Crazy by Chiari
Technology and Data Security Policy

1. Purpose

The purpose of this Technology and Data Security Policy is to establish guidelines and procedures for the secure and responsible use of technology resources and the protection of sensitive data by **Crazy by Chiari** ("the Organization"). This policy aims to safeguard the organization's information assets, maintain data confidentiality, and mitigate technology-related risks.

2. Acceptable Use of Technology Resources

Section 1: Authorized Use

1.1. All technology resources, including but not limited to computers, servers, software, networks, email, and internet access, shall be used exclusively for official organizational purposes.

Section 2: Prohibited Activities

2.1. Unauthorized access to, modification of, or interference with the organization's technology resources is strictly prohibited.

2.2. Users shall not engage in activities that violate copyright or intellectual property rights, distribute malicious software, engage in hacking or other malicious activities, or transmit offensive, harassing, or inappropriate content.

3. Data Security

Section 1: Data Classification

1.1. Data shall be classified into categories based on sensitivity and confidentiality, such as public, internal, confidential, and restricted. Clear guidelines for handling each data category shall be established.

Section 2: Access Control

2.1. Access to data shall be restricted based on the principle of least privilege, ensuring that individuals only have access to the data necessary to perform their job duties.

2.2. User authentication mechanisms, such as strong passwords, multi-factor authentication, or biometrics, shall be implemented to protect data access.

Section 3: Data Encryption

3.1. Sensitive data, especially when transmitted over networks or stored on portable devices, shall be encrypted using industry-standard encryption methods.

Section 4: Data Backups

4.1. Regular data backups shall be performed to prevent data loss in case of system failures or security incidents.

4.2. Backup copies shall be securely stored and tested for data restoration.

Section 5: Data Retention and Disposal

5.1. Data shall be retained and disposed of in accordance with applicable laws and regulations. A data retention and disposal policy shall be established.

4. Information Security

Section 1: Security Awareness

1.1. Employees and volunteers shall receive training on information security best practices, including data handling, password management, and email security.

Section 2: Incident Reporting

2.1. Suspected security incidents, breaches, or data breaches shall be reported promptly to the designated incident response team or responsible personnel.

Section 3: Security Updates

3.1. All software, operating systems, and security patches shall be regularly updated to protect against known vulnerabilities.

Section 4: Anti-Malware Measures

4.1. Anti-malware software shall be installed and regularly updated on all organizational devices to protect against viruses, spyware, and other malicious software.

5. Mobile Devices and Remote Access

Section 1: Mobile Device Security

1.1. Mobile devices used for organizational purposes shall be protected with passwords, encryption, and remote wipe capabilities.

Section 2: Remote Access Security

2.1. Remote access to organizational resources shall be secured through secure virtual private networks (VPNs) or other approved methods.

6. Compliance with Laws and Regulations

Section 1: Legal Compliance

1.1. The Organization shall comply with all applicable federal, state, and local laws and regulations related to technology and data security, including data protection and privacy laws.

7. Review and Amendments

Section 1: Policy Review

1.1. This Technology and Data Security Policy shall be reviewed annually and may be amended as necessary to ensure its continued relevance and effectiveness.

Crazy by Chiari
Date of Policy Adoption: 1/15/25