

## Social Media Policy



Title Block	
<b>Document Name:</b>  Social Media Policy	<b>Document Number:</b>  ##
<b>Committee Approval Date:</b>	<b>Dept./Individual Responsible for Maintaining/Updating:</b> eBanking Coordinator
<b>Board Approval Date:</b> 05/18/2022	<b>Review Cycle Schedule:</b> Annually

## Table of Contents

<b><i>EXECUTIVE SUMMARY</i></b> .....	<b>3</b>
PURPOSE & SCOPE .....	3
<b><i>SOCIAL MEDIA RISKS ASSESSMENT</i></b> .....	<b>4</b>
COMPLIANCE & LEGAL .....	4
OPERATIONS .....	4
REUPUTATION .....	4
<b><i>GUIDELINES TO LIMIT RISK</i></b> .....	<b>4</b>
ANALYSIS .....	4
GOVERNANACE.....	5
COMMUNICATION .....	5
THIRD PARTY POSTINGS .....	6
MONITORING .....	6
TRAINING & EDUCATION .....	7
DOCUMENTATION .....	7
AUDIT & REVIEW .....	7

**## Social Media Policy****EXECUTIVE SUMMARY**

Social media has changed the way that organizations and individuals communicate. Involvement in social media is a competitive differentiator which grows social connections and community outreach strategies through popular online platforms. This policy is designed to identify, measure, monitor, and control the risks related to social media use for the bank.

The bank may use social media in a variety of ways, but the primary purpose is to develop relationships with existing customers and increase visibility and awareness to non-customers in the community. Since this form of customer interaction tends to be both informal and dynamic, and may occur in a less secure environment, it can present some unique challenges.

As part of the risk management procedures, social media sites will be monitored and updated as needed, with administrative involvement by the bank President, CFO and Senior Operations Officer. Content will be monitored and regulated according to the standards set by a “Rules of Engagement” document publically posted for customers to read and reference.

**PURPOSE AND SCOPE**

For the purpose of this policy, social media is considered to be a form of interactive online communication in which users can generate and share content through text, images, audio, and/or video. These more interactive communication channels include, but are not limited to, blogs, forums, wikis and social networking sites, such as Twitter, Facebook, LinkedIn, YouTube, Instagram and Pinterest, for both business and personal use.

The bank encourages the use of social media to help to build stronger, more successful business relationships. These platforms for online collaboration offer new ways to engage with customers, businesses and non-profits, prospective customers, our local community and beyond.

Official bank profiles and applications will not be used to expressly sell our products; they will be primarily used for:

- Engaging with, informing and responding to customers (with the exception of confidential information)
- Creating/maintaining relationships with online customers
- Keeping our brand fresh and up-to-date
- Educating online community of relevant issues and trends
- Soliciting customer and/or community feedback
- Publicizing sponsored events, seminars, etc.
- Sharing photos and videos of sponsored events, seminars, offices, etc.

When social media is used as a vehicle for direct advertising, the bank will abide by all advertising rules and regulations. Content of this nature is rare and is reviewed by a compliance officer before posting occurs.

## SOCIAL MEDIA RISKS ASSESSMENT

The use of social media by a financial institution for the purpose of attracting and interacting with customers can impact the bank's risk profile by introducing unique compliance, legal, operational and reputational risks. Such risks are the responsibility of the bank to predict and react to with planned risk management efforts. Proper risk identification and planning will protect the institution, its employees and ultimately all bank customers.

### COMPLIANCE & LEGAL

- Participation in social media by bank, employee or consumer are in violation of laws or posted rules and regulations, revealing confidential or inappropriate information
- Record of important communication between consumer and the bank via social media channels are erased or lost
- Privacy breach via social media due to bank's inadequate protection and regulation of employee access and privileges
- Online advertisement posted by bank is not compliant with laws and regulations

### OPERATION

- Customers post information about themselves to various unsecured websites, allowing a criminal to aggregate information and exploit customer's identity online
- Social media vendor (host) makes unpredictable updates or changes to user agreements and site controls
- Bank social media administrators do not adequately balance job responsibilities to include proper social media monitoring, or become distracted by social media sites
- Management cannot easily measure return on investment or report direct results from social media efforts

### REPUTATION

- Comments or complaints are posted on social media sites the bank is not actively monitoring, or the bank name is being used or cited without institution's knowledge
- False, offensive, personal or confidential information is posted to bank's site by a third party
- Customers experience technical issues or security breaches at fault of social media site, yet attribute negative experience with the bank
- Followers of bank's social media sites are disinterested or unsatisfied by the frequency, value, or responsiveness of bank's posted content

## GUIDELINES TO LIMIT RISK – RISK MANAGEMENT

In order to manage and limit these risks, the bank will analyze social media strategies, monitor and respond to posts or messages on bank social media pages, review and evaluate posts for compliance concerns and implement guidelines for employee administration personal use of social media. These

**## Social Media Policy**

risk management efforts are supported by additional policies and procedures created by the bank to protect the institution and its customers from associated risks that may not be listed above.

**ANALYSIS**

The available social media channels are varied in the services they offer, customers they reach and ability for a business to operate a public profile. Third-party relationships with social media vendors can be difficult to analyze due to the lack of vendor contracts and typical channels of communication between the two. The bank will conduct an evaluation of the risks and benefits posed by the prospective third party prior to engaging with it. If it is not possible to practice proper risk management such as reporting, editing or deleting information there should not be any official bank involvement.

In addition to official public profiles, the bank will monitor all known and relevant social media platforms for mention or involvement of the bank and respond appropriately. An account with Social Assurance has been created to track “mentions” about bankcda on the internet and social media. In the event that the bank cannot manage posted information and it should be removed, administrators will make all efforts to involve the site management and original publisher of the content.

**SOCIAL MEDIA GOVERNANCE**

The Bank has granted administrative access and assigned the main point of contact for social media alerts and response to Knock Marketing, as well as, President and Senior Operations Officer. The Senior Operations Officer and President will take responsibility for monitoring and responding to social media needs. Periodic oversight and final social media decisions will involve the bank President. Each individual has a personal profile and login access to social media sites which require personal profiles for administrators, otherwise a bank email address and login will be used for universal administration purposes. Knock Marketing with oversight from the President researches and posts content on behalf of the Bank and is ultimately responsible for maintaining the Bank’s social media sites.

The Bank prohibits non-administrator employees from posting on behalf of the Bank (informational, advertising, or otherwise). This restriction does not extend to “liking”, “sharing” or posting a comment from a personal account on the Bank’s social media sites, as these are authorized and encouraged interactions. Employees participating in social media communities in their personal time should use good judgment and take personal and professional responsibility for what is published. In accordance to the banks’ Technology and Internet Usage Policy employees are required to follow the bank’s guidelines in both off-duty and official participation to protect the bank’s integrity and reputation.

**COMMUNICATION**

As previously stated, the purpose of the bank’s social media presence is to engage with the community and interact with customers online. Social media users have an opportunity to use the available communication channels to post feedback, questions or personal comments on the bank’s site, related to the bank and its services or not. To guide customer participation and avoid the bank deleting posted information, social media sites will include documents called “Rules of Engagement”. The Rules of Engagement acts as a terms of use and disclosure for all social media users and the bank. This

**## Social Media Policy**

document includes customer responsibility, best practices and warnings for information sharing and rules for acceptable public content.

If social media is used to market products or originate new accounts, all regulatory and legal restrictions apply. Disclosures and links to additional information will enable customers to make informed decisions about fees, expected returns and all other related terms associated with product or service provided by the bank. All communication will be presented in a way that does not interfere with protection or compliance laws and regulations.

### THIRD PARTY POSTINGS

Third-party posts and comments are monitored by site administrators. The Bank has publicly posted documents to provide customers with social media terms of use and disclosures from the bank. The main purpose of these terms is to warn users not to release private information on a public forum. Additionally the terms state that content including profanity, offensive language, personal attacks, spamming, link-baiting, solicitation, and endorsements is prohibited and will be promptly removed. After review of the activity in question by any site administrator, further action such as permanently blocking the perpetrator may be taken. Disciplinary and/or legal action may be taken when deemed necessary.

Administrators will make edits or deletions to posts made by a third-party if deemed a risk to customers or if a violation to posted rules has been detected. These situations will be discussed by administrators and, if necessary, other members of executive management to ensure proper handling. Timely resolution is the main goal when dealing with a confidentiality risk and, therefore, discussion with management may occur *after* immediate action. Negative posts by a third-party are NOT to be deleted (unless they contain confidential information), but should be addressed as quickly as possible with a response. Response tones should always be positive and professional. Initial responses to complaints should be posted in the same comment thread when possible, displaying transparency and a willingness to address issues and concerns publicly. Additional follow-up on customer issues through more private and secure channels (outside of social media) may be necessary as well.

### MONITORING

Site Administrators are the primary monitor of all social media accounts. Customers and employees active on social media may also act as monitors of content, as they will be encouraged to report to the bank any posted information they believe should be removed

As described in the “Rules of Engagement” for social media, bank administrators reserve the right to edit, delete or block any content/individuals on official bank social media sites. That right will only be exercised if content is offensive, malicious, illegal, confidential or in any other way inappropriate to be viewed by other social media consumers. Negative content, so long as it does not violate these rules, will remain public and be acknowledged by an administrator with an appropriate tone and response.

Given the nature of social media services and availability, the bank is not responsible for monitoring all communications involving the bank when it appears on sites that are not maintained by, or in behalf of

**## Social Media Policy**

the bank. The bank will offer established communication channels for customers on all supported social media sites. Communication away from these channels should be monitored for risk management but may not be managed with a direct response due to the complexity of all available comment/complaint posting channels.

**TRAINING & EDUCATION**

Implementation of the social media strategies for the bank will be openly communicated and discussed with any bank employee. They will receive updates to bank policies and procedures regarding employee expectations and responsibilities. Employees are encouraged to use social media to support stronger, more successful online profiles, so long as employees understand the expectation of personal and professional responsibility for any published material. Employees should not respond to any questions or comments as though representing the bank. Employees upon hire will be trained in bank policies and procedures, including detailed descriptions of approved and non-approved social media communication.

Site administrators have the responsibility of staying up-to-date on current trends and procedures applicable to managing social media sites. The President will be main point of contact to all employees with important news or changes to established procedures.

**DOCUMENTATION**

Under regulation by the Community Reinvestment Act (CRA) the bank is required to maintain a public file containing all written, public comments and responses to those comments specifically relating to the bank's performance in helping to meet community credit needs. The bank maintains a Customer Compliance File documenting all formal and informal consumer complaints regarding federal law or regulation. Social media administrators will document the original comment and all related responses. Responses may require executive or compliance officer input and will be reviewed and handled accordingly.

**AUDIT & REVIEW**

The bank's internal auditor will review all procedures and information disclosures to ensure compliance with applicable regulations. The board of directors will review this policy at least once each year and make any revisions and amendments it deems appropriate.

**RELATED BANKCDA DOCUMENTS**

- Technology and Internet Usage policy
- Compliance Management Policy
- Privacy Policy
- Consumer Complaint Policy