Acceptable Use Policy

1. Policy statement

The Regional ABC Credit Union/Bank recognizes the significance of maintaining the privacy and security of consumer data in accordance with industry best practices and the Gramm-Leach-Bliley Act (GLBA). In order to protect client information, improve IT security, and preserve business productivity, the company creates the following Acceptable Use Policy (AUP).

2. Purpose/Objective

- **Ensure GLBA Compliance:** Put in place procedures to ensure that non-public personal information (NPPI) is protected in accordance with the standards set out by the Gramm-Leach-Bliley Act (GLBA).
- **Enhance IT Security:** Safeguard the organization's IT assets, networks, and systems from unauthorized access, disclosure, or misuse.
- **Maximize Online Banking Services:** Make the most of online banking to effectively service clients across several branches while preserving the confidentiality and integrity of sensitive financial data.
- **Prioritize Customer Service:** To guarantee continuous service and data security, acknowledge and give top priority to the customer service division as a crucial corporate function.
- **Content Filtering:** Use content filtering to keep an eye on and regulate how much time is spent online while reducing the dangers of visiting harmful websites and seeing offensive material.
- **Limit Personal Use:** To improve security and stop potential security risks, prohibit personal use of organization-owned IT assets and systems.
- **Email Security Controls:** Put in place measures to keep an eye on and manage how the system is used, protecting against viruses, phishing scams, and the unapproved sharing of private data.
- **Security Awareness Training:** Incorporate policy review into a yearly security awareness training program to guarantee that all staff members are knowledgeable of and abide by security procedures.

3. Scope

This policy applies to all employees and contractors within the organization and covers the following domains of the IT infrastructure:

- **Network Security:** all network activity, such as using the internet and online banking.
- **Endpoint Security:** security protocols for desktops and mobile devices that are controlled by the enterprise.
- **Email Security:** regulations and standards for using the company's email system.

4. Standard

This policy refers to the following standards:

- **GLBA Compliance Standards:** Respect for GLBA rules pertaining to consumer data security.
- **Internet Content Filtering Standards:** Using content filtering solutions that are approved by the industry to restrict access to the internet.
- **Endpoint Security Standards:** Using endpoint security configurations and technologies to safeguard devices owned by the company.

5. Procedures

- **GLBA Compliance Procedures:** To guarantee GLBA compliance, regular audits and evaluations are conducted.
- **Internet Content Filtering Procedures:** To track and manage internet usage, content filtering programs must be installed and configured.
- **Endpoint Security Procedures:** Consistent updates and oversight of devices controlled by the enterprise to guarantee adherence to security guidelines.
- **Email Security Control Procedures:** These involve putting encryption and spam filters into place, among other email security controls.
- **Security Awareness Training Procedures:** Creating and implementing yearly security awareness training courses for staff members worldwide.

6. Guidelines

- **Implementation Roadblocks:** Prepare for possible difficulties when limiting personal use, and deal with them by communicating clearly and coming up with alternate plans for non-business-related activities.
- **User Cooperation:** Promote user cooperation by educating users about the value of security measures in protecting consumer information and by communicating clearly with them.
- **Continuous Monitoring:** Put systems in place for continuous monitoring in order to quickly detect and handle security incidents and guarantee continued adherence to the AUP.
- **Adaptability:** Review and update the AUP frequently to keep up with changing technology, regulatory requirements, and security concerns.