Backup and Recovery Policy

Double Good Technologies, LP

January 2024

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.1, A1.2

Table 2: Document history

Date	Comment
Jun 15 2023	Initial document

1 Policy Statement

DoubleGood Technology is committed to maintaining a reliable and secure backup and recovery process for its data. This policy outlines the guidelines for data retention, backup procedures, recovery process, and testing to ensure data availability, confidentiality, and integrity. The policy aligns with industry best practices and complies with SOC 2 requirements.

2 Purpose

The purpose of this policy is to protect the confidentiality, integrity, and availability of data for DoubleGood Technology and its customers. It establishes comprehensive backup and recovery procedures to ensure data remains accessible when needed and can be recovered in the event of a system failure, data breach, or disaster.

3 Scope

The scope of this policy encompasses all data within DoubleGood Technology's systems and applies to all employees, contractors, and third-party service providers who have access to the data.

4 Policy

The following guidelines and requirements apply to the backup and recovery process:

4.1 Data Classification and Retention

a. Data Classification: All data within DoubleGood Technology's systems shall be classified based on its sensitivity and regulatory requirements.

b. Data Retention Periods: The retention periods for different data categories shall be defined and documented, considering legal requirements, business needs, and industry standards. The following retention periods apply:

- Financial and accounting data: 7 years
- Customer personal information: 3 years after the end of the customer relationship
- Employee records: 5 years after employment termination
- System logs and audit trails: 1 year

4.2 Backup Procedures

a. Regular Backups: DoubleGood Technology shall perform regular backups of critical data according to the defined backup schedule.

b. Backup Storage: Backed-up data shall be securely stored in AWS S3 or other approved cloud-based storage services, following industry best practices and encryption standards.

c. Backup Integrity: Regular tests and verifications shall be conducted to ensure the integrity and recoverability of backup data.

4.3 Recovery Process

a. Recovery Point Objective (RPO): DoubleGood Technology shall define the maximum acceptable data loss in the event of a system failure or data breach, aligning with the trust service principle of data availability. The RPO requirement is set at 24 hours, meaning that in the event of a disruption, data should be recoverable up to a maximum of 24 hours prior to the incident.

b. Recovery Time Objective (RTO): The timeframe within which data and systems should be restored after a disruption shall be determined and documented, considering the impact on business operations and the trust service principle of data availability. The RTO requirement is set at 6 hours, indicating that systems and data should be restored within a maximum of 6 hours following a disruption.

c. Recovery Testing: Periodic recovery testing shall be conducted to validate the effectiveness and efficiency of the recovery process. This includes testing the restoration of data from backups to ensure the ability to recover critical systems and data. The testing frequency and methodologies will be established to meet the RPO and RTO requirements.

d. The data restoration procedures must be tested and documented. Documentation should include exactly who is responsible for the restore, how it is performed, under what circumstances it is to be performed, and how long it should take from request to restoration. It is extremely important that the procedures are clear and concise such that they are not A) misinterpreted by readers other than the backup administrator, and B) confusing during a time of crisis.

4.4 Policy Review and Updates

a. Regular Review: The backup and recovery policy, including the data retention aspects, shall be reviewed periodically to ensure compliance with changing legal and regulatory requirements.

b. Policy Updates: Any necessary updates or revisions to the retention policy shall be documented, communicated, and implemented accordingly.

5 Appendices

5.1 Example of journal of backups and recoveries

Date	Time	Action	Responsible Person
2023-05-15	10:00 AM	Creating database backup	John Smith
2023-05-15	10:15 AM	Checking backup integrity	Sarah Johnson
2023-05-16	09:30 AM	Data recovery after system failure	David Thompson
2023-05-18	11:45 AM	Restoring files from backup for us	Emma Davis