



WEBSITE OPERATION

Overview

The {COMPANY-NAME} website provides information to members, potential members, and non-members regarding {COMPANY-NAME}. It is designed to allow members to transact business with {COMPANY-NAME} and assist non-members with information on how to join {COMPANY-NAME}. {COMPANY-NAME}'s website may provide links to websites, outside its website, that also serve this purpose.

Purpose

The purpose of this policy is to establish guidelines with respect to communication and updates of {COMPANY-NAME}'s public facing website. Protecting the information on and within the {COMPANY-NAME} website, with the same safety and confidentiality standards utilized in the transaction of all {COMPANY-NAME} business, is vital to {COMPANY-NAME}'s success.

Policy Detail

To be successful, the {COMPANY-NAME} website requires a collaborative, proactive approach by the stakeholders. All stakeholders share the same broad goals and objectives:

- Support the goals and key initiatives of {COMPANY-NAME}
- Develop content that is member focused, relevant, and valuable, while ensuring the best possible presentation, navigation, interactivity, and accuracy
- Promote a consistent image and identity to enhance marketing effectiveness
- Periodically assess the effectiveness of web pages

Responsibility

The Marketing Department and Chief Experience Officer (CXO) are responsible for the website content and ensuring that materials meet legal and policy requirements.

The IT Department is responsible for the security, functionality, and infrastructure of the website. The System Administrators will monitor the {COMPANY-NAME} website for response time and to resolve any issues encountered. The Core System Analyst will monitor the Online Banking Program for outages and will open a case with the appropriate vendor to log the event.

Links

{COMPANY-NAME} is not responsible for, and does not endorse, the information on any linked website, unless {COMPANY-NAME}'s website and/or this policy states otherwise. The following criteria will be used to decide whether to place specific links on the {COMPANY-NAME} website. {COMPANY-NAME} will place a link on the website if it serves the general purpose of {COMPANY-NAME}'s website and provides a benefit to its members.

{COMPANY-NAME}'s website will provide links to websites for:

- Secure member transactions such as bill pay, home banking, and loan applications
- Secure methods for members to receive information such as monthly statements
- Ancillary services that are provided to members through third-parties, such as ordering checks, mortgage loan applications, identity theft protection
- The {COMPANY-NAME} website contains a web link disclosure
- The {COMPANY-NAME} website will not provide links to websites for:
 - Illegal or discriminatory activities
 - Candidates for local, state, or federal offices
 - Political organizations or other organizations advocating a political position on an issue
 - Individual or personal home pages

Security

When a login is required, various forms of multi-factor authentication are implemented to ensure the privacy of member information and security of their transactions. This process is to be implemented for access to Online Banking.

The {COMPANY-NAME} website, as well as linked sites, may read some information from the users' computers. The website or linked transactional websites may create and place cookies on the user's computer to ensure the user does not have to answer challenge questions when returning to the site. The multi-factor authentication process will still be required at the next login. This cookie will not contain personally identifying information and will not compromise the user's privacy or security.

Website Changes

Changes to the website will be executed by the {COMPANY-NAME} Marketing Department, another trained and qualified employee, or a specialized firm or individual they may retain, and only with the explicit approval of the President/CEO or senior executive designated. Website changes require two parties in order to implement. On an annual basis, the {COMPANY-NAME} website is reviewed by a third-party compliance expert. At the time of any significant changes to the website, a compliance review will be conducted by the Director of Fraud and Compliance, legal counsel, or another reputable 3rd party compliance expert.

Regulatory Compliance

The {COMPANY-NAME} website must comply with all regulations dealing with security of member information, including, but not limited to:

- Part 748 of NCUA Rules and Regulations: Security Program;
- Report of Crime and Catastrophic Act;
- Bank Secrecy Act Compliance;
- As well as all other regulations, such as disclosure requirements.

At a minimum, the following disclosures will appear on the website:

- Privacy Policy and Web Privacy Policy
- EStatements and Disclosures
- Electronic Funds Transfer
- Monthly Billing Rights/Error Resolution Notice
- Web Links Disclaimer

Website Design

The {COMPANY-NAME} website maintains a cohesive and professional appearance. While a sophisticated set of services is offered on the website, the goal is to maintain relatively simplistic navigation to ensure ease of use. Security on the website and protection of member information is the highest priority in the layout and functionality of the site.