Technology Solutions – Backup & Data Protection

Department: Technology Solutions
Procedure Name: Backup & Data Protection
Procedure ID: TS-PROC-017
Effective Date: 01/22/2026
Last Reviewed: 01/22/2026

Owner: Chief Information Officer (CIO)

Applies To: Technology Solutions staff responsible for systems, infrastructure, databases, and data protection

1. Purpose

This procedure defines how Technology Solutions protects institutional systems and data through consistent, automated backup and retention practices to ensure recoverability and operational continuity.

2. Scope

This procedure applies to all virtual servers, databases, file systems, identity services, applications, and institutional workloads, whether on-premises or cloud-based.

3. Guiding Principles

- Backups are mandatory for institutional systems
- Backup configuration must be automated and policy-driven
- Service Level Agreements define protection expectations
- Manual backup configuration is avoided where possible
- Verification and accountability are required

4. Backup Platforms & Architecture

Nutanix serves as the virtualization platform, and Rubrik is the enterprise backup and recovery solution. Backup onboarding is automated using Nutanix VM tags mapped directly to Rubrik SLA Domains.

5. Backup SLA Assignment (Mandatory)

5.1 Nutanix Tagging Requirement

All servers must be assigned a Nutanix tag that determines the appropriate Rubrik SLA. Untagged servers are considered non-compliant. Manual Rubrik SLA assignment is prohibited unless approved by the CIO.

6. Backup Service Level Agreements (SLAs)

SLA Name	Base Frequency	Secondary	Tertiary	Total Retention	Backup Retention	Archive Retention
Academic Servers	7 days	N/A	N/A	2 weeks	N/A	N/A
Administrative Servers	7 days	N/A	N/A	2 weeks	N/A	N/A
Banner – NonProduction	1 day	N/A	N/A	15 days	N/A	N/A
Banner – Production	1 day	N/A	N/A	61 days	30 days	31 days
Entra ID Daily	1 day	N/A	N/A	46 days	N/A	N/A
File Servers	4 hours	N/A	N/A	30 days	N/A	N/A
General – Daily	1 day	N/A	N/A	46 days	15 days	31 days
Marketing	1 day	N/A	N/A	30 days	N/A	N/A
Networking Services	1 week	N/A	N/A	8 weeks	N/A	N/A
Oracle Databases	4 hr/7d	1 day/14d	1 month/8m	243 days	30 days	213 days
Relic Objects – 30 Days	1 day	N/A	N/A	46 days	1 day	45 days
Relic Objects – 60 Days	1 day	N/A	N/A	62 days	1 day	61 days
SQL Databases	1 day	N/A	N/A	46 days	N/A	N/A
Virtual Desktops	1 week	N/A	N/A	4 weeks	N/A	N/A

7. Backup Verification & Monitoring

Backup jobs are monitored routinely. Failures must be investigated and remediated promptly. Periodic restore testing may be conducted to validate recoverability.

8. Restore Requests

Restore requests must be authorized by the system owner or leadership. Restores impacting production or sensitive systems may require change approval.

9. Exclusions & Exceptions

Systems excluded from backups require CIO approval and must be documented, time-bound, and reviewed periodically.

10. Incident Alignment

Backup failures impacting recoverability are treated as incidents and follow TS-PROC-007. Data loss events follow TS-PROC-013.

11. Compliance & Enforcement

Failure to comply with this procedure may result in increased risk, audit findings, or corrective action. This procedure is governed under TS-PROC-001.

12. Review Cycle

This procedure will be reviewed annually or as backup architecture or institutional requirements change.