Social Media Policy

GENERAL POLICY STATEMENT AND DEFINITION:
SeaComm Federal Credit Union ("credit union") supports the use of social media to attract and interact with member and potential members as outlined in its marketing and communications strategies. For the purpose of this policy, social media is inclusive of any form of interactive online communication, in which users can generate and share content through text, images, audio and video, including but not limited to micro-blogging sites (e.g., Facebook, Google Plus, MySpace and Twitter); forums, blogs, customer review web sites and bulletin boards (e.g., Yelp); photo and video sites (e.g., Flickr and YouTube); sites that enable professional networking (e.g., LinkedIn); virtual world (e.g., Second Life); and social games (e.g., FarmVille and CityVille). Social media can be distinguished from other online formats based on the interaction and popularity of its communications.

SeaComm recognizes the value-add of leveraging social media. Being active in social media networking allows the credit union to be current and relevant while leveraging low-cost marketing tools. It provides an opportunity for the credit union to build a community of supporters; share credit union objectives and mission to provide quality financial products and services and promote financial education.

RISK RECOGNITION:
SeaComm recognizes that there are certain inherent risks with respect to social media regardless of the credit unions active participation in it. Social media poses additional legal, compliance, financial, reputational and operational risk. SeaComm's Board of Directors has approved this Social Media Policy to facilitate both directives and guidance to the credit union's employees and directors to mitigate such risks.

POLICY RESPONSIBILITY:
The primary responsibility for ensuring compliance with this policy and its operating procedures rests with senior management and each employee. The Vice President of Marketing and Communications is responsible for ensuring appropriate directives are implemented and administered in compliance with this Board approved policy. The Board of Directors shall review and approve this policy where applicable, for any changes that may be necessary to ensure the credit union's compliance for risk mitigation.

Any violation of this policy must be promptly reported to the Vice President of Marketing and Communications, and/or the President and Chief Executive Officer.

COMPLIANCE AND LEGAL RISKS:
Compliance and legal risk arise from the potential for violations of, or nonconformance with, laws, rules, regulations, prescribed practices, internal policies and procedures, or ethical standards. These risks also arise in situations in which the credit union's policies and procedures governing certain products or activities may not have kept pace with changes in the marketplace. This is particularly pertinent to an emerging medium like social media. Further, the potential for defamation or libel risk exists where there is broad distribution of information exchanges. Failure to adequately address these risks can expose the credit union to enforcement actions and/or civil lawsuits.

If the credit union deems it necessary to engage in social media to market products and originate new accounts, the credit union will take appropriate steps to ensure that advertising, account origination, and document retention are performed in compliance with applicable consumer protection and compliance laws and regulations.

REPUTATION RISK:

Reputation risk is the risk arising from negative public opinion. Activities that result in dissatisfied consumers and/or negative publicity could harm the reputation and standing of the credit union, even if the credit union has not violated any law. SeaComm's media activities will be sensitive to, and properly manage, any reputational risk that arises from those activities, including;

- Fraud and Brand Identity;
- Third Party Concerns;
- Privacy Concerns;
- Social Media Policy
- Consumer Complaints and Inquiries; and
- Employee Use of Social Media Sites.

OPERATIONAL RISK:

Operational risk is the risk of loss resulting from inadequate or failed processes, people, or systems. The root cause can be either internal or external events. Operational risk includes the risks posed by the credit union's use of information technology (IT), which encompasses social media. Social media is one of several platforms vulnerable to account takeover and the distribution of malware. The credit union will ensure it implements controls to protect its systems and safeguard member information from malicious software, adequately address social media usage, including its incident response protocol regarding a security event, such as a data breach or account takeover as appropriate.

SOCIAL MEDIA RISK MANAGEMENT:

In the event the credit union chooses not to use social media through certain mediums, the credit union will still be prepared to address the potential for negative comments or complaints that may arise within the many social media platforms and provide guidance for employee use of social media.

- Policies and/or procedures (either stand-alone or incorporated into other policies and/or procedures) regarding the use and monitoring of social media and compliance with all applicable consumer protection laws, regulations, and guidance. Further, policies and procedures should incorporate methodologies to address risks from online postings, edits, replies, and retention;
- A due diligence process for selecting and managing third-party service provider relationships in connection with social media and as required under the credit union's Third Party/Vendor Management Policy;
- An employee training program that incorporates the credit union's policies and/or procedures for official, work-related use of social media, and potentially for other uses of social media, including defining impermissible activities;
- An oversight process for monitoring information posted to proprietary social media sites administered by the credit union or a contracted third party;
- Audit and compliance functions to ensure ongoing compliance with internal policies and all applicable laws, regulations, and guidance; and
- Parameters for providing appropriate reporting to the credit union's President and CEO and/or Board of Directors that enable periodic evaluation of the effectiveness of the social media program and whether the program is achieving its stated objectives.

REPORTING AND MONITORING:

The Vice President of Marketing and Communications and/or delegated staff will monitor websites, blogs, forums, news, social media sites and bulletin boards for defamatory and malicious discussion or comments, rumors or inaccuracies as well as positive discussion, including comments referencing brand abuse and/or identity theft

leveraging search tools such as Google Alerts and search features on common sites such as Facebook, Twitter, Google, LinkedIn, Instagram and such others as may be appropriate.

Due to the fast-pace of social media, relevant posts and quick responses are a requirement. Therefore the Vice President of Marketing and Communications will be notified of all credit union mentions that require immediate action and engage the necessary staff to mitigate, sustain and/or terminate any references made regarding the credit union that may cause harm to its reputation, brand, members and/or employees.

USE OF SOCIA MEDIA:

Authorized employees may engage in social media activity during work time provided that such activity is directly related to their work and does not interfere with their or their co-workers' work. In the event of comments posted by member or non-members regarding the Institution, all such comments will be addressed proactively and timely. The Vice President of Marketing and Communications is authorized to evaluate any negative information posted on social media regarding the credit union, and to make the final determination as to how to respond. Authorized responses are limited to posting positive information about the credit union, answering questions about with factual unbiased information.

The credit union has an interest in public statements and other public content that refers to the credit union, their respective employees, officers, directors and members. It is important to recognize that employee use of social media websites may unintentionally or inadvertently create risks for the credit union. These risks include but are not limited to, accusations of harassment, discrimination and employment-related defamation. Therefore, employees' personal off-duty use of social media should be governed as follows:

- Unless specified in a job description and/or with the express approval of authorized credit union representatives, you are not authorized to speak or act on behalf of the credit union.
- Note that if you identify yourself as an employee of the credit union, you may be viewed as a representative of the credit union. Therefore, do not publicly post items that are derogatory, defamatory, harassing, or otherwise inappropriate, where such postings could be viewed as a negative reflection on the credit union.
- A disclaimer should be used when generating content that deals with the credit union or individuals associated with the credit union. A disclaimer such as, "The following comments are my own. They are not made on behalf of the credit union and are not intended to represent the credit union's positions, strategies, or opinions."
- Identify yourself as an employee of the credit union if you endorse its products through your personal social media communications. This is a legal requirement.
- If your employment terminates with the credit union, modify all references to your employment status on all social media websites.
- Maintain a professional presence; you are responsible for all content posted on your publicly accessible social media page(s) where you could be identified as an employee of the credit union.
- Employees are required to comply with the law regarding copyright or plagiarism when it pertains to postings related to the credit union, its vendors, or any other entity the employee may have contact with while employed at the credit union.
- Private or confidential information about the credit union should not be disclosed. Ensure common sense is exercised and strictly follow the credit union's policy on preserving confidential information
- You are not obligated to join a co-worker's network or to "friend" a coworker; it is your right to choose how you will engage via social media.
- A best practice is that supervisors should not "friend" their direct reports or join common networks where personal information may be shared.
- Remember that the credit union has the right to read what you write or say and determine if it meets the professional standards of the credit union or damages its reputation. Written or stated comments harmful or damaging to the credit union, its employees, volunteers, etc. may result in disciplinary action and may lead to termination.

- If you are asked by a co-worker or former co-worker of the credit union to give a personal reference, you must use a disclaimer such as, “The following comments are my own, not made on behalf of the credit union and are not intended to represent the credit union’s positions, strategies, or opinions.” Please follow the credit union’s established procedures for reference requests.
- Any communications that reference or could reflect on the credit union must comply with the Code of Conduct, Policies and Procedures of the credit union.
- Employees are prohibited from disclosing information related to the credit union or any of its employees, volunteers, officers, vendors, or members. Employees are also prohibited from disclosing any information that could identify another employee, volunteer, officer, vendor or member without that individual’s prior authorization.

VIOLATIONS AND DISCIPLINARY ACTION:

The credit union reserves the right to monitor, intercept, and review, without further notice, employees’ social media activity using the credit union’s technology resources. The credit union reserves the right to monitor and review public statements that refer to the credit union, its employees, officers, directors, vendors and members. Violation of the above stated guidelines and any other credit union policies may result in investigation and disciplinary action, up to and including termination.

LEGAL COMPLINACE:

The credit union intends this policy to comply with all applicable laws, including laws protecting certain employee activities and will enforce this policy consistent with legal requirements

4/20