Backup & Restore Policy

Brunel University London

***An ISO/IEC 27001:2013:** Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security Officer

Document History

Version	Author	Comments	Date
V 0.1	Andrew Clarke	First Draft	08/02/2018
V 0.2	Andrew Clarke	Multiple technical revisions from P Polkinghorne	01/03/2018
V 0.3	Andrew Clarke	Amendment to Bronze level backups/restore	05/03/2018
V 1.0	Andrew Clarke	CISA Approval (add Cloud backup RTO/RPO provision, replace reference to BackupExec with BackupExpress)	07/09/2018

Document Approval

The contents of this document are classified as Protect to Brunel University London (University) information classification. Proprietary information presented in this document may not be used without written consent from University and remains the exclusive property of University unless otherwise agreed to in writing.

This document requires the approval from University as defined in the ISMS Compliance document.

Document Owner: Andrew Clarke	Document Approver: Mick Jenkins
Cyber & Information Security Manager	Chief Information Security Officer

Document Distribution

Name	Title	Version	Date of Issue

Contents

1. About this document

1.1 Purpose of Document

This Policy establishes the area within Brunel University London covering Backup and Restore.

Please refer to Brunel University London ISMS Document University-GLOS-000 - SyOPs Glossary of Terms for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

1.2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
Head of Infrastructure & Operations	Is responsible for ensuring that server and network backup and restore are in line with the security requirements of the ISMS.
Chief Information Security Officer	Is responsible for approving requests for backup data from 3rd parties.
Systems Manager	Responsible for ensuring that the IS staff execute the identified backups for central systems and devices as required and for identifying and reporting any faults, failures or error
Information / asset owners	Responsible for ensuring that the University's critical information is being backed up
Business Continuity Manager	Responsible for documenting, testing and maintaining the restoration process in line with business needs
Cyber & Information Security manager	Is responsible for ensuring Backup and Restore best practice and ensuring compliance with legislative and regulatory requirements. Owner of the policy.

1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A.12 – Operations Security
ISO 27001:2013 Conformance Control	Information backup A.12.3.1 Backup and recovery

1.4 Scope

All the University's information assets are subject to backup requirements. The service and hence this policy has been designed and implemented with disaster recovery/business continuity (i.e. the ability to recover recent live data in the event of a partial or total loss of data) as key deliverable and is not therefore designed as a method of archiving material for extended periods of time. The 'data' backups covers all systems managed by the IS department. Data held and managed locally in departments is excluded unless departments have entered into specific arrangements with IS. All staff are reminded that they are individually responsible for data held locally on their desktop or laptop computer and all critical data *must* be stored on the network drives provided or central email services.

1.5 References

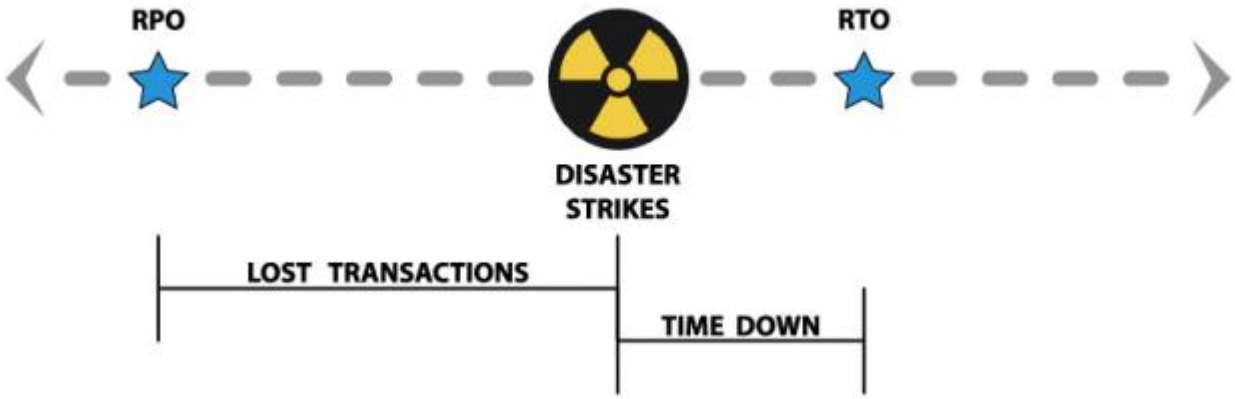
Good Practice Guide 13 - Protective Monitoring PMC8

1.6 Recovery Point Objective (RPO) and Recovery Time Objective (RTO)

Recovery Point Objective (RPO) and **Recovery Time Objective** (RTO) are one of the most important parameters of a disaster recovery or data protection plan and essential to understand and define the Backup policy. These objectives guide the University to choose the optimal data backup plan

Recovery Point Objective (RPO) refers to the point in time in the past to which you will recover;

Recovery Time Objective (RTO) refers to the point in time in the future at which you will be up and running again;



The RPO will be the point to which you will have all data up to that point recovered. The gap between the disaster and the RPO will likely be lost as a result of the disaster.
The backup frequency schedule will be dependent upon the acceptable RPO as this will be the point at which backups can be restored to.
On the timeline, RTO is the point in the future at which you will be back up and running full speed ahead. The gap between the disaster and the RTO is the timeframe for which your app will be down and non-functioning.
The accepted RTO determines the methodology of the backup schedule, whether incremental, full or differential.

2.0 Backup, Restore and Archiving Policy

2.1 Backup

2.1.1 All server hardware configurations, NAS and SANS must be configured using RAID technologies that offer protection from a single drive failure - RAID 10 (RAID 1+0) or RAID 1 or a RAID 6 configuration which persists when 2 disks fail simultaneously;

2.1.2 University backups are performed under a two tier infrastructure provision, Virtual infrastructure utilising VEEAM, (Virtual Workloads - VMware and Hyper-V along with supported physical server infrastructure) and BackupExpress for physical server infrastructure (comprising unsupported Oracle DB's);

2.1.3 University backups are defined within a three tier regime dependent upon the importance and classification of the data being backed up, the RPO and the RTO;

2.1.3.1 GOLD
2.1.3.2 SILVER
2.1.3.3 BRONZE

2.1.4 Not all systems or infrastructure are within the Backup schedules, systems excluded are:

- Non-production;
- Non-unique systems (where identical systems are in production and are backup up);

2.1.5 New requests for the backup of information and systems must be submitted to IS by email from the information asset owners or Systems team deploying the new infrastructure. The backup schedule can only be amended upon the advice provided by such requests. Ad-hoc requests for clone/backup can be accommodated by request;

2.1.6 The required level and frequency of backup for University data is:

2.1.6.1 GOLD;

1) Daily Forever Forward Incremental Backup to disk[1];

[1] Copies only VM data blocks that have changed since the last performed backup (full or incremental) and saves these blocks as an incremental backup file (VIB) in the backup chain.

2) Four-week Synthetic Full to tape[2];
3) Veeam Configuration Backup encrypted to disk[3];

2.1.6.2 SILVER;

4) No Daily;
5) Four-week cycle Daily Forever Forward Incremental Backup to disk [4];

2.1.6.3 BRONZE;

6) Ad-hoc Backup;
7) Client backups;

2.1.6.4 Any deviations from this are agreed by email with the information asset owners;

2.1.7 The IS Backup systems have been designed to ensure that routine backup operations require no manual intervention;

2.1.8 The IS department monitor backup operations and the status for backup jobs is checked on a daily basis during the working week;

2.1.9 Any failed backups are monitored by the Security Information and Event Management system and reported to IS to ensure re-run on the next scheduled working day;

2.1.10 The DOC 12.3.1 - PROC - Backup and Restore Procedure describes how Backup and Restore jobs are completed, how to execute the backup, what records should be made as evidence of successful backup, and what faults, failures or errors should be identified and how they should be reported;

2.1.11 Each device and recovery is tested as part of the Business Continuity Management framework;

2.1.12 Requests for backup data from 3rd parties must be approved by the CISO;

2.1.13 Where possible backups are run overnight and are completed before 8am on working days;

[2] Synthetic full backup is identical to a regular full backup – but does not use network resources: it is created from backup files already on disk.
[3] Configuration backups contain all the information about Veeam Backup & Replication, Backup Infrastructure components and objects.
[4] Forever Incremental accumulates irregular and infrequent file changes.

2.1.14 Backup data integrity is performed automatically by comparing the backup information with the source data (VEEAM only);

2.2 Storage Snap-Shots

2.2.1 On selected storage volumes, it is possible to provide additional backup in the form of Snap-shots[5]. This provides a quick RTO with a more recent RPO;

i) GOLD – Hourly Snap-Shot;

ii) SILVER - Daily Snap-Shot;

2.3 SITS Backup

2.3.1 The required level and frequency of backup for SITS data is one full backup per night and transaction log backups every 15 mins;

2.3.2 Backups for SITS are stored in University, all production University data is replicated to the second data centre in Slough;

2.4 Home Drive Backups

2.4.1 In addition to backup we now take shadow copies of home drive data twice a day. Files or directories can be restored from these copies by contacting Computing support. They will remotely access your PC to do this restore.

2.5 Retention

2.5.1 GOLD

i) Daily Forever Forward Incremental Backup are retained for 35 days before being merged with the full backup;
ii) Four-week cycle Full Backup are retained for 6 months before being overwritten;

2.5.2 SILVER

i) Four-week cycle Daily Forever Forward Incremental Backup are retained for a 5 week period before being overwritten;

2.5.3 BRONZE

i) Ad-hoc requests for retention;

[5] A snapshot uses a differencing disk -- a virtual hard disk (VHD) -- that stores changes made to another virtual disk or the guest operating system providing an accessible copy of data that can be used to roll back to.

2.5.4 Backup tapes backups are retained securely and then recycled to be overwritten;

2.5.5 Upon completion of backups, media copies (tape) are moved to a secure site on an alternative location on campus (fire-safe) for disaster recovery purposes;

2.5.6 Backups are stored in secure locations. A limited number of authorised personnel have access to the backup application and media copies;

2.6 Recovery and Restoring of Data Files

2.6.1 Data is available for restore within a few minutes of a backup job completing on the daily schedule;

2.6.2 Data will be available during the retention policy of each backup job – which is currently defined as a maximum of 6 months;

2.6.3 Recent data is available from this system on completion of the daily backup jobs, which means that there is potential data loss during a working day on some systems. The IS systems at University have been specified to minimise data loss between backup windows by having elements of system redundancy;

2.6.4 Requests for data recovery should be submitted to the IS Service desk;

2.6.5 Recovery can only be performed by authorised administrators;

2.6.6 The Recovery reason/purpose must be documented during the recovery process to ensure an auditable trial exists;

2.7 Backing up Data on Portable Computers

2.7.1 IS recommend that no critical University data is stored on portable devices;

2.8 Gap Analysis

2.8.1 IS to execute every six months a report on existing backup schedules and to provide an analysis of gaps within backup coverage and existing infrastructure/data;

2.9 Cloud

2.9.1 Cloud backup provision will be addressed during the third party Due Diligence. (Cloud Supplier Due Diligence Section 16)

2.9.2 The RPO and RTO will be reviewed and determined dependent upon the critical nature of the Cloud service and SLA's.

2.10 Archiving Electronic Files

2.10.1 Originating departments should retain all electronic records which they need for their own operational purposes for as long as they need them. Backups will be conducted as above in 2.1;

2.10.2 Records should only be transferred to the University Archive when they cease to be operationally relevant.

2.10.3 Records requiring specific retention for longer than the period detailed should contact IS for assistance;

Ref. University Archive Policy