Backup Policy

Media storage service



Project Members:

* Kaloyan Andreev

Elaboration Date: 05/06/2022

Table of content

[1. Purpose of this document is to ensure that a consistent procedure is used for the backup of critical for the company data: 2](#_Toc106215440)

[2. Scope 2](#_Toc106215441)

[3. Backup Policy 2](#_Toc106215442)

[4. Restoration 2](#_Toc106215443)

# Purpose of this document is to ensure that a consistent procedure is used for the backup of critical for the company data:

* Backups are in place to ease system recovery in case of a major disaster or hardware failure.
* Backups are in place to help recovery of vital systems and applications for the company as well as important documents.

# Scope

* + This document is applicable to Media storage service and covers OS, applications, logs, critical devices and files.

# Backup Policy

* + Backup should be made on a regular basis that will ensure the continuity of processing in the event of a processing interruption.
  + All backups must be recorded, identified and securely stored and disposed following secure procedures.
  + Copies of backup files and documents must be kept off-site in a secure location.
  + There should be a periodic testing of backup media at both on-site and off-site locations (at least once a year) to ensure that backup are in useable condition for recovery and that their contents are as documented. Copies of backups moved to and from off-site storage must be provided with a level of security.
  + All backups and backup related processes must be monitored and logged.
  + When a computer equipment is changed, consideration should be given to the backup media and data formats to ensure that they can still be restored.
  + Automated backups must be used where applicable.
  + The backup strategy for each system must be formally documented and approved by the system and data owners.
  + All on-site and off-site tape must be properly labelled.

# Restoration

* + In the event of system failure, escalation procedure must be in place and made aware to system administrator.
  + Recovery and restart procedures must be established and brief to relevant parties. The document must be easily accessible to the authorized parties.
  + Source documents, reports and backup media for reconstruction of a system must be identified and documented.
  + Restoration of the current configuration must be within agreed recovery timescales.