Goodyear Employees Credit Union, Inc.

Website Policy

The Credit Union maintains a website that is hosted by AMI Inc.(formerly CUC). All content is developed and maintained by Goodyear Employees CU. Using the World Wide Web (Web) is strongly encouraged in that it provides the Credit Union with a tool to convey information quickly and efficiently on a broad range of topics relating to its products, services, activities, objectives, policies and disclosures.

The Credit Union offers the following services electronically: Home Banking

Guidelines:

1. **POLICY AND PROGRAM RESPONSIBILITY**

    A. The Credit Union manager is responsible for maintaining the Credit Union's website operations. Any new website ideas or initiatives must be approved by the Board of Directors.

    B. Management will provide the necessary resources, specifically training , to adequately support website operations.

2. **COPYRIGHTED MATERIAL**. Copyrighted material will be used only when allowed by prevailing copyright laws and may be used only if the materials relate to the website's mission and should be approved by Management prior to use.

3. **EXTERNAL LINKS.** When external links to non- Credit Union websites are included, the Credit Union is responsible for ensuring that a disclaimer is made that the Credit Union does not endorses the product at the destination, nor does the Credit Union exercise any responsibility over the content at the destination.

    A. A disclaimer shall be displayed when linking to external sites. The disclaimer may appear on the page or pages listing external links whenever a request is made for any site other than the Official Credit Union website.

4. **RISK ASSESSMENT**

    A. Our Vendor semi-annually does a broadcast scan on our system to ensure proper working order and to prevent security breaches.

    B. Our Vendor regularly monitors security risks associated with technological and operational changes and maintains a current list of our critical website data.

5. **COMPLIANCE AND LEGAL**

A. The Credit Union ensures that its website will comply with all applicable laws and regulations.

B. The Credit Union has secured bond coverage for all of its website policies and procedures. Management has ensured that bond coverage is sufficient in the event of any loss due to an electronic transaction. Bond coverage is regularly assessed to ensure the sufficiency of coverage.

C. The Credit Union will provide disclosures regarding its website policies and procedures to members who have entered into a Home Banking relationship with the Credit Union upon request. In addition, the Credit Union will place appropriate warnings on its website, clearly stating that unauthorized access or use of the website is not permitted and may constitute a crime punishable by law.

D. The Credit Union maintains a privacy disclosure that is available to all members who visit the Credit Union website. The Credit Union monitors and enforces compliance with its privacy disclosures.

E. The Credit Union monitors its website on a regular basis to ensure that all disclosures are accurate and up-to-date.

6. AUDIT AND CONSULTING SERVICES

A. The Credit Union's website activities will be subject to an independent audit and quality review at least annually, and more frequently when appropriate. At a minimum, these reviews will cover website: security, penetration testing, regulatory compliance, privacy, application development and maintenance, incident response and business continuity, and virus detection and protection. The Credit Union management will correct the issues of concern uncovered by the independent audit and/or quality review.

7. VENDOR MANAGEMENT

The Credit Union's website was designed and is maintained by AMI Corp. our System supplier. The Credit Union has exercised due diligence in selecting its vendor to ensure that proper security measures are in place to protect member account information. The Credit Union will work with AMI to ensure the operational integrity and security of the computer and network supporting the website are maintained. The Credit Union will monitor this vendor relationship to ensure that they continue to meet the needs of the Credit Union (i.e., hardware, software, network services, content accuracy, availability, usability, security, and privacy). The Credit Union will periodically review security procedures employed by vendor to ensure it meets the Credit Union's minimum requirements.

8. **MEMBER SERVICE AND SUPPORT**

A. Management has established procedures and practices for promptly resolving member support issues, such as forgotten Login information. Management will take steps to ensure that adequate staff levels and training are in place to address member support issues.
B. We will inform members of maintenance or other technical issues that may affect access to the website activities through online messages.

9. **SYSTEM ARCHITECTURE AND CONTROLS**

A. The Credit Union maintains an inventory of hardware and software to ensure continuity of service in the event of a technological failure, natural disaster, or intentional destruction of its electronic systems. The Credit Union (or its vendor) maintains procedures to allow the Credit Union to restore its previous configuration in the event a software modification adversely affects the website.

B. The Credit Union has implemented a disaster recovery system as part of its business continuity plan. This system will be monitored regularly and updated as needed as a result of changes in technology, legislation, and infrastructure.

10. **SECURITY INFRASTRUCTURE AND CONTROLS**

A. The Credit Union maintains security measures consistent with the requirements of federal and state regulations, including risk management systems designed to prevent unauthorized access, both internal and external, to member information.

B. The Credit Union has procedures in place to protect member information systems in the event of natural disasters, intentional destruction, or technical failure.

C. Employees and Volunteers are educated on the importance of maintaining the confidentiality of member information.

D. All member account information is stored on servers protected with TSL using SHA-256 with RSA encryption to prevent unauthorized access and/or damage. These protections are monitored on a regular basis to assess potential security weaknesses.

E. Access to member accounts is restricted to members through the use of user ID

numbers and passwords. Account passwords that are not entered correctly after the 5th time will result in an automatic log-off to the session.

11. E-MAIL USE

A. The Credit Union forbids any employee or person with access to the Credit Union's electronic communication systems from misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or any of the Credit Union electronic communications systems. The user name, electronic mail address, organizational affiliation, and related information included with electronic messages or postings must reflect the actual originator of the message or posting.

B. The Credit Union forbids sending any message that could be construed as harassing, intimidating, threatening, illegal, fraudulent, embarrassing, defamatory, sexually explicit, obscene, or otherwise inappropriate.

.