DATA BACKUP and RECOVERY

General Overview

One of the most critical functions any I.T. organization can undertake is ensuring a structured and highly formalized data backup policy and procedures are in place. After all, an organization without its data – or the inability to retrieve and restore such data in a complete, accurate, and timely manner – faces serious issues as a viable entity. Backups are a must, especially considering today's growing regulatory compliance mandates and the ever-increasing cyber security threats for which business face on a daily basis. Yet even without compliance mandates, a well-though out, efficient, and reliable backup and recovery plan is a must for ensuring the confidentiality, integrity, and availability of (CIA) critical data.

As for data backups or the process of "backing up", it's essentially the copying, storing – and possible restore and recovery – of computer data. Simply stated, data, in whatever format it may be in, should be regularly copied, then stored and archived accordingly, and available for possible restore and recovery, if necessary. Sounds straightforward – and it is – yet organizations struggle immensely with putting in place best practices such as these for backups.

Data Backup and Recovery Policy and Procedures

Title	**[company name] Data Backup and Recovery Policy and Procedures**
Version	Version 1.0
Date	TBD
Language	English
Individual and/or Department Responsible for Distribution of Document	[company name] Information Technology Department
Individual and/ or Department Responsible for Timely Update of Document	[name and title]
Developed by:	[company name]
Subject	Data Backup and Recovery
Approval Date	TBD
Purpose of Document	To implement comprehensive data backup and recovery policies, procedures, and practices whereby all employees and other intended parties are readily aware of the organization's data backup initiatives.
Distribution of Document	Disbursed to all employees of [company name] and available by request to all other intended parties.

1.0 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, quarterly] basis for ensuring its adequacy and relevancy regarding [company name]'s needs and goals.

1.0 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. Compliance with the stated policy and supporting procedures helps ensure the safety and security of [company name] I.T. system resources and all supporting assets. Backups are a critical process for any organization, especially considering today's growing regulatory compliance mandates and the ever-increasing cyber security threats for which business face on a daily basis. Yet even without compliance mandates, a well-though out, efficient, and reliable backup and recovery is a must for ensuring the confidentiality, integrity, and availability (CIA) of critical data.

1.0 Scope

This policy and supporting procedures encompasses 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] system resources and supporting assets.

1.0 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 initiatives is to properly identify all environments – and the associated data – that required 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 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) such as 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, 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)
- Flash cards
- USB drives, removable media, memory sticks

As for the backup processes performed, the following are considered acceptable by [company name] when conducting backups of all necessary data:

- **Manual** – Manual backups are those performed by choosing what data to back up, when to backup, and to what device – all in a manual process. Though it creates great flexibility and customization, it's not recommended as a viable long-term solution for any type of environment.

- **Semi-Automated** – Semi automated backups are those performed using backup tools and software, but still require somebody to initiate and launch the backup process itself. The disadvantage of these backups is that there prone to human error, such as missing a critical time for backups, etc.

- **Completely Automated** – Completely automated backup processes have fast become the norm in many environments, as they effectively ensure the backup process is run on a regular scheduled time, complete with reporting metrics and other critical information.

Types of Backups and Default Backup Scheduling

It's critically important to design and deploy a backup process that's 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 backup process:

- **Full** – A full backup is simply a complete backup of all data. It's the most comprehensive and time-consuming type of data, yet it ensure 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 backups was conducted, regardless of the type of backup (Full, differential, or incremental).

Additionally, backup activities for full, differential, and incremental are to take place on an as-needed basis, such as in the following manner:

- Full: At a minimum, once a week.
- Differential: At a minimum, daily.
- Incremental: As necessary.

Backup 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 require 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.

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:

- E-mails confirming the current status and final 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 current status and final result – such as success or failure – of the backup.

Backups that are successful are to be recorded as such, yet backup failures an 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 and 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 secured and monitored at all times and whereby only authorized personnel have physical access to the backups. Thus, "secured" and "monitored" implies that the facility has in place the following physical security and environmental security controls:

- 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/readers). Furthermore, 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 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.

Either in manual form or electronic format, the following information is to be recorded regarding backups:

- 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.

- 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

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 ensuring its safety and security at all times during movement. The following best practices are to be adhered to at all times, 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.

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 authored personnel. As for the restore 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. Lastly, the restore 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] 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. Thus, for purposes of disposal for the actual physical devices used for storing such data, they consist of the following:

- 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.

Backup Recovery Abilities

On a regular basis, such as 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 required 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.

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). As such, 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 function 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

1.0 Procedures

[Company name] has developed and implemented a comprehensive data backup and recovery process, which encompasses the following categories and supporting activities listed below. These policy directives will be fully enforced by [company name] for ensuring the data backup and recovery initiatives are executed in a formal manner and on a consistent basis for all specified systems.

Note: The "Policy" sections contained within this specific policy and procedure document simply state general best-of-breed practices that should be in place. However, the "Procedures" sections list and describes the actual steps to undertake for ensuring compliance with the aforementioned policies. As such, look upon the policies as statements, formal guidelines, and the general framework for a particular subject matter. As for the procedures, these are the actual processes, steps, workflow activities and supporting initiatives that illustrate how the actual policies are implemented. In summary, policies state what are to be done, while procedures show you how they are done.

Additionally, if you want to provide any more information that's relevant to each section listed below, please use the "Additional Information" box [shown under each section], as this allows you to document any additional evidence of the procedures undertaken for meeting adherence with the stated policies. All information in light blue text should be deleted as this information is merely stated for reference purposes.

Backup Environments

[Note: The "Policy" section within this document simply states general best-of-breed practices that should be in place regarding backup environments. Thus, please use the "Procedures" section to actually describe various specifics pertaining to backup environments, such as what specific environments are being backed up and included within the scope of this document.

Additional Information
General Notes | Comments:

Backup Utilities and Supporting Tools

[Note: The "Policy" section within this document simply states general best-of-breed practices that should be in place regarding backup utilities and supporting tools. Thus, please use the "Procedures" section to actually describe various specifics pertaining to backup utilities and supporting tools, such as what specific software and agents are used, tape libraries, and other supporting software and hardware apparatus.

Additional Information
General Notes | Comments:

Types of Backups and Default Scheduling

[Note: The "Policy" section within this document simply states general best-of-breed practices that should be in place regarding types of backups and default scheduling. Thus, please use the "Procedures" section to actually describe various specifics pertaining to the types of backups and the default scheduling, such as Full, Differential, and Incremental backups, daily, weekly, hourly, etc.

Additional Information
General Notes | Comments:

Backup Exceptions

[Note: The "Policy" section within this document simply states general best-of-breed practices that should be in place regarding backup exceptions. Thus, please use the "Procedures" section to actually describe various specifics pertaining to backup exceptions, such as what procedures are enacted, by whom, etc.

Additional Information
General Notes | Comments: