

FIXMYPCANYWHERE.COM

ENCRYPTGATE DATA SOLUTIONS

DATA BACKUP POLICY

This policy outlines the procedures and responsibilities for backing up customer and internal business data to ensure data integrity, security, and recoverability in case of system failures, cyberattacks, or other incidents.

Scope: This policy applies to all employees, contractors, and third-party vendors associated with ENCRYPTGATE DATA SOLUTIONS. It covers all customer data entrusted to the company as well as the organization's internal data.

\*Policy Statement

Data Classification

All data is classified into two categories:

-Customer Data: Includes files, configurations, and sensitive information retrieved from clients' devices.

-Business Data: Includes operational records, financial documents, and internal communications.

\*Backup Frequency

Customer Data: Backups are created immediately after receiving the data and periodically during the repair process.

Business Data: A full backup is conducted weekly, with incremental backups daily.

Backup Storage

Backups are stored on secure, encrypted external drives and/or cloud services.

\*Data retention periods are as follows:

Customer Data: Retained for 30 days post-service completion unless otherwise required.

Business Data: Retained in line with legal and operational requirements.

\*Data Access and Security

Only authorized personnel (MYSELF) have access to backup systems and files.

Customer data backups are strictly isolated and handled per privacy agreements.

\*Testing and Validation

Regular testing of backup recoverability is conducted at least once a month.

Errors or failures in the backup process are resolved promptly.

\*Data Disposal

Expired backups are securely destroyed through industry-standard methods to ensure data confidentiality.

\*Emergency Recovery

In case of data loss or corruption, backups will be restored following prioritized recovery procedures.

Recovery times are documented and optimized to meet business continuity objectives.

\*Roles and Responsibilities

IT Technicians: Perform regular backups and monitor their integrity. Ensure compliance with this policy when handling customer data.

\*Management: Oversee implementation and compliance with the policy. Authorize data retention extensions if required.

Data Protection Officer (Robin Lauscher): Manage overall data security and ensure backups align with data protection regulations.

\*Policy Review

This policy is reviewed annually or whenever significant changes occur in business practices, legal requirements, or technology systems.

\*Enforcement: Any violation of this policy may result in disciplinary action, up to and including termination of employment or service contracts.