Softer Ingenuity, LLC
September 25, 2023

Security and Privacy Policy

1. Information Security and Privacy Objectives

1.1 To protect sensitive information and safeguard all sensitive data, including client information, proprietary software, and intellectual property.

1.2 To maintain compliance with laws and regulations, adhering to relevant data protection, privacy, and security laws and regulations applicable to our industry and client contracts.

2. Access Control

2.1 User Authentication:

- Use strong authentication mechanisms for system access, including at least two-factor authentication to access client systems.

2.2 User Authorization:

- Ensure access is granted on a need-to-know basis and follows the principle of least privilege.

3. Data Protection and Privacy

3.1 Data Encryption:

- Make use of virtual private networks (VPN) to create a secure connection between computing devices and client computer networks to protect sensitive client data.

3.2 Data Handling:

- Establish procedures for secure storage, transfer, and disposal of data in compliance with relevant data protection laws.

3.3 Children's Privacy:

- Softer Ingenuity does not knowingly collect personal information from children under the age of 13. If you believe that we have unintentionally collected personal information from a child under 13, please contact us immediately so that we can take appropriate steps to remove such information from our records.

4. Security Awareness and Training

4.1 Employee Training:

- Conduct regular security awareness training for all staff to promote a culture of security.

4.2 Incident Reporting:

- Report security incidents or potential vulnerabilities promptly.

5. Physical Security

5.1 Secure Work Environment:

- Ensure the physical security of workspaces and equipment to prevent unauthorized access.

6. Vendor Management

6.1 Third-Party Assessments:

Assess the security practices of third-party vendors and contractors who have access to our systems or data.

7. Security Updates and Patch Management

7.1 Regular Updates:

- Keep all software, operating systems, and applications up-to-date with security patches.

8. Business Continuity and Disaster Recovery

8.1 Business Continuity Plan:

- Develop and maintain a plan to ensure the continuity of critical business operations in the event of disruptions.

8.2 Data Backup:

- Regularly back up critical data to ensure recoverability in case of data loss or system failure.

9. Compliance and Audit

9.1 Access Logs:

- Log access to client networks via VPNs; maintain logs for at least six months.

10. Incident Reporting and Accountability

- Employees or Contractors of Softer Ingenuity must immediately report all suspected breaches of systems or data to the Chief Information Security Officer (CISO) at (518) 227-0880.