DATA BACKUP POLICY

DOCUMENT CONTROL PAGE

Document ID	SCG/DABP/024/1.0
Security Classification	Confidential
Date Issued	30-Jul-2025
Version	1.0
Project Name	NA
Author	AJ KHAN

VERSION HISTORY / CHANGE HISTORY

Version	Date Issued	Issued to	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

REVIEWERS

Version	Review Date	Reviewed By	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

APPROVERS

Version	Date Approved	Approved By	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

DISTRIBUTION LIST

Date	Name / Distribution List	Comments
30-Jul-2025	Customer_DL_ABC	Published to Customer ABC

DOCUMENT CONTROL PAGE

RELATED DOCUMENTS

DOC_ID	DOC Version#	DOC Link	Comments
SCG/BASEINS/005/1.0			Base Template Instructions
SCG/PXF/008/1.0			Policy Exception Form
SCG/RXT/037/1.0			Risk Exception Template

CONFIDENTIALITY STATEMENT

This document is the exclusive property of [SecureCyberGates]. This document contains proprietary and confidential information. Duplication, Redistribution, or use, in whole or in part, in any form, requires consent of [SecureCyberGates].

[SecureCyberGates] may share this document with auditors under non-disclosure agreements [NDA] to demonstrate Security Audit requirement compliance.

Contents

1) Objective

Our Data Backup Policy establishes the activities that need to be carried out by each Business Unit, Technology Unit, and Corporate Units (departments) within [SecureCyberGates].All departments must utilize this methodology to properly backup and store media that contains critical data and information. All electronic records existing on [SecureCyberGates] data processing systems must be backed up and sent to an offsite location according to Offsite Storage Requirements of this policy. Retention standards must be defined and put into action to support business and regulatory requirements.

2) Roles &Responsibilities

Roles	Responsibilities
CISO	Accountable - Overseeing the implementation and enforcement of this policy [Review and Approve Policy]
DPO [Data Privacy Officer]	Responsible to review this Policy.
IT Team / Security Team	1. Responsible for ensuring Data backup requirements are in place. 2. Responsible for enforcing these requirements. 3. The [SecureCyberGates] IT Department shall possess ownership responsibility for the overall Data Backup Policy & Standards and ensuring uniformity of the Data Backup process. Additionally, the [SecureCyberGates] IT Department shall work with the Security and BU department on implementing tape backup schedules, procedures and activities.
BU Heads or Project Managers	1. Ensuring that employees under their supervision comply with this policy. [Review and Approve this Policy]. 2. Each BU head must accept responsibility for ensuring critical data is stored on [SecureCyberGates] data processing systems and that those systems are being backed up. The BU head is also responsible for relaying the information about the criticality of the data to the [SecureCyberGates] IT Department.
Employees / Contractors	1. Read this this Policy 2. Ask questions /Provide Feedbacks 3. Report possible or actual violations of this Policy.

3) Scope

Data Backup activities are performed to protect against the loss or damage of **critical data** contained on [SecureCyberGates]'s data processing systems. All departments using electronic data, critical data, regulatory data, etc., must determine and document their information availability requirements.

4) Data Backup Process

Data backups can be accomplished in various ways. However, not all methods of backups are appropriate for data that contains customer or confidential information. Only secure and authenticated resources can be used for the storage and backup of confidential data. Some practices that can be implemented for backup of daily data (not confidential data) like forms, reports, templates, etc. are as follows: (this type of data would be located on your PC, department PC, etc.)

Compact Disk: CDs are low-cost storage media and have a higher storage capacity than floppy diskettes. If you choose this method, you will need a PC equipped with a CD-RW drive (rewritable CD).

Network Storage: Data stored on networked PCs can be backed up to a networked disk or a network storage device. This is typically what most users will call their K: Drive or N: Drive. This is an assigned path to the network storage drive for them to save their data to.

Removable Cartridges: Removable cartridges are not common in desktop computers are often offered as a backup solution as a portable or external device. Removable cartridges, such as a Zip Drive storage device, are more expensive than floppy diskettes and are comparable in price to tape media depending on the media model and make. However, removable cartridges are fast, and their portability allows for flexibility. The portable devices come with special drivers and application to facilitate data backups.

Cloud Storage: Storing data on alternate sites / DR sites.
In addition to backing up critical data stored on PCs, all critical servers must be backed up on a regular basis. Servers can be backed up by an individual tape drive or by means of a centralized system, where a centralized backup device is attached to one server.

Three types of system backup practices are available to safeguard server data:

- **Full:** A full backup is the starting point for all other backups and contains all the data in the folders and files that are selected to be backed up. Because the full backup stores all files and folders, frequent full backups result in faster and simpler restore operations. In addition, because all files and folders were stored on a single media, locating a particular file is simple. However, the time required to complete a full backup can be time consuming.
- **Incremental:** An incremental backup captures files that were created or changed since the last backup, regardless of the type. The time it takes to execute the backup may be a fraction of the time it takes to perform a full backup. However, to recover a system from an incremental backup, media from different backup operations may be required.
- **Differential:** A differential backup stores files that were created or modified since the last full backup. The advantaged of a differential backup is that it shortens restore

time compared to a full back upon an incremental backup. As a disadvantage, differential backups take longer to complete than incremental backups.

[SecureCyberGates] deploys a strategy of **weekly full backups** with **daily incremental backups with a retention of 1 month**. On cloud, a block storage snapshot policy is selected to achieve this from the respective cloud provider for compute instances and the database service backup function is also utilized. This help ensure a backup is performed daily in any environment

5) Data Backup Requirements

The following activities provide the foundation for developing and implementing the Data Backup Process. The following tasks have been defined as part of the Standard Operating Procedures for Data Backup on Data Center Technology components. Responsibilities have been assigned to the [SecureCyberGates] IT Department.

- Identify and define the type of backups necessary to protect data.
- Develop, implement and document detailed procedures on how to backup and restore data for each of these systems.
- Establish and document backup schedules for each technology component that requires their data to be backed up.
- All backup jobs should be verified for completion and documented in a log.
- Define procedures and create documentation for sending tapes offsite to a Vendor or another [SecureCyberGates] owned facility.
- All tapes must be recorded as to when they were sent offsite and when they are expected to be returned (offsite tape log)
- Establish and document a test schedule to periodically test the restoration of data to an isolated server, platform, application, database, etc. (Use the Testing Process)
- Identify methods for recycling and retiring backup tapes

Data Backup

- Daily backups of data hosted in cloud environments will be performed.
- Backups are stored securely in object storage with encryption enabled.
- Data recovery procedures will be tested.

Disaster Recovery

- Disaster recovery plans have been established to ensure business continuity in the event of cloud service disruptions or outages.
- Recovery time objectives (RTOs) and recovery point objectives (RPOs) will be defined depending on services subscribed
- Disaster recovery will be tested at least annually.

6) Data Backup Frequency

Backups should be based on results of the **Application & Data Criticality Analysis** and the **Business Impact Analysis**. If data isn't being backed up frequently and is critical to the business unit, strategies should be implemented to support the business requirement. Defining and implementing backup schedules is mandatory. Each server must have a backup scheduled created and followed. At a minimum, all servers should have a full backup completed **weekly**. The entire backup scheduled should be recorded in the Data Backup Plan and incorporated into the daily computer operations standard operating procedures.

7) Data Backup Testing

Backup strategies for crucial systems must be regularly tested according to the Testing & Revision Policy & Standards. (Testing levels are determined by the Business Unit's overall RTO for the data.)

8) Offsite Storage

All electronic records with an obligation for accessibility identified in the Data Backup Plan must be stored offsite in a safe, protected environment available to [SecureCyberGates] in time periods that meet business operations / recovery requirements. Furthermore, it is suggested that intermittent audits of the offsite material are performed to make certain that data stored offsite is recent, properly synchronized with onsite records, available and functional to support the business requirements of [SecureCyberGates]. As a general standard, all backup activities conducted in the [SecureCyberGates] environment will, at a minimum, maintain **two generations of a backup offsite at all times.**

9) New Project / Change Management Requirements

Any project for a new technology component (computer system) must include an evaluation of the affect the addition will have on data backup and retention schedules. The implementation of any changes to the backup system to accommodate the new system must be included in the **project management process**. New systems must have the following ascertained and documented:

- Recovery time objective (RTO)
- Application to be backed up [Web App, Mobile App, Desktop App etc.]
- Environment details [Development, SIT, UAT, Prod etc.]

- Database details
- Application interface points
- Application Dependencies
- Application users
- Synchronization points with other applications
- Recovery Requirements (Requires a new plan to be created)

Any change to an existing technology component must comprise of an evaluation of the affect the change will have on data backup and retention schedules. A major change should result in a preliminary backup and recovery audit being performed as per the Audit Requirements below.

Audit Requirements:

Processes and procedures must be defined, documented and implemented for periodic audits of backup processes to ensure:

- All necessary data is being backed up
- Backups are tested to ensure data can be resorted
- Materials designated to be offsite are offsite as expected

10) Employee Training and Awareness

10.1) All [SecureCyberGates] employees SHOULD undergo training and assessment on this policy during their initial induction [Onboarding].

10.2) Security team to conduct periodic trainings **ATLEAST ONCE** a year.

11) Compliance and Monitoring

11.1) Compliance with this policy is **MANDATORY**. Employees violating this policy will be subject to disciplinary action up to and including termination.

11.2) Third-party users, contractors, and vendors who **FAIL** to comply with this policy may have their access to [SecureCyberGates]systems , Application and networks revoked or suspended until compliance is achieved. Repeated or severe violations may result in the termination of their contracts or business relationships with [SecureCyberGates].

11.3) Periodic Audits and Assessments : [SecureCyberGates]'s IT department, in collaboration with the Information Security team, will conduct periodic audits and assessments to evaluate compliance with this password security policy.

11.4) Procedures must be defined and employed for monitoring backup jobs, times, data volumes and success rates of backup activities. This data must be assembled for tracking reasons and for evaluation of compliancy for established service level agreements,

business processing objectives, etc. Additionally, procedures need to be implemented for monitoring, reporting and tracking of problems that occur during the backup process.

12) Escalation Matrix

12.1) In case of any policy violations issues, the following escalation structure shall be followed to ensure timely resolution and appropriate accountability:

Level	Role	Contact
Level 1	Team Lead /Reporting Manager	First-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]
Level 2	Group Manager / Senior Managers	Second-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]
Level 3	CISO	Final-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]

12.2) Employee SHOULD provide sufficient evidences and details , Clear description of the issue.

12.3) Security team to define issue severity and proper SLA for issue resolution as per severity.

13) Policy Exceptions

13.1) There may be requirements where Employee needs policy exception for legitimate reasons, In such cases, employee should follow POLICY EXCEPTIONS template and approval process. **[Kindly refer Policy exception form [Document ID SCG/PXF/008/1.0]]**

14) Policy Review and Updates

14.1) This policy shall be periodically reviewed **[Atleast Once in a YEAR]**and updated to ensure its effectiveness, relevance, and alignment with [SecureCyberGates]objectives,legal requirements and industry best practices.

14.2) Feedback from employees, stakeholders, and external audits shall be solicited and considered for continuous improvement of the policy and associated procedures.

14.3) Regular audits and inspections shall be conducted to assess compliance with this policy and associated procedures, with non-conformances addressed through corrective actions and preventive measures.

14.4) Any updates or revisions to this policy will be communicated to all employees and relevant stakeholders through appropriate channels. Employees are responsible for familiarizing themselves with the latest version of the policy and adhering to its requirements.

15) Conclusion

By implementing and adhering to this policy, [SecureCyberGates] aims to ensure Company data is always available and protect its sensitive information, intellectual property, and critical systems from unauthorized access and data breaches. This policy aligns with industry best practices and incorporates robust requirements for password construction, protection, management, and system development standards.

SECURE CYBER GATES

THANKYOU!
FOR CYBER-SECURITY RELATED UPDATES, KINDLY FOLLOW BELOW PAGES...

https://www.linkedin.com/in/aj57/
https://www.linkedin.com/company/securecybergates
https://www.youtube.com/@SecureCyberGates
https://securecybergates.com/services
https://hackerone.com/crypto-khan
https://x.com/securecybergate
securecybergates@gmail.com

SECURE CYBER GATES