Data Encryption Policy

1. Purpose

The purpose of this Data Encryption Policy is to establish and maintain the framework needed to ensure data confidentiality and integrity through the use of encryption techniques. This policy applies to all employees, contractors, and third-party users of Razzberry's Tech Services Inc.

2. Scope

This policy covers all data (electronic, printed, or otherwise) owned, used, or managed by [Organization Name], across all mediums and formats.

3. Policy Statement

Razzberry's Cyber Security Solutions Inc. is committed to protecting its data assets from unauthorized access and exposure by employing encryption technologies.

4. Data Classification

- **4.1 Confidential Data:** Includes sensitive information, personal data, trade secrets, etc. All confidential data must be encrypted both at rest and in transit.
- **4.2 Internal Data:** Non-public data, internal communications, etc. Encryption is recommended, especially when transmitted over unsecured networks.
- **4.3 Public Data:** Publicly available information. Encryption is optional.

5. Encryption Standards

- **5.1 Approved Encryption Techniques:** Use only industry-standard encryption methods (e.g., AES, RSA).
- **5.2 Encryption Strength:** Minimum of 256-bit encryption for data at rest and 128-bit encryption for data in transit.
- **5.3 Key Management:** Secure storage and handling of encryption keys, with regular rotations and restricted access.

6. Implementation

- **6.1 Data at Rest:** Encrypt all confidential data stored on servers, workstations, laptops, removable media, and backup systems.
- **6.2 Data in Transit:** Use encrypted connections (e.g., SSL/TLS, VPN) for transmitting confidential data across networks.
- **6.3 Mobile and Portable Devices:** Mandatory encryption for any confidential data stored on mobile devices, including laptops, tablets, and smartphones.

7. Compliance

- **7.1 User Responsibility:** All users must comply with this policy and report any suspected security breaches.
- **7.2 Auditing and Monitoring:** Regular audits to ensure compliance and effectiveness of encryption practices.
- **7.3 Violations:** Violations of this policy may result in disciplinary action, up to and including termination of employment.

8. Training and Awareness

All employees must receive training on this policy and the proper use of encryption technologies.

9. Policy Review and Modification

This policy will be reviewed annually and updated as necessary to reflect changes in legal, technical, and business environments.

10. Approval and Implementation

Signature: Mitchell Laframboise

Name (Print): Mitchell Laframboise

Title: Executive Director

Date: 07 October 2024