SECURE
CYBER
GATES

BUSINESS CONTINUITY & DISASTER RECOVERY POLICY

SECURE
CYBER
GATES

SECURE CYBER GATES

DOCUMENT CONTROL PAGE

Document ID	SCG/BCDRP/029/1.0
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 Business Continuity & Disaster Recovery Policy serves as guidance for establishing processes that will help [SecureCyberGates] recover from adverse situations with the minimal impact to operations. This Business Continuity & Disaster Recovery Policy establishes standards that promote fairness in establishing and managing the capability for maintaining the Continuity of Operations to ensure the availability of critical technology resources during adverse conditions.

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/ Security Team	1. Responsible for ensuring Business Continuity and Disaster Recovery requirements are in place. 2. Responsible for enforcing these requirements. 3. Overseeing the implementation and enforcement of this policy.
BU Heads or Project Managers	1. Ensuring that employees under their supervision comply with this policy. [Review and Approve this Policy].
Employees / Contractors	1. Ask questions /Provide Feedbacks 2. Report possible or actual violations of this Policy. 3. Understanding and complying with this policy and related procedures.

3) Scope

This Policy applies to anyone who conducts business for or on behalf of [SecureCyberGates] including:

- All employees
- Management and company owners
- External business partners who act on [SecureCyberGates]'s behalf or in our interest as Third Party Representatives

It is important to note that every situation may not be addressed in this Business Continuity & Disaster Recovery (BCDRP) Policy; if you are unsure how [SecureCyberGates] standards or values apply in a given situation, please ask questions and seek further guidance from the Security , IT Team. Each and every one of us are responsible for ensuring that we follow these guidelines, and we will be held accountable for upholding our commitments to this Business Continuity & Disaster Recovery Policy.

4) Contingency Plan

4.1) Control Objective

The organization develops, implements, and governs processes and documentation to facilitate the implementation of an enterprise-wide Continuity of Operations policy, as well as associated standards, controls and procedures.

4.2) Standard

[SecureCyberGates] shall establish procedures, supporting business processes, and implement technical measures to ensure the continuity and availability of operations while operating in other-than-normal conditions, which include:

(a) Developing a contingency plan that:

1. Identifies essential missions and business functions along with associated contingency requirements;
2. Provides recovery objectives, restoration priorities, and metrics;
3. Addresses contingency roles, responsibilities, and assigned individuals with contact information;
4. Addresses maintaining essential missions and business functions despite system disruptions, compromises, or failures;
5. Addresses eventual full system restoration without compromising initially planned security measures;
6. Is subject to review and approval by company management;

(b) Distributing copies of the contingency plan to key contingency personnel;
(c) Communicating contingency plan changes and updates to key contingency personnel;
(d) Coordinating contingency planning activities with incident handling activities;
(e) Reviewing the contingency plan at least annually;
(f) Revising the contingency plan to address necessary changes; and
(g) Establishing procedures for obtaining access to sensitive data during other-than-normal or emergency conditions.

4.3) Guidelines

A consistent, unified framework for business continuity planning and plan development should be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance and information security requirements.

Requirements for business continuity plans include the following:

- ➢ Defined purpose and scope, aligned with relevant dependencies
- ➢ Accessible to and understood by those who will use them
- ➢ Owned by a named person(s) who is responsible for their review, update, and approval
- ➢ Defined lines of communication, roles, and responsibilities

- ➢ Detailed recovery procedures, manual workaround, and reference information
- ➢ Method for plan invocation

[SecureCyberGates] will establish detailed response and recovery procedures to address specific incidents. These procedures will be communicated to relevant personnel, and regular training and drills will be conducted.

5) Contingency Plan Root Cause Analysis & Lessons Learned

5.1) Control Objective

The organization incorporates lessons learned for contingency plans.

5.2) Standards

Asset custodians and data / process owners are required to:

(a) Perform a Root Cause Analysis following events that trigger usage of continuity plans; and

(b) Incorporate lessons learned in updates to the continuity plans

5.3) Contingency Plan Update

The organization regularly updates recovery strategies to keep current with business needs and technology changes.

Asset custodians and data / process owners are required to:

(a) Review the entire contingency plan at least once a year;

(b) Review any test / exercise results; and

(c) Initiate corrective actions, as necessary.

6) Data Backups

6.1) Control Objective

The organization:

- ➢ Conducts backups of user-level information contained in the systems;
- ➢ Conducts backups of system-level information contained in the systems;
- ➢ Conducts backups of system documentation including security-related documentation; and
- ➢ Protects the confidentiality and integrity of backup information at the storage location.

6.2) Standards

Asset custodians and data / process owners are responsible for:

(a) Conducting backups of user-level information contained in systems;

(b) Conducting backups of system-level information contained in systems;

(c) Conducting backups of system documentation including security-related documentation; and
(d) Protecting the confidentiality and integrity of backup information at the storage location.

6.3) Guidelines

Data / process owners should ensure that each system is automatically backed up on at least a weekly basis and more often for systems storing sensitive information. To help ensure the ability to rapidly restore a system from backup, the operating system, application software and data on a machine should each be included in the overall backup procedure. These three components of a system do not have to be included in the same backup file or use the same backup software. There should be multiple backups over time, so that in the event of malware infection, restoration can be from a version that is believed to predate the original infection. All backup policies should be compliant with any regulatory or official requirements.

System backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information. It is necessary for orderly and efficient data backup and restoration. The individual responsible for data backups should fully document the following items for each generated data backup:

- Date of data backup;
- Type of data backup (e.g., differential, incremental, full or copy);
- Individual responsible for data backup;
- Extent of data backup (e.g., files / directories);
- Data media on which the operational data are stored;
- Data media on which the backup data are stored;
- Data backup hardware and software with version number(s);
- Data backup parameters (e.g., type of data backup, etc.); and
- Storage location of backup copies.

Selecting the appropriate backup technology is a management decision. The level of risk will determine the level of data backup technologies and redundancies required. Regardless of the available technology solution, the following methods of data backup may be used:

Data Backup Methods:

- **Full:** A full backup is a backup of every file on a file system, whether that file has changed or not. The alternatives to a full backup are incremental backup and differential backup. A full backup takes longer to accomplish and requires the most storage space on the backup media, but it also provides the quickest restore times. A full backup should be performed weekly on production systems, along with daily differential or incremental backups. A full backup should also be performed before any major planned changes to the system.

- **Incremental:** An incremental backup image is a copy of all database data that has changed since the most recent, successful, backup operation (whether that was a full or incremental backup). This is also known as a cumulative backup image, because a series of incremental backups taken over time will each have the contents of the previous incremental backup image. The predecessor of an incremental backup image is always the most recent successful backup of the same object.

- **Differential (Delta):** A delta or incremental delta, backup image is a copy of all database data that has changed since the last successful backup (full) of the data in question. This is also known as a differential or non-cumulative, backup image. The predecessor of a delta backup image is the most recent full backup.

Continuous Data Protection Backups

Continuous Data Protection (CDP), also called continuous backup or disk-to-disk (D2D), refers to backup of computer data by automatically saving a copy of every change made to that data, essentially capturing every version of the data that the user saves. It allows the user or administrator to restore data to any point in time.

CDP backups should be used in conjunction with archiving backups, such as tape or HDD cassette backups. This rationale is due to the need to have archived "snapshots" of the data in case the current and CDP data become corrupted.

Internet-Based Backups

The preferred method for data backups is through utilizing both a local copy of a backup, be it tape, HDD cassette or CDP device, as well as an automated Internet-based data backup provider. Internet-based backups help eliminate human error associated with manually producing tape backups and can be scheduled each day, without human intervention.

6.4) Current back-up configuration

- Back-ups are conducted daily.
- Backup Teams will conduct back-ups as scheduled.
- Backups will be stored in a separate Cloud region than primary storage.

6.5) Backup Policy Update

[SecureCyberGates]'s IT department is required to provide for the recovery and reconstitution of systems to a known state after a disruption, compromise, or failure. This includes but is not limited to:

(a) Conducting backups;

(b) Maintaining backup solutions and media; and

(c) Periodically testing backup solutions to validate that successful recovery is possible.

Recovery is executing system contingency plan activities to restore organizational missions / business functions. Reconstitution takes place following recovery and includes activities for returning organizational systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities, recovery point / time and reconstitution objectives and established organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of any interim system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored system capabilities, reestablishment of continuous monitoring activities, potential system reauthorizations and activities to prepare the systems against future disruptions, compromises, or failures.

7) BCDRP Strategy

[SecureCyberGates] Business Continuity Disaster Recovery Plan (BCDRP) consists of approaches and practices to ensure that in the event of disaster or other eventualities, [SecureCyberGates] customer services and solutions are not impacted. [SecureCyberGates]'s Business Continuity Plan covers **2 areas:**

i. **Software**
   a. All source code versions and implemented software modules are saved and archived to back up sites
   b. Frequently accessed files are also on-line archived to multiple locations
      i. NAS back-up in HQ office [On premise]
      ii. AWS S3 (encrypted using AES-256). [Cloud]
   c. The back-up policy for frequently accessed files is daily from 12 midnight onwards and software programs for deployed modules are stored in VM (backed-up quarterly into external hard drives).

ii. **Human capital:**
   a. Comprehensive policies to retain skilled talent
   b. Rotate resources on a biennial basis to ensure knowledge parity
   c. Agile development practices

Critical business processes are identified, and continuity objectives are formalized at the solution definition period or at the biennial management meeting. Risk assessments are performed biennially to identify operational threats and to mitigate disruptions to any [SecureCyberGates] service/solution. Risk treatment remedies such as upgrading back-up equipment, moving archived material to online back-up etc are done.
Monitoring and Planning activities include but not limited to:

i) Ad-hoc or biennial monitoring of checklists
ii) Constant monitoring of activities and back up procedures
iii) Reporting and brainstorming meetings for possible improvements with the CTO

iv) Well documented and reported DR drills: Full cycle of testing where the systems switch from Production -> DR -> Production to test the fallback integrity (performed live typically starting from midnight Friday till Saturday).

[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

8) Employee Training and Awareness

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

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

9) Compliance and Monitoring

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

9.2) 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].

9.3) 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 security policy.

10) Escalation Matrix

10.1) 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]

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

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

11) Policy Exceptions

11.1) 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]]**

12) Policy Review and Updates

12.1) 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.

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

12.3) 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.

12.4) 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.

13) Conclusion

[SecureCyberGates] is committed to protecting the confidentiality, integrity, and availability of its data and information assets through the implementation of appropriate security controls. By adhering to the requirements and guidelines outlined in this policy, [SecureCyberGates] aims to minimize the risk of unauthorized access, data breaches, and other security incidents, while ensuring compliance with applicable laws, regulations, and industry standards, including the SOC 2 standard.

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

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