**Backup Retention Policy Template***By Brien Posey*

<Company Name>

*Use this template as a framework for creating a data backup policy. For more information, read the accompanying guide about* [*backup retention policies*](https://www.techtarget.com/searchdatabackup/answer/What-are-some-data-retention-policy-best-practices)*.*

***Revisions control page***

|  |  |  |
| --- | --- | --- |
| **Date** | **Summary of changes made** | **Changes made by (Name)** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

***Table of Contents***

* Purpose
* Scope
* Roles and Responsibilities
* Backup Frequency and Retention Period
* Security and Access Controls
* Backup Testing
* Backup Lifecycle Management
* Compliance and Auditing
* Policy Review and Updating

***Purpose***

This policy establishes the requirements for the retention and deletion of backups in accordance with regulatory and business requirements.

<*Augment or modify this statement in accordance with your organization's needs*.>

***Scope***

This backup retention policy applies to all IT systems created or maintained by the organization's IT department. This includes systems owned by the organization, as well as cloud-based systems. It applies to unstructured (file) data, structured data (databases), physical and VMs, email and messaging systems, network endpoints, applications, and system configurations.

<*Augment or modify this statement in accordance with your organization's needs.>*

***Roles and Responsibilities***

|  |  |
| --- | --- |
| **Roles** | **Responsibilities** |
| IT Department | Create, implement, and enforce backup policies and monitor compliance. |
| Stakeholders  | Identify data and its location and approve backup and retention schedules. |
| Compliance Officer | Ensure that all regulatory, legal, and business requirements are adhered to. |
| Security Team | Implement security mechanisms and access controls to protect backups against unauthorized access or data leakage. |
|  |  |
|  |  |
|  |  |

*<Add any additional roles or responsibilities as they relate to specific teams or individual staff members>*

***Backup Frequency and Retention Period***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dataset** | **Owner** | **Retention period**  | **Backup frequency** | **Backup target location** | **Secondary backup tiers used** | **Additional safeguards** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

***Security and Access Controls***

**Encryption:** *<Insert requirements for data encryption.>*

**Access Controls:** Backup data must be accessible only by authorized individuals. *<Insert statements regarding who is authorized to access the data.>*

**Immutable Storage**: *<Insert the organization’s policies regarding immutable storage.>*

**Multi-Site Storage:** *<Insert the organization’s policy regarding geographically separated, redundant backup storage.>*

**Ransomware Protection:** *<Insert a statement about the safeguards that will be put in place to protect backups from ransomware.>*

**Air Gapped Backups:** <*Insert a statement governing the use of removable media.>*

***Backup Testing***

*<Insert a statement regarding the frequency with which backups should be tested and how those tests should be performed.>*

*<Insert a statement regarding who is responsible for performing these tests.>*

*<Insert a statement indicating what should happen if a backup recovery test fails.>*

***Backup Lifecycle Management***

Backup lifecycle management will be automated to adhere to the organization's data retention policies. Data subject to eDiscovery and litigation hold will be exempted from automated lifecycle management.

*<Describe the mechanism used to make sure that data is retained for the required period of time.>*

*<Describe the mechanism that will be used to purge expired backups.>*

*<Explain how litigation hold can be applied to a dataset and how you will prevent affected backups from being purged when they expire.>*

*<Describe how you will test and validate your automated backup lifecycle management.>*

***Compliance and Auditing***

*<Describe your procedure for logging and reviewing any activities related to backing up or restoring data.>*

*<Describe the frequency with which the organization will conduct internal backup compliance audits and what those audits entail.>*

*<Describe the reporting procedures for any non-compliance incidents discovered, as well as any applicable corrective or disciplinary actions.>*

***Policy Review and Updating***

This policy will be reviewed <*review frequency*> or as required by evolving business or regulatory requirements or in response to technological changes. <Reviewer/team> must review and approve all updates.