Data Backup and Disaster Recovery Policy

1. Purpose and Scope:

This policy outlines the procedures and guidelines for the backup and recovery of data to ensure the integrity, availability, and continuity of critical business operations in the event of data loss, corruption, or disaster.

2. Responsibilities:

- The Chief Information Officer (CIO) or designated IT manager is responsible for overseeing the implementation and maintenance of the backup and disaster recovery procedures.
- System administrators are responsible for executing backup operations, monitoring backup processes, and coordinating recovery efforts.
- All Go Daddy employees are responsible for adhering to data backup policies and promptly reporting any data loss or corruption incidents to the IT department.

3. Data Backup Procedures:

- Regular backups of all critical data, including databases, applications, and user files, will be performed according to predefined schedules.
- Backup frequency, retention periods, and storage locations are determined based on data criticality, regulatory requirements, and business needs.
- Backup operations will utilise reliable backup technologies and encryption methods to ensure data confidentiality and integrity during transmission and storage.

4. Backup Storage and Security:

- Backup data is stored in secure, off-site locations to mitigate the risk of data loss due to on-premises disasters such as fires, floods, or theft.
- Access controls and encryption are implemented to restrict unauthorised access to backup media and prevent data breaches.

5. Disaster Recovery Planning:

- A comprehensive disaster recovery plan (DRP) has been developed by Go Daddy to outline the procedures and responsibilities for responding to different types of disasters.
- The DRP includes detailed recovery objectives, priorities, and strategies for restoring critical systems and data within specified recovery time objectives (RTOs) and recovery point objectives (RPOs).

6. Testing and Maintenance:

- Regular testing and validation of backup and recovery procedures will be conducted to ensure their effectiveness and identify any deficiencies.
- Backup systems and recovery processes are periodically reviewed, updated, and optimised to accommodate changes in technology, infrastructure, and business requirements.

7. Incident Response and Reporting:

- In the event of data loss, corruption, or disaster, the incident response team will promptly initiate the appropriate recovery procedures as outlined in the DRP.
- All data loss incidents and recovery activities are documented, analysed, and reported to management for review and follow-up actions.

8. Training and Awareness:

- Go Daddy employees will receive regular training and awareness programs on data backup best practices, disaster recovery procedures, and their roles and responsibilities during recovery efforts.

9. Compliance and Audit:

- The backup and disaster recovery processes comply with relevant regulatory requirements, industry standards, and organisational policies.
- Periodic audits and assessments are conducted to evaluate the effectiveness of backup and recovery controls and ensure compliance with established policies and procedures.

10. Policy Review and Revision:

- This policy will; be periodically reviewed, updated, and communicated to all relevant stakeholders to reflect changes in technology, business operations, or regulatory requirements.

Safe 2 Open* Leadership Team

11th March 2024

* Safe 2 open is a trading name of TWH holdings Limited