

Backup Policy

Purpose

A backup that has never been restored is a hypothesis, not a recovery capability. This policy defines how Your Organization backs up critical data and systems, and — because the existence of a backup proves nothing on its own — how backup integrity and restorability are actually verified.

Scope

This policy applies to every system and data store holding Your Organization production data or Controlled Unclassified Information (CUI), and to the engineering and platform teams responsible for configuring, monitoring, and restoring backups.

The 3-2-1 rule

Critical data is backed up following the 3-2-1 rule as a baseline: at least **3** copies of the data, on at least **2** different storage media or platforms, with at least **1** copy stored off-site or in a separate cloud region/account from the production system. A system owner may exceed this baseline for a Tier 1 system; nothing may fall below it.

Backup frequency

Backup frequency is set to meet the RPO committed for the system's tier in the recovery register — a backup schedule that cannot meet its system's RPO is a policy exception, not a rounding error, and requires the same documented approval any other exception does.

Immutability

Backups of Tier 1 and Tier 2 systems are written to storage configured with immutability (write-once, object-lock, or an equivalent control) for a retention window covering at least the backup retention period below. Immutability exists specifically to defeat a ransomware or insider scenario in which an attacker with valid credentials attempts to delete or encrypt backup copies alongside production data — a mutable backup reachable by the same credentials that were compromised is not a control.

Access and encryption

- Backups are encrypted at rest and in transit.
- Access to backup storage and to backup management consoles is restricted to named roles and reviewed on the same cadence as other privileged access (Access Control Policy).
- Backup encryption keys are managed and rotated per the Access Control and system/communications protection standards; a key with the same blast radius as the production system it protects is a finding.

Restore testing

Backup integrity is verified through restoration tests, not by confirming a backup job reported success — a completed job proves the write happened, not that the data is usable. Restore tests are performed:

- At least quarterly for a sample of Tier 1 and Tier 2 systems, on a rotating basis so every such system is tested at least annually.
- Whenever a system's backup configuration changes materially.
- As part of every scheduled Disaster Recovery Plan test, which exercises the full restore-and-validate path rather than a backup-only spot check.

A failed or partial restore test opens a remediation item owned by the system owner, tracked the same way a failed DR test is.

Retention

- Production system backups are retained for a minimum of 30 days of daily backups, 12 months of monthly backups, and per the Data Retention and Disposal Policy's schedule thereafter for any backup subject to a longer legal, contractual, or regulatory retention requirement.
- Backups containing CUI or other regulated data are retained and disposed of per the same schedule and sanitization standard as the source data (Data Retention and Disposal Policy, Media Protection Policy).
- A backup is deleted only through the documented retention process — never as an ad hoc storage-cleanup action.

Review cadence

This policy is reviewed annually by the BCM Lead and system owners, or sooner following a failed restore test, a real recovery event, or a material change to backup architecture.

Effective date: [the date this policy takes effect]