# Server Backup Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

|  |  |
| --- | --- |
| **Policy Owner** | Name the person/group responsible for this policy’s management. |
| **Policy Approver(s)** | Name the person/group responsible for implementation approval of this policy. |
| **Related Policies** | Name other related enterprise policies both within or external to this manual. |
| **Related Procedures** | Name other related enterprise procedures both within or external to this manual. |
| **Storage Location** | Describe physical or digital location of copies of this policy. |
| **Effective Date** | List the date that this policy went into effect. |
| **Next Review Date** | List the date that this policy must undergo review and update. |

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

Data is one of [Company Name]’s most important assets. In order to protect this asset from loss or destruction, it is imperative that it be safely and securely captured, copied, and stored. The goal of this document is to outline a policy that governs how and when data residing on company servers will be backed up and stored for the purpose of providing restoration capability. In addition, it will address methods for requesting that backed up data be restored to individual systems.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

This policy refers to the backing up of data that resides on [Company Name]’s servers. Servers and the files and/or data types on these servers that are covered by this policy include:

* [insert server name/description]
  + [insert file name/data type]
  + [insert file name/data type]
* [insert server name/description]
  + [insert file name/data type]
  + [insert file name/data type]
* [insert server name/description]
  + [insert file name/data type]
  + [insert file name/data type]

This policy does not refer to backing up of data that resides on individual PC or notebook hard drives. Responsibility for backing up data on local desktop systems or laptops rests solely with the individual user. It is strongly encouraged that end users save their data to the appropriate server listed above in order for their data to be backed up regularly in accordance with this policy.

In addition, files that are left open at the time the backup procedure is initiated may not be backed up. End users are reminded to save and close all files, as well as all related applications, prior to the backup procedure window.

It is the responsibility of server administrators to ensure that all new servers be added to this policy, and that this policy be applied to each new server’s maintenance routine. Prior to deploying a new server, a full backup must be performed and the ability to perform a full restoration from that backup confirmed. Prior to retiring a server, a full backup must be performed and placed in permanent storage.

# Definitions

Define any key terms, acronyms, or concepts that will be used in the policy. A standard glossary approach is sufficient.

# Governing Laws & Regulations

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

Backups are conducted [manually/automatically]. [Insert a description of any technologies or tools used to conduct backups that are specific to your organization.]

The servers listed above must be backed up according to the following procedure. This method ensures that no more than one day’s working data will be missing in the event of a data loss incident:

1. All backup tapes are to be labeled using the following labeling conventions:

[describe labeling convention here].

1. All backup tapes stored on site are to be stored [identify location and associated procedures].
2. All backup tapes stored off site are to be stored [identify location and associated procedures, including who is responsible for ensuring transport and by what means].
3. All backups will take place between the hours of [insert time range]. This timeframe has been selected to minimize the impact of server downtime on end users that may be caused by the need to take servers offline in order to perform the backup itself. If this backup schedule in some way interferes with a critical work process, then the affected user(s) is to notify the IT Department so that exceptions or alternative arrangements can be made.
4. Incremental backups (only files changed since the last backup) will be performed daily, Monday through Thursday. [Expand this to Saturday if your business operates on weekends.] These tapes will be stored onsite during the following backup cycle. At the end of the latter cycle, the daily tapes will be removed to a predetermined offsite location for storage for [insert number] weeks. When this [insert number] week period has elapsed, the tapes will be brought back on site for reuse for a period not to exceed one year.
5. A full backup will be performed each Friday. [Move to Sunday if your business operates on the weekend.] This tape will be stored on site during the following backup cycle. At the end of the latter cycle, the weekly tape will be removed to a predetermined offsite location for storage for [insert number] weeks. When this [insert number] week period has elapsed, the tapes will be brought back on site for reuse for a period not to exceed one year.
6. A full backup will be performed at the end of each month. This tape will be immediately removed to a predetermined offsite location for permanent storage. These tapes will never be reused.
7. All server backups performed must be noted in the server backup log immediately upon completion. All server backup log sheets must be kept in an appropriately labeled three-ring binder in an agreed-upon, centralized location. The log must include:

Server name,

Date and time of backup,

Name of administrator performing the backup,

Files backed up and/or skipped,

Software used to perform the backup,

Backup medium used and its label/name, and

Whether the backup was successful or not.

1. If, for some reason, the backup cannot be completed, is missed, or crashes, then it must be completed by 9:00 a.m. the following morning. The reason for non-completion of the originally scheduled backup must be noted in the server backup log. In addition, if a backup fails more than one day in a row, end users in the organization must be notified.
2. If a tape is discovered to be damaged or corrupt, then the tape must be destroyed to prevent further use and replaced with a new one.

**Relevant Procedures**

Consider creating formal procedure documents that reinforce and support the policy statements above. Note, it is best practice to house policies and procedures in separate documents to keep the content focused and reduce the number of times the policy must be reapproved by senior management.

The ultimate goal of any backup process is to ensure that a restorable copy of data exists. If the data cannot be restored, then the process is useless. As a result, it’s essential to regularly test one’s ability to restore data from its storage media.

1. All daily tapes must be tested at least once every [insert number] months to ensure that the data they contain can be completely restored.
2. All weekly tapes must be tested at least once every [insert number] months to ensure that the data they contain can be completely restored.
3. All monthly tapes must be tested at least once every [insert number] years to ensure that the data they contain can be completely restored.

Data will be restored from a backup if:

There is an intrusion or attack.

Files have been corrupted, deleted, or modified.

Information must be accessed that is located on an archived backup.

[Add other conditions under which data will be restored.]

In the event a data restore is desired or required, the following policy will be adhered to:

1. The individual responsible for overseeing backup and restore procedures is [insert name here]. If a user has a restore request, they can contact [insert name here] by calling [phone number], sending an email to [email address], or filling out and submitting a request form located at [URL or shared drive location].
2. In the event of unplanned downtime, attack, or disaster, consult [Company Name]’s Disaster Recovery Plan for full restoration procedures.
3. In the event of a local data loss due to human error, the end user affected must contact the IT Department and request a data restore. The end user must provide the following information:

Name.

Contact information.

Name of file(s) and/or folder(s) affected.

Last known location of files(s) and/or folder(s) affected.

Extent and nature of data loss.

Events leading to data loss, including last modified date and time (if known).

Urgency of restore.

1. Depending on the extent of data loss, a daily tape, weekly tape, or combination of both will need to be used. The timing in the cycle will dictate whether or not these tapes are onsite or offsite. Tapes must be retrieved by the server administrator or pre-determined replacement. If tapes are offsite and the restore is not urgent, then the end user affected may be required to wait up to [insert time frame] for a time- and cost-effective opportunity for the tape(s) to be retrieved.
2. If the data loss was due to user error or a lack of adherence to procedure, then the end user responsible may be required to participate in a tutorial on effective data backup practices.

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.

# Agreement

Include a section that confirms understanding and agreement to comply with the policy. Both signatures and dates are required. A sample statement is provided below.

I have read and understand the [name of policy]. I understand that if I violate the rules explained herein, I may face legal or disciplinary action according to applicable laws or company policy.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Signature Date

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

For acceptable use of this template, refer to Info-Tech's [Terms of Use](http://www.infotech.com/terms). These documents are intended to supply general information only, not specific professional or personal advice, and are not intended to be used as a substitute for any kind of professional advice. Use this document either in whole or in part as a basis and guide for document creation. To customize this document with corporate marks and titles, simply replace the Info-Tech information in the Header and Footer fields of this document.