QCR HOLDINGS, INC.

a relationship driven organization™

www.qcrh.com

Technology Usage and Information Security Policy

Effective Date:	March 1, 2005
Last Modified:	June 2019
Approved By:	QCRH Senior Technology and Operations Risk Committee, and each bank/entity board
Date Approved:	June (STORC), July/Aug 2019 (boards)
Next Review Date:	May 2020
Contact Person/Officer	VP Chief Technology Officer, SVP Chief Risk Officer

Table of Contents

PURPOSE AND SCOPE

The Board of Directors and management of QCR Holdings, Inc (QCRH) are committed to the establishment of an effective information security policy that identifies management's responsibilities for the protection of our customers' non-public personal information and our company's non-public information. Management realizes the importance of security controls to safeguard customer and company non-public information from unauthorized or accidental modification, destruction and disclosure. Therefore management establishes this *Technology Usage and Information Security Policy* as a guide to implement procedures for the protection of non-public personal and company information.

This policy applies to all employees of QCR Holdings, Inc. and its subsidiaries (the "Company"), and any non- employees such as temporary or contracted workers, consultants, vendors or agents (all hereafter referred to as "Users") who have access to the Company's technology resources, or with which the Company contracts to provide technology services. This policy covers activities on Company premises and remote access, through wire or wireless communication channels, or any off-site location. The Company reserves the right to amend this policy at its discretion. In case of amendments, Users will be informed appropriately.

The purpose of this policy is to:

- Communicate the requirements and expectations of technology use, including, but not limited to, hardware, software, e-mail, remote access and Internet usage. The policy discusses acceptable and unacceptable use and describes possible enforcement action for non-compliance.
- Ensure the Company's information assets are appropriately protected from unauthorized or accidental destruction, alteration or disclosure. Information assets include, but are not limited to, financial information, non-financial information and customer information.
- Set standards to ensure inter-compatibility of all systems, to ensure strength of security of systems, and to manage the cost of administration and use of resources.
- Provide guidance for the use of encryption to protect sensitive information. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

RESPONSIBILITIES

Everyone associated with the Company has a role in information security. The Company is a trusted custodian of data provided to us by our customers, vendors, candidates, and employees; therefore it is everyone's responsibility to ensure that due care is exercised in the protection of this data.

QCRH Senior Technology and Operations Risk Committee - The QCRH Senior Technology and Operations Risk Committee ("STORC") is responsible for providing overall guidance and establishing policy for the acquisition, operation, and disposition of hardware and software used within the Company, as well as physical and logical security. They are responsible for setting standards for all hardware and software used throughout the Company. STORC is also responsible for approving certain activities and overrides as addressed throughout the policy. Activities of this Committee are reported to the QCRH Management Cabinet which consists of select executive/senior management.

QCRH Best In Class (BIC) Council – The Best in Class Council is responsible for ensuring consistent applications and processes when appropriate across our organizations. They are responsible for oversight of projects, managing budgets, and approving project related Capital Expenditure Requests as applicable.

User Responsibilities - All Users are required to know and understand this policy. Users are required to respect all copyrights, software licensing rules, property rights, and the privacy of non-public customer and company information. Users are also responsible for using corporate information and computing resources responsibly and for authorized purposes. Users must be security-conscious and report any known issues or suspected violations immediately to their supervisor, a senior manager, or the AVP IT Operations Manager or to Risk Management. All Users are required to annually review this policy and electronically sign the "Statement of Understanding" provided during annual training.

QCRH Information Services Department - The management of systems and their support is generally centralized at QCRH. The QCRH Information Services Department (IS Department) serves all Company entities, and is granted the authority and responsibility for daily administration of the network and for implementing processes to appropriately monitor technology usage and compliance with technology and security standards. They are also responsible for the oversight of general applications used throughout the Company such as word processing, spreadsheet, e-mail, and database programs. The department will maintain separate departmental policies and procedures related to ensuring the confidentiality, integrity and availability of the Company's applications and computing resources.

QCRH SVP Chief Information Officer - The SVP Chief Information Officer ("CIO")is responsible for ensuring that appropriate policies, procedures and resources exist within the IS Departments to support this policy. The CIO is responsible for ensuring that user controls specified within vendor Service Control Organization ("SOC") reports (third-party security review) are properly implemented and reviewed on an annual basis. CIO is also responsible for monitoring their department budget.

QCRH VP Chief Technology Officer – The VP Chief Technology Officer ("CTO") is responsible for the day to day security function including monitoring for and responding to cybersecurity incidents. The CTO is responsible for maintaining security standards and processes and for implementing appropriate security technologies. The CTO is also responsible for submitting monthly cybersecurity reports to STORC. The CTO is also responsible for overall policy oversight, budget analysis and recommendations, and technology standards, selections, and strategy.

QCRH AVP IT Operations Manager – The AVP, IT Operations Manager is responsible for managing information technology for the Company. This position is responsible for managing the daily operations within the QCRH IS Department. Also, the position will act as technical consultant for information technology related issues for the Company.

QCRH AVP Security Administration Manager - This position will act as the primary point-of-contact for information security issues for the Company. In this capacity, the position will recommend, employ and enforce policy related to information security.

Senior Managers - Senior managers are responsible for applications specific to their departments. They are responsible for ensuring proper application security is applied, for staying current with application changes and upgrades, and for ensuring that personnel are trained on all software and hardware used by their department(s) as well as the contents of this policy. Additional guidance for the application security is provided within the Access Controls section of this policy. Senior managers should also ensure that personnel work directly with the IS Department to resolve department or user information technology (IT) issues. Senior managers are also responsible for ensuring an appropriate lead-time is provided to the IS Department for changes of any kind. At least a two-week notice must be provided for simple installs, department additions or changes, or equipment purchases so that appropriate resources may be adequately applied, while meeting project priorities. Managers may discuss exceptions to the two-week notice with the Chief Information Officer or AVP IT Operations Manager. The Director of Human Resources is responsible for ensuring that all new employees and temporary staff are trained on this policy and complete the "Statement of Understanding" upon employment.

QCRH SVP Chief Risk Officer - The SVP Chief Risk Officer ("CRO") is responsible for ensuring an annual review and report is submitted to the Board of Directors that includes results of an annual risk assessment, service providers' adherence to privacy requirements, results of compliance testing and security reviews, and any security breaches. The CRO is also responsible for ensuring that all employees receive annual information security training.

Board of Directors – Each entity's board of directors is ultimately held responsible by the regulators for oversight of information security and safeguarding of customer information. Therefore, each entity's board of directors should approve this policy annually. Each bank must name an Information Security Officer that is accountable for ensuring that annual reports are submitted to the board. As of the current date of the revision of this policy, entity boards responsible include the following:

- Quad City Bank & Trust ("QCBT")
- Cedar Rapids Bank & Trust ("CRBT")

- Rockford Bank & Trust ("RBT")
- M2 Lease Funds, Inc. ("m2")
- Community State Bank ("CSB")
- Springfield First Community Bank ("SFC")

Any banks or entities acquired or formed via de novo organization subsequent to this revision are held responsible for the same.

POLICY AND PRACTICES

Data and Equipment Ownership
Personal Computer (PC) equipment and software and all data residing on the Company's network and placed on Company PCs are the sole property of the Company. For the purposes of this policy, PC equipment also includes lap tops and mobile hand held devices (i.e., tablets, phones, smart phones, etc.) and printers. All Company-owned PC equipment is subject to the security parameters set forth in this policy.

Temporary employees and certain contractors may be provided with Company-owned equipment for services rendered at the discretion of the supervisor and the CIO or CTO. Consultants, defined as those who are providing professional services as an expert (i.e., IT consultants, accountants, attorneys, etc.) must use their own equipment, unless otherwise approved by the CIO or CTO. Contractors and consultants will need to complete and sign the QCRH Third Party Access Agreement, if access to company resources or the network is granted. Temporary employees must sign a Confidentiality agreement.

All Users are expressly prohibited from taking or transferring data for personal use. Furthermore, upon the end of employment or contract with the Company, users shall deliver promptly to the Company all materials relating to the Company and/or its customers, whether electronic or photographic, that are within the User's custody or control, or that are within the custody or control of anyone operating on the User's behalf. Under no circumstances shall information be downloaded or retained for personal or professional use upon termination of employment or contract.

Use of removable media (i.e., diskettes or writeable compact discs [CD/R or CD/RW]) or removable flash / jump drives [USB drives], digital frames and MP3 players that have the capacity to store data are strictly prohibited for use with computer equipment within the Company, and is enforced via Group Policy in Active Directory. The CRO and either the CIO or AVP IT Operations Manager must expressly authorize exceptions to this directive.

The use of any personal software on Company-owned PCs is prohibited. Any files downloaded via the Internet or otherwise placed onto Company-owned PC equipment become the property of the Company. Any such files may be used only in ways that are consistent with applicable licenses or copyrights.

Personal Use of Company Owned PC Equipment
A User's departmental manager may grant personal use of Company PC Equipment (inside or outside of Company office locations) under the following circumstances. Please note that all requirements and expectations of technology use within the Company remain applicable.

- *Educational Use* - The Company encourages employee educational advancement and allows a User to request use of a Company-owned PC for educational related work.

- *Community Involvement Use* - The Company encourages community involvement and allows a User to request use of a Company-owned PC for volunteer service. Example: a User requests use of a PC to organize and plan a fundraiser for a charity or community event.

Technology Standards
The QCRH Senior Technology Operations Risk Committee establishes standards for all hardware and software utilized throughout the Company. These standards are necessary in order to reap cost savings, control training costs, and facilitate monitoring and maintenance of equipment. All users are responsible for complying with these standards as described within this policy.

Any new software or hardware will be installed under the IS Department's direction to ensure system compatibility and virus protection. Only freeware that has been researched as safe and is approved by the CIO should be used on company-owned equipment.

Hardware and Software Purchase Authority
Certain individuals / Committees have authority to approve the purchase of technology-related hardware and software. These amounts are included in Appendix A to this policy, and may be updated periodically as needed by management.

In some cases, a business-case or cost justification will be required for presentation to the applicable BIC Council(s). All hardware/software changes must go through the Change Management process. Please see the Change Management Policy for further information.

Software Licensing
All software used within the Company will be licensed in the Company's name. The Company will maintain compliance with license agreements including named licenses and subscriptions. The IS Department or designated application owner is responsible for coordinating the licensing of all software and hardware, and will maintain licenses and original copies of software within the department. The IS Department should be contacted if additional licenses are needed.

Users must obey all copyright laws. Users are prohibited from creating or transmitting copies of Company-owned software.

Open Source Software
The use of open source software is not a generally accepted practice. However, the Company recognizes that some third parties rely on this technology to provide cost effective and adaptive software tools and services. The use of open source software will be considered in special cases where appropriate controls are present. In certain instances a Business Risk Acceptance (BRA) statement must approved by STORC before contracting or using any open source software that may not appropriately controlled.

Passwords and Password Security
Passwords are the first defense against unauthorized access to confidential computer information. Therefore it is critical to implement and properly protect passwords. At a minimum, passwords should contain at least eight alphanumeric characters, using both upper case and lower case characters, and at least one special character (such as "!", "@", "#", etc). Passwords should not be associated with anything personal including your name, relative's names, phone or social security numbers, birth date, etc.

Since secure and complex passwords can often be difficult to remember, the Company recommends employees use passphrases for their passwords. A phrase meets the requirements on length and complexity, but it is easier to remember.

For some ideas on coming up with a passphrase, consider the following examples:

- •"Fall2017" - This password is short and easy for you to remember. It is important to realize, this password would also be extremely easy to figure out or guess. This is an example of a VERY insecure password and should not be used.

- •"acan1itn!" - This password takes the first letter of each word in the phrase "Awesome cubs are number 1 in the nation!". This password is much more complex, but can be harder to remember.

- •"awesomecubsarenumber1?" This passphrase is long, complex, and easier to remember than the previous example.

Employees should use Password Vault software to organize their ID's and complex passwords/passphrases to various applications. The "vault" will store the information in a secured encrypted manner.

Passwords should be changed at least every 60 days, or changed immediately if a user suspects someone has gained knowledge of their password (this includes divulging passwords to the Help Desk). This is critical because each individual user is responsible for any access gained by the system using their password. Users should contact the Help Desk for assistance if passwords have been compromised. To assist in proper password security, the IS Department has established password parameters on the network that force certain password compliance, and security against invalid password attempts. Where possible, applications should have and follow similar password parameters.

Passwords should not be re-used, and passwords should never be shared with others or written down so that others may gain access to them. Passwords should never be disclosed in any way to any internal or external party. Employees should not use the "remember password" feature offered by some applications.

To be effective, information security should be an integral part of the technology and business planning process from initiation. To ensure that security requirements are defined and implemented, the IS Department should be notified of any new systems or applications before implementation.

Network Monitoring Notice

Users are connected to monitored proprietary systems (i.e., Company network, Signature). Law prohibits unauthorized access and use of the Company's network and computer systems. Violators may be subject to criminal and civil penalties. Use of a Company workstation infers acceptance of this policy. Remote monitoring is carried out to ensure compliance. Anyone using the system expressly consents to such monitoring.

Physical Security

Users are responsible for the physical safety of their computer as well as the safety of its software and the information it processes. Users are responsible for immediately reporting any violations, abuses or other security weaknesses to their supervisors and to the Help Desk. It is also the employee's responsibility to report to their supervisor any suspected tampering with their PC. Privacy screens should be used where needed on monitors.

While the system is set to automatically lock workstation screen savers after 20 minutes of inactivity, users should sign-off the network or lock their workstation (hit Ctrl-Alt-Del) if their PC will be unattended for any period of time. Remember, all individual users are accountable for all activity and access that occurs under their assigned log-on ID and password.

Employees will be provided with security devices (i.e., FOBs/card keys, keys), which allow for physical access to Company facilities based upon position responsibilities. It is the employee's responsibility to keep their security device secure. Lost or stolen devices should be reported immediately to the Security Officer for de-activation and re-issuance.

Movement of PC Equipment
Other than mobile devices, users are not permitted to move PC equipment without approval by authorized personnel. Moving or transferring a PC to another department or location must only be done with the approval and direction of the following personnel:

QCBT	EVP of Operations/Cashier
QCRH, m2	QCRH AVP IT Operations Manager
CRBT -	EVP of Operations / Cashier
RKFD –	EVP of Operations / Cashier
CSB -	SVP of Operations/Cashier
SFC-	SVP of Operations/Cashier

In some instances it will be necessary for the EVP/SVP of Operations/Cashier at the entities to consult with the QCRH AVP IT Operations Manager prior to moving hardware or making system changes. The QCRH AVP IT Operations Manager will be provided details relative to the move in order to update the IS Department's PC inventory tracking documentation.

Users should not allow vendors to remove any PC equipment from Company premises without ensuring that proper notification has been performed as stated previously.

Access Controls
The level of network or application security provided to each employee must be no more than that required to perform the job functions as defined in job descriptions. Requests for system access are to be submitted by the employee's supervisor or departmental manager on the electronic form (*Employee Access Form located on QNews*). Management may restrict access to the network during non-business hours.

Senior Managers are responsible for ensuring that access to significant applications used specifically in their departments is appropriate. To accomplish this, senior management will ensure that the following is completed for their applications:

- Access is reviewed at least annually and documented to ensure that access is appropriate and that all terminated employees have been removed from the system.
- If available, access exception reports are periodically reviewed
- Processes exist to remove access when employees are terminated, or to change access when employee duties or positions change
- The process for annual review, report review and access changes is documented for their department.

The Risk Management Department is responsible to ensure the annual access reviews for Signature and Nautilus are completed. The Risk Management Department will also ensure that someone is designated to

review Signature administrator activity and access changes. The IS department is responsible for ensuring semi-annual access reviews are completed for the network.

These reviews shall include reviews for stale or obsolete accounts, validate terminated employees have been removed and should include groups, group rights and individual access rights. Reviews will be properly documented

Data Back Up Procedures
The goal of data backup is to ensure that adequate information exists to restore information in the event of a machine malfunction, damage to programs, data or Company location. Users should save all information to their assigned depository (e.g., Sharepoint database, network directories, such as in "shared" files, or their personal folder on a network drive), where appropriate. Data stored in these locations is backed up daily by IS Department systems. Information saved locally to a PC (i.e., c:\ [hard disk]) or removable media (i.e., a:\ or d:\drives [jumpdrives, or otherwise]) is NOT backed-up by the IS Department. This is the responsibility of the end user to address with the IS Department if necessary

Internet and Email Usage, Social Networking
Internet access should be restricted to business-related purposes only, such as researching relevant business topics, and obtaining useful business information. The Company reserves the right to have in place and use, at any time, software and systems to monitor and record all Internet activities. No employee should have any expectation of privacy as to Internet usage. Users are also responsible for conducting themselves appropriately on the Internet. Inappropriate uses of the Company's network equipment, hardware, software, and Internet connectivity include the following:

- Uploading, downloading, or otherwise knowingly accessing or transmitting or sharing in any fashion:
  - Abusive, hateful, degrading, demeaning, derogatory or defamatory materials, information, or communications.
  - Pornographic, obscene, sexually explicit, indecent, or vulgar materials, information, or communications.
  - Any confidential records of the Company, its customers, or vendors without adequate authority and security to do so.
  - Any materials or programs, including access and registration codes, which are in violation of copyright protections.
  - Any trade secrets of the Company.
  - Resumes or other activities related to seeking employment outside of the Company.
  - Chain letters, distasteful jokes, or gambling of any nature (including sports or baby pools).
  - Any malware. (See section on Malware Protection for further information.)
  - Anything that would attempt to disable or overload any computer system or attempt to circumvent any system intended to protect the privacy or security of another user.
- Vandalizing, damaging, disabling, or gaining access to another entity's computer files or data.
- Engaging in any other activity restricted or prohibited by local, state, federal, or international laws.

The Company recognizes the growing use and significance of social media and respects an employee's choice to use it. However, it is the right and duty of the Company to protect itself from compliance, legal and operations risks, and ensure its customers are not harmed. Social media is defined as interactive online communication in which users can generate and share content through text, images, audio and/or video. Social media includes but is not limited to micro blogging sites (e.g., Facebook, Twitter, Tumblr, etc), forums, blogs, customer review websites and bulletin boards, photo and video sites (e.g., YouTube, Vimeo, Instagram), professional networking sites (e.g. Linked In), virtual worlds (e.g., Second Life, Warcraft) and

social games. The Company has established the following guidelines for responsible use of social media for all executive officers, board members and employees.

- Use of social media during work time hours for non-company business is prohibited.
- Employees, unless specifically authorized, cannot use employer-owned equipment, including computers, company-licensed software or other electronic equipment, nor facilities or company time, to conduct personal blogging or social networking activities.
- Employees are prohibited from acting as a spokesperson for the Company or posting comments as a representative of the Company, unless specifically authorized by the Company. All communications should be governed by the Media and Crisis Communications Policy and the Company's Social Media Networks Program and Procedures.
- Other than Linked-In, which is authorized for professional networking, employees cannot use their work email address for contact information on personal blogs or social networking sites. Employees using LinkedIn should refer communications to the company email address as soon as practical so that business conversations are appropriately recorded.
- Employees cannot post on personal blogs and social networking sites any advertisements or photographs of company products, nor sell company products or services without proper authorization. Only authorized postings regarding company products or services or intellectual property may be posted to personal networking sites.
- Employees may not publicly discuss or comment on clients, products, employees, whether confidential or not, outside company-authorized and monitored communications. This policy is not intended to prohibit or preclude employees from discussing or disclosing terms or conditions of employment on social media sites.
- Employees are expected to protect the privacy of the Company and its employees and clients and are prohibited from disclosing confidential employee and nonemployee information and any other proprietary (including copyrighted information or company-issued documents) and nonpublic information to which employees have access. Such information includes, but is not limited to customer information, trade secrets, operational information, security practices, financial information, vendor contracts and information, and strategic business plans.
- Employees cannot post on personal blogs or other sites the same, trademarks or logos belonging to the Company without permission from the Company.
- Unless specifically authorized within the QCRH Social Media Networks Program and Procedures, employees cannot post on personal blogs or social networking sites photographs of the Company, other employees, clients, vendors or suppliers, nor can employees post photographs of persons engaged in Company business or events.
- Employees cannot link from a personal blog or social networking site to the Company's internal or external website.
- Employees cannot use blogs or social networking sites to harass, threaten, discriminate or disparage against employees or anyone associated with or doing business with the Company.
- Employees involved with broker/dealer or investment advisor activities should follow the broker/dealer organizations policies and FIRREA regulations

Finally, it is generally recommended that employees not identify themselves as a Company employee on personal social networking sites or personal blogs. If you do choose to do so, please understand that some readers may view you as a spokesperson for the Company. Because of this possibility, you must state that your views expressed in your blog or social networking area are your own and not those of the Company, nor of any person or organization affiliated or doing business with the Company.

Company e-mail is a business communication tool and users are required to use this tool in a responsible, effective and lawful manner. The Company discourages the use of Company email for non-business communication. Emails should be used for communicating with co-workers, customers, vendors and regulators, or community volunteerism. Excessive use of the Company's email system for non-business use can result in disciplinary action, including termination.

The Company considers e-mail an important means of communication and recognizes the importance of proper e-mail content prompt replies, and conveying a professional image and delivering good customer service. There are also legal risks to email.

All e-mail and Instant Messaging ("IM") communications sent or received using bank systems and equipment are the property of the Company and as such, are not private, and may be monitored without prior notification. All e-mail communications may be subject to legal discovery and may be provided to opposing counsel in a legal, regulatory or government proceeding. Therefore, users should be aware of these legal risks and take the same care in drafting an e-mail as they would for any other communication. If you send or forward e-mails with any libelous, defamatory, offensive, racist or obscene remarks, you and the Company can be held liable for the following:

- Unlawfully forwarding confidential information.
- Unlawfully forwarding or copying messages without permission.
- Sending an attachment that contains a virus.

Depending on the content, e-mail and any attachments may be considered as records under the Company's record retention policy. To properly manage and protect these communications, the following requirements have been developed for the storage and retention of these messages:

- Messages should only be permanently saved and retained on company equipment. E-mail on portable devices such as phones or tablets should be deleted when read, if possible. Due to security concerns, mobile hot spots should not be used if company email is received on the device. This applies to both personal and company-owned devices.
- Phones that receive company email will be password protected.
- Messages sent or received should be deleted as soon as it is no longer required. (Exceptions apply for legal holds. Please see the Record Retention Policy for more information.) If messages are retained for ongoing business reasons, it should be moved to a personal archive folder, and then disposed of consistent with company retention policies.
- To preserve storage space, all e-mails located in the "deleted items" e-mail folder will be automatically deleted by the e-mail systems after 90 days, unless a legal hold has been issued.

Due to current limitations and risks, IM communications must be limited to internal communications only. It must not be used to communicate with external parties. Only Microsoft Skype for Business will be used for IM communications. No other IM communication software is allowed or should be downloaded. IM should be used for short messages. Lengthy conversations, complex information, or confidential information should be shared via email, over the phone, or in person.

Because texting cannot be recorded, texting should not be used to conduct business internally or with external clients and vendors. IM and text messages should not consist of anything that would be construed as a Company record. For example, IM or text messaging should not be used for any approvals or transaction-related activities. Rules and policies discussed above governing sexual/racial harassment, pornographic, obscene, sexually explicit, indecent, or vulgar materials, information, or communications, and discrimination also apply to IM and text content.

Video and Telephone Conference Calling
The Company uses Zoom for video and telephone conference calling.

- Only the meeting host will be able to record meetings or approve the recordation of meetings. If meetings are recorded, due to laws in certain states it is the host's responsibility to verbally notify participants of the meeting that it is being recorded.

File Sharing
The Company uses Sharefile for external file sharing. Sharefile enables users to manage external file sharing sites, and to share large volumes of documents with external parties, such as investors, legal teams, clients, and vendors. Access to Sharefile must be approved by a supervisor and Risk Management. Sharefile should not be used for personal use or benefit. External file sharing sites such as DropBox, Box.com are blocked by the Company. Access to these types of sites must be approved by a supervisor and Risk Management so that those with this type of access may be tracked and monitored.

Confidentiality of Information (Company and Customer)
Critical information, defined as information that contains non-public company or customer information, whether it resides on paper, the network, optical or other physical media (i.e., diskette, CDROM) or within departmental applications is considered a corporate asset and is confidential. As with any asset, protection from theft, damage, modification, and unauthorized use is necessary to the ongoing success of the Company. Therefore, Users are responsible for monitoring the usage of data and ensuring that any disclosure of data is properly authorized and done in a secure manner. Information should always be properly safeguarded and discussed and shared on a need-to-know basis only.

Any and all customer information that is shared with a customer, regulator or vendor should be properly secured. The following processes should be followed depending on the request and the format of the information:

- Users shall not use removable media (CD/DVD, or jumpdrive) to download or save data. Any requests for such downloads should be made through the IS Department, and be accompanied by senior management approval. The IS Department is authorized to disable the means to complete such downloads on any computer equipment.
- If removable media must be mailed, the media will be password protected and sent via certified or registered mail to provide a return receipt and audit trail.
- Users are responsible for storing files containing sensitive or confidential information in designated locations(ie. file shares, application databases) that are secured using the principle of least privilege, or a "need to know" basis. Storing files in locations that is widely accessible puts this information at a higher risk of exposure, both accidental and malicious. As an example, users should not store files containing confidential information in O:\Public.
- Faxed information must use a confidentiality disclosure.
- All employees are responsible for protecting sensitive information on their desk, in their office and on their computer screen when visitors are near or when going to lunch, a meeting or leaving for the day. Printed material will be kept, secured, out of sight or shredded. Examples of printed materials containing sensitive information include, but are not limited to, Signature screen prints, new account forms, CIP forms, loan applications, loan and credit files, financial statements, Signature reports, etc. Employees should empty personal shred bins each evening into the locked storage bins provided at each location.
- Information that is e-mailed must be setup with the IS Department with encryption and/or password protection prior to transmission.

- Some regulators have set up means for secure, encrypted transfer of information that they request for examinations or other communications. These mediums should be used at all times. Please contact the SVP Chief Risk Officer for information on how to use these communication/delivery channels.

Information should not be orally disclosed unless the customer has been properly authenticated. Social security number or a variation thereof or public information (telephone number, address, etc.) does NOT constitute proper authentication. It is extremely important that we authenticate our customers via information that only we and our customers know. Examples of this type of information include:

- The customer's established security word (if established – this is located in the CIF record under User Defined Fields)
- The customer's specific recent transaction information, (date of last deposit and amount, last payment amount and/or date, last advance and/or date).

If the customer is unable to provide this information, employees should forward the call to their account officer. If for some reason the account officer, cannot be reached ask the customer for the name of someone else in the bank that they might know that could authenticate them.

If the customer cannot be properly authenticated, information should not be disclosed. Employees should ask the customer to call back with the appropriate information. While this may be difficult, customers will comply once they are trained that they will need to have this information when they contact us.

Accidental disclosure of customer and/or corporate information could have a significant detrimental impact on the Company. The Company may face severe penalties from the SEC if non-public company information is provided to an outsider and proper disclosure of that information is not made to the rest of the Company's shareholders and investor community. In addition, disclosure of customer information may result in loss of customer confidence and loss of reputation. Whenever a user becomes aware that information is located in an incorrect area or that access is available to individuals not entitled to that access, the employee must immediately report this information to their supervisor and to the QCRH IS Department/SFC SVP-IT, and Incident Response procedures should be followed (See Incident Response Plan). The loss or theft of any mobile device (laptop or other device) containing customer or corporate data must be reported immediately.

Disposal of used or obsolete PC, scanner and copy equipment or software is prohibited by all personnel outside of the IS Department.

Encryption

Proven, standard technologies should be used for encrypting sensitive information (e.g., documents containing social security number and/or financial information) that is transmitted or transported outside of the QCRH network. All mobile devices and remote desktops will have encryption services installed on them and employees will be trained on the use of the encryption. Because email can contain sensitive information, outbound mail will be screened to detect information that should be encrypted. Any outbound email messages that are found to contain sensitive information will be automatically encrypted and then forwarded onto the original recipient. Where automated encryption is not possible, employees must manually encrypt emails.

All encryption technologies utilized must be approved by the IS Department. Users should be aware that the export of encryption technologies is restricted by the U.S. Government, and that there are restrictions on taking (importing) encryption technologies to other countries when traveling abroad. Before taking technologies into other countries, contact the IS Department to assist you in determining restrictions that may affect you.

Malware Protection
The Company requires the use of malware protection (anti-virus, -spyware, -ransomware, etc.) software on all computing systems. Generally, malware is designed to destroy or erase data or programs. Malware can replicate itself to other disks, programs or computers in the network without the user's knowledge, spreading their destructive affect. Malware may be spread through e-mails and their attachments, mass-distributed software, public domain programs, pirated software and programs obtained from computer clubs and computer bulletin boards, freeware, as well as storage devices such as jumpdrives, CDs/DVDs, digital picture frames, MP3 players, etc. Symptoms of malware may include a sudden volume of e-mails spreading throughout the network, a reduction in memory or disk space, disappearing programs, or display of unusual error or pop-up messages.

Spyware is a type of program that secretly gathers information about a user and/or the computer and sends it to an information collection point. Some spyware has the ability to install keystroke loggers, which may capture user IDs and passwords to internal systems. Some spyware is just adware that helps marketers to target consumers. However, a lot of spyware does not have the most honorable of intentions.

Malware poses a very real threat to the Company's computing environment and its ability to maintain confidential bank and customer information, as well as the Company's reputation with customers and the business community. Due to this exposure, the Company must take considerable measures to limit any risk. Therefore, the Company installs anti-malware on all PCs and the network, and scans all incoming and outgoing e-mail. Even though system protections are in place, the network is still vulnerable to new malware that can appear at any time.

Therefore, one of the best ways to prevent malware is not to open e-mails from unknown sources or e-mail attachments, especially when malware is being actively circulated. Recipients of e-mails from unknown sources with file attachments should delete the e-mail altogether, and not click on suspicious links. If necessary scan the attachment(s) first for malware. Users should contact the Help Desk if they require training or instruction on how to use the anti-malware software to scan e-mail attachments.

Freeware is another area that can introduce malware to the company's environment. Generally users are not allowed to download software on their computers without a network administrator's assistance. Only freeware that has been researched as safe and is approved by the CIO should be used on company-owned equipment. Users should be aware that free applications (apps) for mobile devices also can present a risk of malware. Users that use a personal mobile device to access company email are encouraged to exercise care in downloading freeware or free apps to their devices. Such applications should be researched and should come from well-known companies and should be free of malware that could affect the security of company email and systems.

In addition, Users should scan any "removable media", which includes but is not limited to jumpdrives and CDs/DVDs, prior to their use. Since the IS Department is the only authorized department to load new or updated software, the IS Department will scan any newly purchased software on removable media from vendors.

For those Users with laptops, only approved, Company-sponsored wireless access points should be used. Wireless at "hot spots", hotels, etc, are not secured and should not be used because these areas are prime places for malware to be downloaded to computers without user knowledge. To help prevent the usage of unsecured wireless access, the standard wireless access on the laptops has been disabled. Please work with your supervisor and/or the IS Department to obtain secured wireless access.

Users who suspect their terminal or computer system has malware, or has otherwise been improperly accessed or used, should immediately call the Help Desk. Under no circumstances should the User continue to work on their computer. The employee should not turn off the computer or delete suspicious files. Leaving the computer in the condition it was in when the security incident was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem. The IS Department will follow the Incident Response Plan and procedures, and will attempt to remove the malware and attempt to determine its source. Whenever possible, the User will be issued a temporary laptop or computer to use until the original computer is cleaned of the malware.

Remote Access

The definition of Remote Access is any access to the QCR Holdings, Inc. network through a controlled network, device (PC), or other medium. Remote Access is used primarily for those Users that require access to the network while working away from the office or in cases where software applications require remote system capabilities. Remote Access will be achieved by implementing telecommunications connections that include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, wireless access point (WAP) or cable modem. Employees connecting to the QCRH network through a VPN connection are required to use multifactor authentication.

Supervisors/Managers that determine specific staff require Remote Access will complete a request for Remote Access through the Employee Access Form located on QNews and submit it to the QCRH IS Department/SFC SVP-IT for review and approval by the SVP CRO, and the CIO or the CTO. Remote Access users are required to ensure that their Remote Access connection is given the same consideration as the user's on-site connection to the QCR Holdings, Inc. network. The remote user (employee) bears responsibility for the consequences should the Remote Access be misused. In addition remote access employees must give the same considerations to the security of printed materials, including proper disposal (shredding).

Mobile Device Management

Company-owned devices

The Company may provide devices to users in certain positions as a productivity tool for business use. The Company reserves the right to terminate services for non-use, limited business use, or excessive personal use. The Company reserves the right to dictate the carriers and the plan used, which may change from time to time. Mobile device care is the responsibility of each mobile device user. Failure to adhere to the guidelines listed below may result in personal liability and/or retraction of device privileges. Users are responsible for maintaining usage within the carrier plan parameters.

Users of Company-owned mobile devices are also responsible for:

- Protection of the device from theft, damage, abuse, and unauthorized use.
- Reporting lost, stolen, damaged, destroyed, compromised or non-functional devices to the Help Desk, immediately, or as soon as practical. Lost or stolen devices will be locked and disabled.
- Abiding by the laws governing use of mobile cell phones and/or smart phones while driving (e.g. hands-free use and/or texting.
- Maintaining the original device operating system and keeping the device current with security patches and updates, as released by the manufacturer. The user will not "Jail Break" the device (installing software that allows the user to bypass standard built-in security features and controls).
- Not sharing the device with other individuals or family members, due to the business use of the device (access to Company emails)

- Being aware of, and taking proper security measures to protect the mobile device from malware and unauthorized access. Users will be held responsible in the event malware is introduced to the Company environment.

The Company will deploy mobile device management (MDM) software to manage security around mobile devices. The Company has chosen not to deploy features that interfere with the functionality of the devices. The Company has deployed MDM functionality that will secure company email and calendars to ensure that information is encrypted. The Company reserves the right to deploy additional security features at its discretion.

As noted above, users of Company-owned devices do not have a right, nor should they have the expectation, of privacy while using Company-owned equipment at any time, including accessing the Internet and using e-mail and voice communications. To the extent that employees wish that their private activities remain private, they should avoid using the device for limited personal use. By acceptance of the Company-owned device, employees imply their consent to disclosing and/or monitoring of device usage, including the contents of any files or information maintained or passed-through that device.

Bring-Your-Own-Device

Generally, the Company allows users to access and sync business emails, calendars and contacts with a personally-owned mobile device. Users should obtain approval from their supervisor for accessing the Company's email with a personally-owned mobile device. Users should not have access to the network or other computing resources other than email with personally-owned devices.

Users of personally-owned mobile devices that access Company resources are responsible for the same measures as bulleted above for Company-owned devices. The Company reserves the right to deploy MDM software on the device for the purposes noted above. In the event that MDM is not deployed to the device, the Company will enforce strong password protection to access the device.

Electronic Signatures

The Company has a separate policy regarding the use of electronic signature software. Only certain software meeting that criteria should be used for documents requiring a signature that are deemed to be a record of the company. Please refer to the Electronic Signature Usage Policy for requirements.

Third Party Access

Vendors or other third parties will not be allowed to physically connect to any Company network unless there is an engagement/agreement with the Company and they have completed a QCRH Third Party Access Agreement, which requires them to have appropriate information security practices, and confidentiality measures in place before access can be provided. This applies to any access, including but not limited to the demonstration of solutions, or fulfilling contractual requirements such as troubleshooting systems.

Training

Ongoing training pertaining to this policy for existing employees and training for new employees and temporary and contracted workers will be performed at least annually to ensure compliance with each department's respective procedures.

Policy Enforcement

Violations of this policy may result in disciplinary actions. Depending on the severity or frequency of the violations, this may include the following:

- Written warnings for policy violations will be placed in personnel file in HR.

- Suspension/termination of Internet or PC privileges. This could then result in a position/function reassignment, and the employee's compensation package may be affected.
- Termination of employment.
- Personal liability under applicable local, state, federal, or international laws, resulting in civil or criminal penalties.

REGULATORY REFERENCE

- Gramm-Leach-Bliley Act
- Interagency Guidelines Establishing Standards for Safeguarding of Customer Information (12 CFR 208 – Reg H, and 12 CFR 225)
- FIRREA
- National Labor Relations Act (Social Media Use)

RELATED POLICIES AND PROCEDURES

Users should also be familiar with the following:

- QCRH Code of Conduct and Ethics Policy,
- QCRH Cyber/Information Security Program,
- QCRH Incident Response Plan,
- QCRH Change Management Policy,
- QCRH Vendor Management Policy,
- QCRH Record Retention Policy,
- QCRH Security Policy,
- QCRH Social Media Networks Program and Procedures,
- QCRH Media and Crisis Communications Program,
- Disaster Recovery Plans
- Business Continuity Plans, and
- QCRH Cell-phone Reimbursement Policy
- QCRH Electronic Signature Usage Policy

The IS department will maintain departmental policies and procedures for managing systems and information security.

RENEWAL/REVIEW

This policy should be reviewed and approved annually by STORC. The SVP CRO may make periodic changes to the policy based upon emerging technologies or emerging issues with technology as it applies to the Company. Any periodic changes will be approved by the CIO, and communicated to employees via e-mail.

Modification History

Date:	Details:
January 2005	Combined e-mail usage policy, technology policy elements pertaining to end users, and the Information Security policy.
March 2006	Added bank board responsibilities, and references to other policies within the Information Security Program.
May 2006	Added prohibition of users taking data upon termination of employment, and prohibition of removable media.
February 2007	The Policy was amended to reflect the addition of the Chief Technology Officer position, replacing the roles and responsibilities of the SVP of Information Services. Changes were made to the monetary limits associated with the purchase of Technology hardware and software at enterprise and entity levels.
March 2007	Added FWBT references. Moved purchasing authority to Appendix A.
February 2008	Revised Contact Person. Updated approval Title for moving PC's for QCBT sites.
July 2008	Added responsibility for annual access reviews. Included screen saver lockouts after 20 minutes of inactivity, and guidance for encryption. Provided guidance for loss of mobile devices and spyware. Replaced logo.
August 2009	Updated titles, removed references to the QCRH Board Tech Committee, updated email usage section.
June 2010	Added information regarding proper customer authentication and social networking. Moved email sections.
July 2011	Minor updates and clarification, including: • Printing of emails and their attachments remotely - information should still be secured, shredded and otherwise securely maintained. • Personal phones used to access company email need to be password protected • Require shred bins to be emptied every night
June 2012	Updated approval limits
July 2013	Included guidance on freeware, updated confidentiality paragraph regarding "clean" desk. Added guidance on use of "hot spots" for devices with company email.
July 2014	Updated titles, included guidance on BYOD (non-bank equipment) and Mobile Device Management. Added additional existing policies to the list of related policies and procedures.
June 2015	Revision included additions for social networking which contemplate DOL rules and FIRREA, changes for electronic sign off of the policy, third party access, and title changes. Also updated password guidance.
June 2016	Title changes, blog/social networking postings change
October 2016	Add in CSB
July 2017	Added VP CTO responsibilities, updated Technology Standards to include VP CTO. Added content regarding storage of sensitive files on the network. Added content regarding Open Source Software. Appendix A - added VP CTO purchase authority. Replaced the term malware for viruses, spyware, etc. Updated statement of understanding for electronic "agreement".
June 2018	Updated titles. Replaced VP Information Services Officer with AVP, IT Operations Officer. Updated VP & CTO approvals for remote access. Added AVP, Security Administration Manager to notification requirements.

October 2018	Added IM policy, SFC
June 2019	Added content regarding video conferencing, file sharing software, texting. Updated responsibilities for STORC, BIC. Reflected committee title changes. In anticipation of SFC conversion and network implementation, incorporated SFC into current processes, eliminating need to call them out separately.

QCR HOLDINGS, INC.

a relationship driven organization™

www.qcrh.com

Technology Usage and Information Security Policy - Statement of Understanding

I have read and fully understand the terms of this policy and agree to abide by them.

I will comply with all technology standards and software licensing terms.

I will use secure passwords/passphrases and protect them from unauthorized use. I will not share my passwords/passphrases. I will safeguard all confidential information and secure my workstation when not in use.

I will keep Company and customer information secure. I will not send Customer or Company information via e-mail unless I know the information has been secured via password or encryption software. I will not save confidential information to network folders that are not designated to retain confidential information. I will not misuse file sharing software.

I will ensure that critical information is saved to a network location that is backed up. I will protect information and computing systems by scanning for malware as per this policy.

I realize that the Company may use monitoring software at any time and may record the Internet address of any site I visit. The Company may keep a record of any network/internet activity in which I transmit or receive any kind of message and/or file. I acknowledge that any message I send or receive may be recorded and stored in an archive file. These archives may be accessed by law enforcement agencies when required legal processes are executed.

I will follow the requirements of the Company's social networking policy, and will not post to personal sites while I am supposed to be working. I will not solicit or conduct Company business via a personal site, or list my Company email address as contact information unless formally authorized to do so. I will not post information, photographs or other items to a personal site pertaining to work, fellow employees, clients, or others doing business with the Company unless formally authorized to do so.

I will notify my supervisor, the QCRH Information Services Department or a Senior Manager of any potential issues or violations of this policy.

I know that any violation of this policy could lead to disciplinary action, suspension, dismissal or applicable criminal prosecution.

_____ _____

Signature Date

_____

Printed Name

*This policy may be periodically updated. Updates will be communicated to employees via e-mail. Employee will agree to the Statement of Understanding via BVS annually.

Technology Usage and Information Security Policy
Appendix A - *Hardware and Software Purchase Authority*

***Cedar Rapids Bank & Trust (CRBT) - EVP of Operations / Cashier*……...Up to $50,000**
Quad City Bank & Trust – QCRH EVP Chief Operations Officer/Cashier, QCBT CFO…Up to $50,000
***Rockford Bank & Trust (RKFD) – EVP of Operations / Cashier*…….……..Up to $50,000**
***Community State Bank(CSB) - SVP Retail Banking/Cashier*…….……..Up to $50,000**
***Springfield First Community Bank (SFC) – SVP CFO*…….……..Up to $50,000**
***QCRH VP, Chief Technology Officer*……...……Up to $50,000**
***QCRH SVP, Chief Information Officer*……...……..Up to $250,000**
***QCR Holdings, Inc (QCRH) President*……...……..Up to $250,000**
***QCRH CEO*……..Up to $250,000**

Anything above the established limits require two of the above signatures.

Hardware and Software Purchase Procedures

Users - Users that have a specific Technology related need(s) should contact their Senior Manager.

Senior Managers - *For projects less than $10,000*, Senior Managers are requested to complete and submit the Hardware/Software Request Form to the IS Department for approval.

For projects in excess of $10,000, Senior Managers are requested to complete and submit a *Capital Expenditure Request* (CER) form to the Chief Information Officer.