouds or disk storages) that are used to store backed-up data.
Backup schedule	Besides the option to invoke a one-time backup (e.g. prior to planned changes on IT systems), most backups run according to a defined schedule. The backup schedule is part of the backup definition.
Backup tool	At Grünenthal, multiple backup tools are in use. The choice of an appropriate backup tool to given backup requirements lies within the responsibility of the AM Backup.
Backup window	For some applications, running backups will degrade the service quality of the application - sometimes even an application downtime will be required for backup. With respect to this fact, the backup definition of such applications will include backup windows during which the backups are performed. The backup window is part of the backup definition.
Full backup & Incremental backup	A full backup represents a complete copy of all data to be backed up to the backup media. To reduce backup media consumption, incremental backups only store data that has changed since the last backup. Starting with one full backup multiple backup generations may be stored as incremental backups.
Data Mirroring	Enterprise level storage systems allow to copy storage data "on the fly" to a secondary storage system. Every block of data that is written to the primary storage is mirrored immediately to a secondary storage system. At Grünenthal, data mirroring is implemented to mitigate disaster scenarios (e.g. if the primary storage fails). In these scenarios, mirrored data on the secondary storage system can be activated. Data mirroring cannot be regarded as a solution for backup & restore.
Snapshots	In virtualized environments, data, complete servers or storage units can be subject of snapshotting. When a snapshot is invoked, all current data in scope gets frozen. Starting from that point in time, data changes (add, modify or delete) are stored to another place with references to the snapshotted data. On demand, snapshotted data can be reverted back to the point in time when the snapshot was taken. Grünenthal makes use of several snapshot techniques to implement the backup definitions.
Restore	Restore is the subsequent restoration of records, data or software when required.
Recovery	"Recovery" are techniques to rebuild IT applications on an infrastructure (i.e. servers or applications) to a backed-up recovery point. Outcome is a running application.
Service Desk	Service Desk is the first level support for users
End User Devices	Any IT hardware device, which Grünenthal individually assigns to a specific employee or which Grünenthal otherwise makes available to its employees, including temporary workers, regardless of whether such device is stationary or handheld, for example: <ul style="list-style-type: none"> • Personal Computers (PCs). • mobile phones/smartphones. • tablet-computers, e-readers. • printers. storage devices.
RPO	Recovery Point Objective (RPO) is the distance between points in time to which systems can be recovered to, or data can be restored to. An RPO of 1 day means, that on every day a backup is made.
ITSM	Information Technology Service Management System. System in which the most important IT processes are managed. In the ITSM system all changes and configuration activities on the IT-Infrastructure are managed and documented.
GDPR	General Data Protection Regulation

Term	Definition / Explanation
RTO	Recovery Time Objective defines how quickly data needs to be restored in case of failure or disaster.
TLogs	Transaction logs.

5 PROCESS

The following backup and restore services are offered by Global IT. This Standard Operating Procedure describes:

- Default backup services
- Definition of individual backup requirements
- Backup process and control
- Regular restore tests
- Retention periods of backup sets
- Spatial separation of original data and backup data

5.1 Default backup services

The following default backup service definitions are applied before and after every software modification, only applied to production servers/applications (quality and development environments only by request).

RTO definition is according to Incident Management SLA's (PROC-002095). All Backup windows and schedules are defined according to local time zone.

Default backup service for servers provided by GIT	
Backup schedule	Full: 1 backup per weekend (Friday to Monday) Incremental: 1 daily backup on Monday to Thursday
Single file restore possible	Yes
RPO	1 working day
Backup window	Monday to Thursday: 22:00 to 06:00 and Friday 22:00 to Monday 06:00
Backup retention	Daily backups: 4 weeks One backup per month: 3 month
Backup type	Veeam Image Level Backup
Backup Copy	Azure Blob Storage
Backup Copy Retention	7 daily in Capacity tier + 12 monthly in Archive tier

Default backup service for file share data on primary NetApp storage (does not include file shares on servers)	
Backup schedule	<p>Incremental:</p> <ul style="list-style-type: none"> • 2-hourly snapshots: 4 per day (Monday to Sunday) • Daily snapshots: 1 per day (Monday to Saturday) <p>Full: Weekly snapshots: 1 per weekend (Sunday)</p>
Single file restore possible	Yes
RPO	<p>According to backup schedule:</p> <p>Incremental:</p> <ul style="list-style-type: none"> • 2-hourly snapshots: 4 per day (Monday to Sunday) • Daily snapshots: 1 per day (Monday to Saturday) <p>Full: Weekly snapshots: 1 per weekend (Sunday)</p>
Backup window	24/7 (production and non-production environnements)
Backup retention	<p>2-hourly snapshots: 24 hours</p> <p>Daily snapshots: 12 days</p> <p>Weekly snapshots: 12 weeks</p> <p>Monthly snapshots: 12 months</p>
Backup Type	Netapp Snapshot + Snapmirror Veeam File Backup*
Backup Copy*	Azure Blob Storage
Backup Copy Retention*	92 days

*On top of "Netapp Snapshot". Not part of the default service: a demand is required.

Default backup service for databases	
Backup schedule	<p>1 backup per weekend (Friday to Monday)</p> <p>1 daily backup on Monday to Thursday</p> <p>TLogs backups every 15 min</p> <p>For non-production systems: 1 backup per week (weekend)</p>
Single item restore possible	No
RPO	<p>For production systems: 1 working day</p> <p>For non-production systems: 1 week</p>
Backup window	24/7 (for production and non-production environments)
Backup retention	4 weeks

Backup Type	Veeam image Level backup + TLogs backups * and when applicable RMAN Backup (to Veeam)
Backup Copy	Azure Blob Storage
Backup Copy Retention	7 daily in Capacity tier + 12 monthly in Archive tier

* TLogs backups are retained until the corresponding image-level backup is deleted.

Default backup service for applications provided by MS Office 365 (for example: Exchange online, Sharepoint Online, OneDrive for Business, Teams, Groups, Planner, ...)	
Backup schedule	at least one backup per day for each application
Single item restore possible	Yes
RPO	1 working day
Backup window	None
Backup retention	1 year

5.2 Defining individual backup services

If backup requirements differ from the default backup services described in chapter 5.1, the Business Process Owner is responsible for defining the data requiring backup and the Application Manager of the related system is responsible to provide a demand for a specific backup definition to GIT department. The request is documented in ITSM (Demand module) and must specify the individual backup requirements based on the following parameters:

- Data, files or systems to be backed-up
- If applicable: files to be excluded from backup
- If applicable: the possibility of single item restore
- RPO definition
- Which / how many backup generations to be kept
- If required: the backup window definition
- Name of the responsible Process Owner or Application Manager who authorizes restores or changes.

5.3 Backup process control

Backups Access Control

Strict access policies must be implemented and regularly reviewed. Access to backup servers and management consoles must follow the principle of least privilege, ensuring that only authorized personnel with a legitimate operational need can perform backup and restore operations. Role-based access control (RBAC) must be enforced to segregate duties (e.g., backup administrators, security auditors, and storage managers), minimizing the risk of misuse or error.

To further enhance security, backup servers must be kept outside the corporate Active Directory domain. This isolation reduces the risk of lateral movement in case the domain is compromised, preserving the integrity of the backup infrastructure. It ensures that, even in the event of a ransomware attack or privilege escalation within the domain, the backup systems remain secure and accessible for recovery.

Additionally, access logs must be enabled and monitored to detect and investigate any unauthorized activity. Combining logical access controls with network segmentation and strong authentication mechanisms—such as multi-factor authentication—further strengthens the resilience of backup systems against both internal and external threats.

Implementation of backup definitions

The AM Backup will implement backups according to backup service definitions as defined in 5.1 “Default Backup Services” or 5.2 “Defining Individual Backup Services”. For any implemented backup definition, the AM Backup will check the successful completion of the first backup by default and troubleshoot backup problems, if necessary. This implementation is documented through the service request (if default services apply) or an IT change is opened (if individual backup services apply).

After the first Backup the AM Backup will restore a sample file (a random file or it can also be a notepad file “Test” with date and time created by the AM Backup) and check the restore job for successful completion by comparing the restored sample file with the original file. This must be a task in the Service Request or in the IT change.

Backup monitoring

The AM Backup is responsible for monitoring the completion of all backups on every working day (Monday to Friday, except for public holidays). The monitoring system provides information and/or warnings regarding the backup result (passed/failed). In case of any failed backup, an Incident in ITSM (follow PROC-002095) is created automatically and the Application Manager is notified. Backup Manager is required to analyze the cause of the failure and implement corrective measures (usually a repetition of the backup during the day).

The Application Manager and the Business Process Owner will evaluate if a quality event/deviation is needed to be raised, in compliance with GxP regulations.

Managing secondary repository for backup media

As backup target, different storage media types are useable. If backup is performed onto suitable backup cloud storage, the backup tool automatically verifies backup data stored on the cloud (as part of the backup execution) and recognizes poor backup media. The AM Backup is responsible for maintaining the available space on the cloud (blob storage).

Changes to backup definitions

If a change in existing backup definitions is required (e.g. a changed backup schedule or a pause of backup execution for planned application maintenance) the AM or BPO needs to open a service request in ITSM. If the system is GxP relevant, the AM or BPO

is responsible to assess if a MOC (following PROC-007059) or any other documentation is required to document this change. The AM Backup will implement the changes accordingly.

The AM Backup may apply changes to backup tools if required to maintain the backup functionality and if the agreed backup definitions are not violated by the changes, e.g. definition of changed backup target media / storage or rescheduling of backups within the backup window may be needed in daily business. All the described changes must follow the procedure PROC-004973.

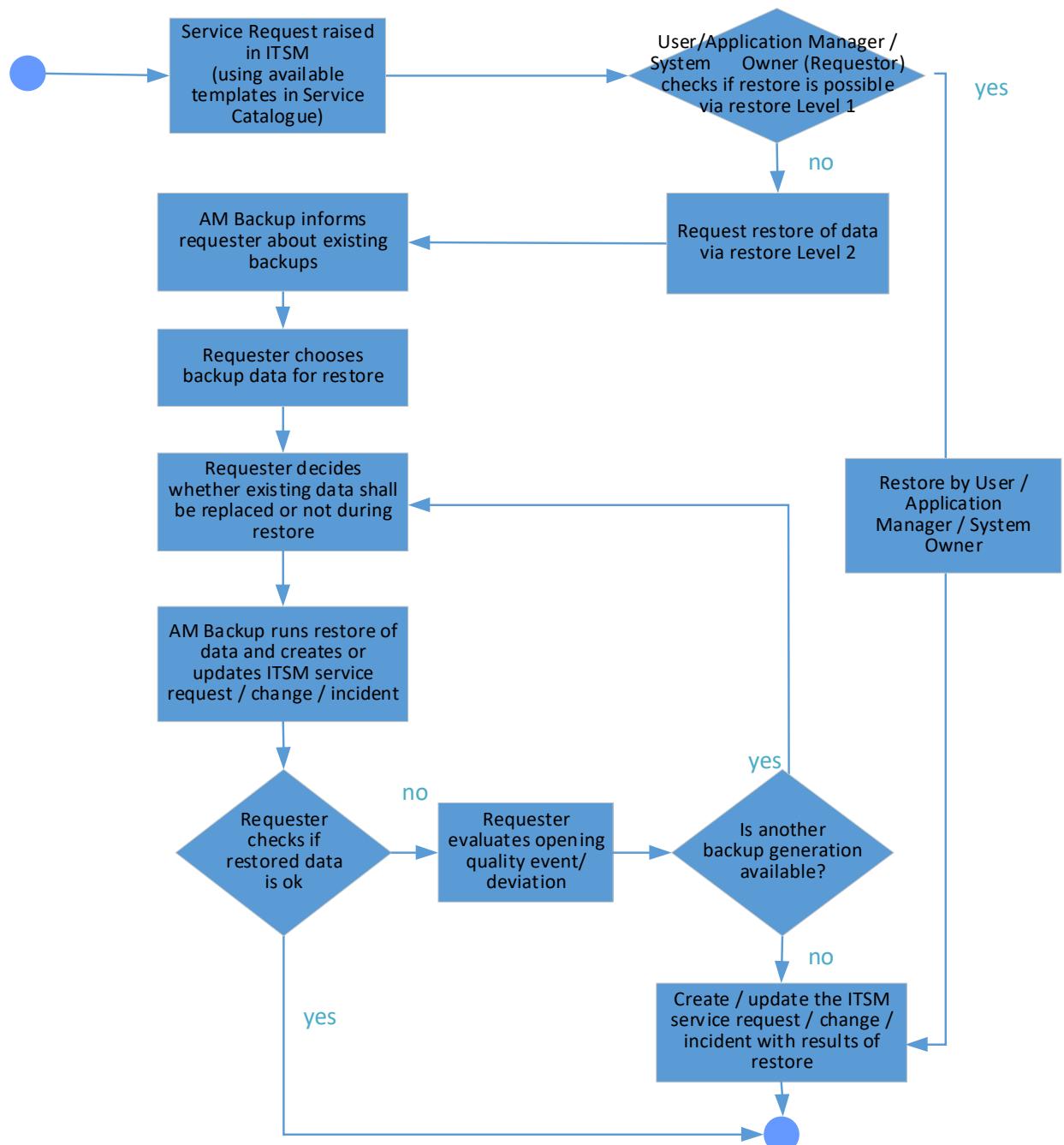
Restore process

Detection of lost or defective data lies in the responsibility of the User, AM or the BPO. The person that detects data loss or defective data (user, AM or BPO) must open a quality event/deviation in case this affects a GxP relevant system, following PROC-005388 and PROC-004019.

The AM Backup will only restore data on explicit request by the User, AM or BPO. A Service Request in ITSM is required to start into the process of restore. The User, AM or BPO that identified the quality event/deviation must introduce the Service Request number as action item in Quality Management System. The restore operation must be documented in the service request through print screens or description.

In case if a GxP or critical system is restored, the Application Manager is responsible to verify and test the correctness of system functionality after the restore (e.g. validation activities). In case the restore fails, a roll back plan must be assessed case by case by the Application Manager together with AM Backup.

The following workflow chart shows the process in detail.



Application	Restore Level 1	Who ?	Restore Level 2	Who ?
Server System	n.a.	n.a.	Server Filesystem data or whole Server System via local Backup solution	Local AM Backup
Filesystem (on Windows Server)	Local VSS (Volume Shadowcopy Services)	User Self-Service	Server Filesystem data via local Backup solution	Local AM Backup
Filesystem (on NetAppFiler)	Local Snapshot	User Self-Service	Remote Snapshot or via local Backup solution	Local AM Backup
Exchange Online	Recycle Bin	User Self-Service	Restore via O365 Backup	Global AM Backup
OneDrive for Business	Recycle Bin	User Self-Service	Restore via O365 Backup	Global AM Backup
Sharepoint Online / Business Worlds	Recycle Bin	User / Owner Self-Service	Restore via O365 Backup	Global AM Backup
TEAMS	Recycle Bin	User / Owner Self-Service	Restore via O365 Backup	Global AM Backup

Decommissioning of backup definitions

A Service Request in ITSM is required to start into the process of decommissioning a system. The requestor (AM, BPO) is responsible to issue the needed documentation (MOC, risk assessment, any other) if the system under decommissioning is GxP relevant. When systems or applications are taken out of service the AM Backup will delete the backup definitions accordingly (this must be a task in the Service Request).

5.4 Periodical restore tests for validated systems

For validated applications / systems, restore of data will be tested at least once per year for productive systems (no restore tests for non-production systems). GxP machines are listed in SUP-011745. This list is updated with info present on the CMDB (reviewed once a year). The local AM Backup will restore sample data files and check the restore job for successful completion by comparing restored and original files. The AM Backup will inform the AM about the results of the restore test. Results are recorded using template SUP-011708 and shared with the AM. These documents are also attached to the IT change opened to document the restore tests. These documents are checked during system Periodic Review – see PROC-004035 and PROC-007444.

However, these tests verify if the backup tool is working as intended. Additional restore procedure that require data integrity checks, must be address by the AM to the AM backup through a service request in which AM identifies the file or database that can

be restored as part of the test. AM must confirm the data integrity of the restored files after restoring. This must be documented within system's validation context.

5.5 Backup retention

Backup generations are retained securely for the defined retention period according to the backup definitions – see: 5.1 “Default backup services” and 5.2 “Defining individual backup services”.

5.6 Spatial separation of original and backup data

Backup data must be stored in a different geographic location than the original data but remaining in a location compliant with local regulation, to assure all applicable data privacy requirements, including GDPR and HIPAA. This means that data produced in Europe shall remain in European Union and European Economic Area, data produced in South America shall remain in South America Market, and data produced in the United States shall remain in the United States.

6 REFERENCES

Not applicable.

7 HISTORICAL INDEX

Version/ document no.	Description of changes
01	Migration to MasterControl System (PROC-004359)
02	General content review, scope changed from local to global, changed from none GxP to GxP (PROC-005477)
03	General review of the document in the context of CAPA-2024-0403. Managing secondary repository for backup media changed for cloud.