**SAMPLE TEMPLATE**

**Data Backup and Recovery Policy**

Last Update Status: *December 2020*

1. **Overview**

In accordance with mandated organizational security requirements set forth and approved by management, <Company Name> has established a formal Data Backup and Recovery policy and supporting

procedures. This policy is to be implemented immediately, along with all relevant and applicable

procedures. Additionally, this policy is to be evaluated on a(n) [*annual, semi-annual, or quarterly*] basis for

ensuring its adequacy and relevancy regarding <Company Name> 's needs and goals.

1. **Purpose**

This policy and supporting procedures are designed to provide <Company Name> with a documented and formalized Data Backup and Recovery Policy that is to be adhered to and utilized throughout the organization at all times. The purpose of the policy is to safeguard the <Company Name>’s information assets, prevent loss of data due to accidental deletion or corruption, and facilitate the timely restoration of information and business processes should a system failure occur.

Business Information and services are a vital part of any organization and should be protected. Creating backups is a critical process for any organization, especially considering today’s growing regulatory compliance

mandates and the ever-increasing cybersecurity threats that businesses face on a daily basis. A well-thought-out, efficient, and reliable backup and recovery is vital to ensuring the confidentiality, integrity, and availability (CIA) of critical data. Simply saving information is not enough; performing backups of all information within <Company Name> will help prevent business downtime and/or loss of data and services. Failure due to computer malfunction, human error, and natural disasters could cause interruptions that are unrecoverable without adequate backups.

1. **Scope**

This policy applies to the use of information, electronic and computing devices, and network resources to conduct <Company Name>’s business or interact with internal networks and business systems, whether owned or leased by <Company Name> employees, or a third party. All employees, contractors, consultants, temporary, and other workers at <Company Name> and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with <Company Name> policies and standards, and local laws and regulation.

This policy and supporting procedures encompass all system resources and supporting assets that are

owned, operated, maintained, and controlled by <Company Name> and all other system resources, both internally and externally, that interact with these systems.

* **Internal system resources** are those owned, operated, maintained, and controlled by <Company Name> and include all network devices (firewalls, routers, switches, load balancers, other network devices), servers (and the operating systems and applications that reside on them, both physical and virtual servers) and any other system resources and supporting assets deemed in scope.

* **External system resources** are those owned, operated, maintained, and controlled by any entity

other than <Company Name> but for which these very resources may impact the confidentiality, integrity, and availability (CIA) of <Company Name>’s system resources and supporting assets.

1. **Policy**

<Company Name> is to ensure that the Data Backup and Recovery Policy adheres to the following conditions for purposes of complying with the mandated organizational security requirements set forth

and approved by management:

### Backup environments

A critical component of any data backup and recovery initiative is to properly identify all environments –

and the associated data – that require backup procedures. While critical environments, such as those

relating to production, development, and staging, require backups, it’s the platforms and the supporting

systems within these environments that are to be identified, with applicable backup procedures in place.

This would include, but are not limited to, the following platforms and supporting systems:

**Network device backups, such as configuration file, rulesets, and other critical data**

* Servers (both virtual and physical stand-alone), all operating systems, and associated applications (i.e., databases, web server applications, etc.) for all Microsoft Windows, UNIX, Linux, and any other type of other operating systems.
* Critical servers, such as all production facing servers, DNS servers, email servers, FTP servers, and all other systems associated with such servers.
* Voicemail, PBX, and Telephone Systems.

**Backup Utilities and Supporting Tools**

All backup processes undertaken by <Company Name> are to utilize approved hardware, software, and other supporting tools for ensuring the confidentiality, integrity, and availability (CIA) of the entire backup platform.

Backup utilities are to consist of, but are not limited to, the following:

* Backup software
* Backup tapes and tape devices
* Backup library
* Backup disks
* Hard drives
* CDs
* DVDs
* Compact flash drives, SD
* Dynamic Random-Access Memory (DRAM)
* Read-Only Memory (ROM and the different variations thereof)
* Random Access Memory (RAM)
* USB Flash Cards
* USB drives, removable media, memory sticks

**Types of Backups and Default Backup Scheduling**

It is critically important to design and deploy a backup process that is comprehensive, efficient, and

includes backups on a regular basis for ultimately ensuring the confidentiality, integrity, and availability

(CIA) of organizational data.

The following types of backups are to be utilized for <Company Name>’s backups:

* **Full** – A full backup is simply a complete backup of all data. It is the most comprehensive and time-consuming type of backup, yet it ensures a complete backup of everything has been undertaken.
* **Differential** - A differential backup provides a backup of files that have effectively changed since the last full backup was performed. A differential backup typically saves only the files that are different or new since the actual last full backup, but this can vary in different backup platforms.
* **Incremental** – An incremental backup is essentially a backup of all the files, or parts of files that have changed since the previous backup was conducted, regardless of the type of backup (full, differential, or incremental).

*Additionally, backup activities for full, differential, and incremental are to take place in the following manner:*

**Full = At a minimum, once a week.**

**Differential = At a minimum, daily.**

**Incremental = As necessary.**

**Backup Reporting Metrics**

Backup reporting activities, for all types of backups (i.e., full, differential, incremental, etc.) are to be monitored on a regular basis for ensuring the success of the backup process itself. Specifically, all

backups conducted are to generate reporting metrics for which authorized personnel are to review in a

timely manner.

Such reporting metrics include, but are not limited to, the following:

* Emails confirming the current status and result– such as success or failure – of the backup.
* Reports generated confirming the current status and final result – such as success or failure – of the backup.
* Portals for which authorized employees can log into for reviewing and confirming the up-to-date status and final result – such as success or failure – of the backup.
* Backups that are successful are to be recorded as such and backup failures and exceptions are to be handled immediately, with all appropriate steps undertaken for ensuring the timely backup of such data.
* Failures and exceptions are delivered via email reports or metrics from the backup utilities notifying authorized employees of such issues. Depending on the nature, severity, and urgency of the backup itself and the resolution for correcting the issue, a thorough analysis is to be undertaken for correcting the issue in a timely manner and for helping mitigate the issue in the future.

**Backup Storage and Security**

Appropriate Security Measures are to be implemented for backups, which includes all necessary physical security controls, such as those related to the safety and security of the actual backup media – specifically – disks, tapes, and any other medium containing backup data. This requires the use of a computer room or other designated area (facility) that is always secured and monitored and whereby only authorized personnel have physical access to the backups.

Thus, "secured" and "monitored" implies the facility has the following physical and environmental security controls in place:

* Constructed in a manner allowing for adequate protection of backups.
* Security alarms that are active during non-business hours, with alarm notifications directly answered by a third-party security service or local police force.
* The use of cages, cabinets, or other designated, secured areas for securing backups.
* Access control mechanisms consisting of traditional lock and key, and/or electronic access control systems (ACS), such as badge readers and biometric recognition (i.e., iris, palm, fingerprint scanners or readers).
* All electronic access control mechanisms are to record all activity and produce log reports that are retained for a minimum of [x] days.
* Adequate closed-circuit monitoring, video surveillance as needed, both internally and externally, with all video recordings kept for a minimum of [x] days for purposes of meeting security best practices and various regulatory requirements.
* Appropriate fire detection and suppression elements, along with fire extinguishers placed in mission-critical areas.
* Appropriate power protection devices for ensuring a continued, balanced load of power to the facility for where the backups reside.

**Media Management and Quality Control**

All backup media is to be clearly labeled, logged accordingly, and rotated as necessary for ensuring all retention periods are adhered to, while also utilizing existing mediums (i.e., tapes, disks, etc.) for writing over and copying as necessary for future backups.

Additionally, media management practices for backups also required that strict policies be in place for transporting media to and from the off-site approved facility being used by <Company Name>. As such, an authorized list is to be kept that includes only select personnel allowed to transport and recall media, with no exceptions.

The following information regarding backups must be recorded, either in manual or electronic format:

* Name and unique identifying number of backup medium
* Contents of the backup
* Data classification of backup
* Location of where it is being stored
* Origination of backup – where the medium initially came from

As for quality control initiatives, backups are to be used until they reach a point far before in which the

quality of the data may come into question, ultimately to avoid media failures. At any time if the quality

of media becomes an issue, the data is to be immediately removed to another medium, with the

compromised medium being disposed in accordance with company policy.

**Transporting of Media**

Transporting backup media is vital for always ensuring its safety and security when in transit or at rest. The

following best practices are to be always adhered to, when applicable:

* Backup media is to be properly packed and stored for ensuring its safety during movement, which means using approved cases and other protective devices.
* Backup media is to be kept away from extreme temperatures, both heat and cold, during movement.
* Backup media is never to be left alone or unsupervised during transportation.
* Only approved transport methods and vehicles are to be utilized.
* Transport is to be in a direct manner as possible, with no unnecessary stops or deviations from the intended route.
* When necessary, transport of media is to also include additional security precautions as required.

*If backups are being transported, the following is to be recorded:*

* Purpose
* Name of individual requesting backup
* Intended destination
* Date of release
* Date of return
* Any other information deemed relevant

**Backup Requests and Retrieval**

Backups are to be available in a timely manner for any such requests for restoration. Such requests require written approval by authorized personal detailing the request, along with all applicable

information as necessary. A change request is to be opened for such requests, and approved by authorized

personnel.

As for the restoration process, it is to be conducted by authorized personnel who will test for

ensuring a complete restoration was achieved, along with conducing any user-acceptance and system testing.

*\*\*The restored media is to be promptly returned to the physically secured area for safe storage.*

**Backup Retention Periods and Disposal Procedures**

Backup retention periods – regarding backups - are those specifically identified for purposes of restore

and recovery of <Company Name>’s data. Thus, it is the responsibility of authorized personnel to ensure the applicable backup retention periods meet all necessary needs of the organization, while also promoting best practices.

Conversely, retention periods, such as those defined by contractual, legal, and regulatory compliance mandates, are specifically detailed within the <Company Name> Data Retention and Disposal

Policy, which outlines policies and procedures regarding data retention length and disposal of the actual

data itself.

Additionally, please note that when referring to disposal procedures in the context of backups, this

specifically applies to the physical devices used for storing such data, and not the actual data itself.

Policies regarding disposal of data – the actual information – are also outlined in the <Company Name>

Data Retention and Disposal Policy.

Acceptable and approved methods of disposal for the actual physical devices used for storing are:

* Disintegration
* Shredding (disk grinding device)
* Incineration by a licensed incinerator
* Pulverization

*Please note that prior to physically destroying any of the actual devices used for storing data, all data must*

*be electronically removed (i.e., wiped, formatted, etc.) as the primary layer of security before being destroyed.*

**Business Continuity and Disaster Recovery Planning (BCDR)**

Documented Business Continuity and Disaster Recovery Planning (BCDRP) is vital to protecting all

<Company Name> assets along with ensuring rapid resumption of critical services in a timely manner.

Because disasters and business interruptions are extremely difficult to predict, it is the responsibility of

authorized <Company Name> personnel to have in place a fully functioning BCDRP process, and one that

also includes specific policies, procedures, and supporting initiatives relating to the safety and security of

backups, and supporting systems for which to restore backup data on.

**Continuous Monitoring of Backup Environment**

It’s also vitally important to undertake continuous monitoring practices over the entire backup

environment for ensuring its confidentiality, integrity, and availability (CIA).

Authorized personnel are to ensure the following:

* All applicable environments requiring backups have been readily identified.
* The backup types (full, differential, and incremental) along with the default backups scheduling, is commensurate with the needs of [company name].
* Backup results are being sent to, reviewed, and assessed by authorized personnel.
* All backup infrastructure – both hardware and software – related are performing and functioning as expected, with no exceptions or deviations regarding performance, accuracy, and other critical measures deemed relevant.

*Infrastructure, includes, but is not limited to, the following:*

* Backup software
* Backup hardware
* Tapes
* Tape and library drives
* Other storage and connectivity apparatus
1. **Policy Compliance**

**Compliance Measurement and Validation:**

On a regular basis, [*quarterly, and no less than twice a year*]*,* authorized personnel are to examine, and report on the ability to effectively restore and recover data in the event of such a request. This requires examining the facility for which data is being stored for ensuring its overall safety and security.

Furthermore, all backup mediums, such as tapes, disks, and other supporting hardware and software utilities are to be examined for ensuring proper function. Such information and all relevant findings are

to be reported upstream to management, with recommendations for improving upon or correcting any issues or concerns.

**Exceptions**

Any exceptions to the types of backups and the default backup scheduling are to be approved by

authorized personnel, with a valid and justified reason. Additionally, such exceptions – which are

ultimately changes to the backup process – are to be submitted with a formal change request, reviewed

and approved by authorized personnel.

Furthermore, changes to any of the tools and utilities used for the backup process also requires the use of a documented change request, initiated by select personnel only. The backup platform is a critical component of the organization’s information technology infrastructure, thus great care and due diligence must be enacted when involving changes to its process.

**Non-Compliance**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

1. **Definitions and Terms**

**Backup -**The procedure for making extra copies of information stored on servers and computers in case the original is lost or damaged.

**Restore -**The process of returning to the former condition using a backup.

**System Owners -**Manager or departmental head responsible for operation and maintenance of a University IT system or overseeing hosted systems under their purview.

**National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)** - provides a policy framework of computer security guidance for how private sector organizations in the United States can access and improve their ability to prevent, detect and respond to cyber-attacks.

**International Organization for Standardization (ISO) 27000** - part of the system for worldwide standardization

1. **Related Standards, Policies and Processes**

ISO/IEC 27001 2013 (More information available upon request)

6.2.1 Mobile device policy (ISO Policy 030602)

8.2.3 Handling of assets (ISO Policy 030606)

12.3.1 Information backup (ISO Policy 030601, 030603-030306)

NIST 800-53: [More information here](https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf)

CP-6 Alternative Storage Site

CP-9 Information System Backup

CP-10 Information System Recovery and Reconstitution

1NIST 800-53: CP-6, CP-9, CP-10

2ISO 27000: 12.3.1

3ISO 27000: 6.2.1

4ISO 27000: 8.2.3

1. **Revision History**

|  |  |  |
| --- | --- | --- |
| Date of Change | Responsible | Summary of Change |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |