RRAR Cyber Security Policy

This policy establishes clear guidelines and standards for protecting sensitive data and digital assets to ensure confidentiality, data integrity, and availability.

Key points about a cybersecurity policy for a one-person organization:

- **Data protection:** Security measures to be in place to protect computers, and other IT systems. This includes, but is not limited to:
    - Using strong passwords
    - Keeping anti-virus software up to date
    - Separating business and personal email accounts
    - Locking file cabinets and office doors
- **Safe practices:** using strong passwords with multi-factor authentication, regularly updating software, securing your Wi-Fi network, backing up important data frequently, being vigilant about phishing emails, using a reputable antivirus program, and limiting access to sensitive data on personal devices, while also considering the potential risks of storing critical information on a single computer.
    - Strong passwords and multi-factor authentication: Create complex passwords for all online accounts and enable multi-factor authentication wherever possible to add an extra layer of security.
    - Software updates: Regularly update operating system, applications, and antivirus software to patch security vulnerabilities.
    - Secure Wi-Fi network: Ensure the Wi-Fi network is password protected and uses a strong encryption protocol like WPA2 or WPA3.
    - Data backups: Regularly back up important data to an external hard drive or cloud storage service to protect against data loss in case of a system failure or cyberattack.
    - Phishing awareness: Be cautious of suspicious emails, links, or attachments, and never click on links or download files from unknown senders.
    - Antivirus software: Install a reputable antivirus program and keep it updated to detect and block malware.
    - Limited access to sensitive data: If possible, store sensitive data on a separate, dedicated device or in a secure cloud storage service, limiting access to personal devices.
    - Device security:
        - Use a screen lock on your devices.
        - Encrypt sensitive data stored on your devices.
        - Consider using a dedicated work profile on your phone or tablet to separate personal and business data.
        - Be mindful of public Wi-Fi: Avoid accessing sensitive information when connected to public Wi-Fi networks.
    - Cybersecurity awareness training: Even as a single-person business, stay informed about current cyber threats and best practices through online resources or short training courses.

RRAR Cyber Security Policy

- **Incident response:** Steps to take in case of a potential security breach, including reporting procedures.
    - **Detection and Analysis:**
        - Monitor for anomalies: Be alert for unusual activity like unexpected emails, system crashes, or unauthorized access attempts.
        - Report suspicious activity: Immediately report any potential incidents to your designated contact or external support provider.
        - Identify the nature of the incident: Try to understand the type of attack, its impact, and the affected systems.
    - **Containment and Eradication:**
        - Isolate affected systems: If possible, disconnect the compromised system from the network to prevent further spread.
        - Change passwords: Reset passwords for compromised accounts.
        - Seek external assistance: If the incident is complex, contact a cybersecurity professional for further guidance and support.
    - **Recovery and Post-Incident Activity:**
        - Restore data from backups: If necessary, restore data from your backups.
        - Review and update security practices: Analyze the incident to identify weaknesses and implement necessary security improvements.
        - Document lessons learned: Record details of the incident and actions taken to improve future responses.

• FBI Cybercrime https://www.fbi.gov/investigate/cyber

• FBI Internet Crime Complaint Center (IC3) https://www.ic3.gov/

• FBI Ransomware https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware

Email Policy

Overview

E-mail at Reelfoot Regional Association of REALTORS® (RRAR) must be managed as valuable and mission critical resources. Thus, this policy is established to:

- Create prudent and acceptable practices regarding the use of information resources
- Educate individuals who may use information resources with respect to their responsibilities associated with such use
- Establish a schedule for retaining and archiving e-mail

Audience

This policy applies equally to all individuals granted access privileges to any RRAR information resource with the capacity to send, receive, or store electronic mail.

Legal

Individuals involved may be held liable for:

- Sending or forwarding e-mails with any libelous, defamatory, offensive, racist, or obscene remarks
- Sending or forwarding confidential information without permission
- Sending or forwarding copyrighted material without permission
- Knowingly sending or forwarding an attachment that contains a virus

Policy Details

Corporate e-mail is not private. Users expressly waive any right of privacy in anything they create, store, send, or receive on RRAR's computer systems. RRAR can, but is not obliged to, monitor emails without prior notification. All e-mails, files, and documents – including personal e-mails, files, and documents – are owned by RRAR, may be subject to open records requests, and may be accessed in accordance with this policy.

Incoming email must be treated with the utmost care due to the inherent information security risks. An anti-virus application is used to identify malicious code(s) or files. All email is subjected to inbound filtering of e-mail attachments to scan for viruses, malicious code, or spam. Spam will be quarantined for the user to review for relevancy. Introducing a virus or malicious code to RRAR systems could wreak havoc on the ability to conduct business.

Anti-spoofing practices have been initiated for detecting spoofed emails. Employees should be diligent in identifying a spoofed email. Incoming emails are scanned for malicious file attachments. If an attachment is identified as having an extension known to be associated with malware, or prone to abuse by malware or bad actors or otherwise poses heightened risk, the attachment will be removed from the email prior to delivery.

Email rejection is achieved through listing domains and IP addresses associated with malicious actors. Any incoming email originating from a known malicious actor will not be delivered. Any email account misbehaving by sending out spam will be shut down. A review of the account will be performed to determine the cause of the actions.

E-mail is to be used for business purposes and in a manner that is consistent with other forms of professional business communication. All outgoing attachments are automatically scanned for virus and malicious code. The transmission of a harmful attachment can not only cause damage to the recipient's system, but also harm RRAR's reputation. The following activities are prohibited by policy:

- Sending e-mail that may be deemed intimidating, harassing, or offensive. This includes, but is not limited to: abusive language, sexually explicit remarks or pictures, profanities, defamatory or discriminatory remarks regarding race, creed, color, sex, age, religion, sexual orientation, national origin, or disability.
- Using e-mail for conducting personal business.
- Using e-mail for the purposes of sending SPAM or other unauthorized solicitations.
- Violating copyright laws by illegally distributing protected works.

- Sending e-mail using another person's e-mail account, except when authorized to send messages for another while serving in an administrative support role.
- Creating a false identity to bypass policy.
- Forging or attempting to forge e-mail messages.
- Using unauthorized e-mail software.
- Knowingly disabling the automatic scanning of attachments on any RRAR personal computer.
- Knowingly circumventing e-mail security measures.
- Sending or forwarding joke e-mails, chain letters, or hoax letters.
- Sending unsolicited messages to large groups, except as required to conduct RRAR business.
- Sending excessively large messages or attachments.
- Knowingly sending or forwarding email with computer viruses.
- Setting up or responding on behalf of RRAR without management approval.

All confidential or sensitive RRAR material transmitted via e-mail, outside RRAR's network, must be encrypted. Passwords to decrypt the data should not be sent via email.
E-mail is not secure. Users must not e-mail passwords, social security numbers, account numbers, pin numbers, dates of birth, mother's maiden name, etc. to parties outside the RRAR network without encrypting the data. All user activity on RRAR information system assets is subject to logging and review. RRAR has software and systems in place to monitor email usage.
E-mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of RRAR, unless appropriately authorized (explicitly or implicitly) to do so. Users must not send, forward, or receive confidential or sensitive RRAR information through non-RRAR email accounts. Examples of non-RRAR e-mail accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, and e- mail provided by other Internet Service Providers (ISP). Users with non-RRAR issued mobile devices must adhere to the Personal Device Acceptable Use and Security Policy for sending, forwarding, receiving, or storing confidential or sensitive RRAR information.

Incidental Use

Incidental personal use of sending e-mail is restricted to RRAR approved users; it does not extend to family members or other acquaintances. Without prior management approval, incidental use must not result in direct costs to RRAR. Incidental use must not interfere with the normal performance of an employee's work duties.
No files or documents may be sent or received that may cause legal liability for or embarrassment to RRAR. Storage of personal files and documents within RRAR's IT systems should be nominal.

Email Retention

- Messages are retained for 36 months. Emails older than 36 months are subject to automatic purging.
- Deleted and archived emails are subject to automatic purging.
- Appointments, Tasks, and Notes older than the retention period are subject to automatic purging.

Email Archive

- Only the owner of a mailbox and the system administrator has access to the archive.
- Messages will be deleted from the online archive 36 months from the original send/receive date.

RRAR Acceptable Use of Information Systems Policy

Data, electronic file content, information systems, and computer systems at Reelfoot Regional Association of REALTORS (RRAR) must be managed as valuable organization resources.

This Policy is not to impose restrictions that are contrary to RRAR's established culture of openness, trust, and integrity. The Policy is committed to protecting RRAR's authorized users, partners, and the company from illegal or damaging actions by individuals either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including, but not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and File Transfer Protocol (FTP) are the property of RRAR.

These systems are to be used for business purposes in serving the interests of RRAR and of its clients and members during normal operations.

Effective security is a team effort involving the participation and support of every RRAR employee, member, volunteer, and affiliate who deals with information and/or information systems.

It is the responsibility of every computer user to know these guidelines and to conduct activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at RRAR. These rules are in place to protect the authorized user and RRAR. Inappropriate use exposes RRAR to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct RRAR business or interacts with internal networks and business systems, whether owned or leased by RRAR, the employee, or a third party.

All employees, members, volunteer/directors, contractors, consultants, temporaries, and other workers at RRAR, including all personnel affiliated with third parties, are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with RRAR policies and standards, local laws, and regulations.

Policy Detail

Ownership Of Electronic Files

All electronic files created, sent, received, or stored on RRAR owned, leased, or administered equipment or otherwise under the custody and control of RRAR are the property of RRAR.

Privacy

Electronic files created, sent, received, or stored on RRAR owned, leased, or administered equipment, or otherwise under the custody and control of RRAR are not private and may be accessed by RRAR IT employees at any time without knowledge of the user, sender, recipient, or owner.
Electronic file content may also be accessed by appropriate personnel in accordance with directives from the association executive.

RRAR Acceptable Use of Information Systems Policy

General Use And Ownership

Authorized users are accountable for all activity that takes place under their username. Authorized users should be aware that the data and files they create on the corporate systems immediately become the property of RRAR. Because of the need to protect RRAR's network, there is no guarantee of privacy or confidentiality of any information stored on any network device belonging to RRAR.

For security and network maintenance purposes, authorized individuals may monitor equipment, systems, and network traffic at any time.

RRAR reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

RRAR reserves the right to remove any non-business related software or files from any system. Examples of non-business related software or files include, but are not limited to; games, instant messengers, pop email, music files, image files, freeware, and shareware.

Security And Proprietary Information

All mobile and computing devices that connect to the internal network must comply with this policy and the following policies:

- Account Management
- Anti-Virus
- Owned Mobile Device Acceptable Use and Security
- E-mail
- Internet
- Safeguarding Member Information
- Personal Device Acceptable Use and Security
- Password
- Cloud Computing
- Wireless (Wi-Fi) Connectivity
- Telecommuting

System level and user level passwords must comply with the Password Policy. Authorized users must not share their RRAR login ID(s), account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authentication purposes.

Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

Authorized users may access, use, or share RRAR proprietary information only to the extent it is authorized and necessary to fulfill the users assigned job duties.

All PCs, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 60 minutes or less.

All users must must log-off, or restart (but not shut down) their PC after their shift.

RRAR Acceptable Use of Information Systems Policy

RRAR proprietary information stored on electronic and computing devices, whether owned or leased by RRAR, the employee, or a third party, remains the sole property of RRAR. All proprietary information must be protected through legal or technical means.

All users are responsible for promptly reporting the theft, loss, or unauthorized disclosure of RRAR proprietary information to their immediate supervisor.

All users must report any weaknesses in RRAR computer security and any incidents of possible misuse or violation of this agreement to their immediate supervisor.
Users must not divulge dial-up or dial-back modem phone numbers to anyone without prior consent.

Authorized users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan Horse codes.

Unacceptable Use

Users must not intentionally access, create, store, or transmit material which RRAR may deem to be offensive, indecent, or obscene.

Under no circumstances is an employee, member, volunteer/director, contractor, consultant, or temporary employee of RRAR authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing RRAR-owned resources.

System And Network Activities

The following activities are prohibited by users, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by RRAR.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution from copyrighted sources, copyrighted music, and the installation of any copyrighted software for which RRAR or the end user does not have an active license is prohibited. Users must report unlicensed copies of installed software to RRAR.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a RRAR computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- Attempting to access any data, electronic content, or programs contained on RRAR systems for which they do not have authorization, explicit consent, or implicit need for their job duties.
- Installing any software, upgrades, updates, or patches on any computer or information system without the prior consent of RRAR.
- Installing or using non-standard shareware or freeware software without RRAR IT approval.
- Installing, disconnecting, or moving any RRAR owned computer equipment and peripheral devices without prior consent of RRAR.
- Purchasing software or hardware, for RRAR use, without prior IT compatibility review.
- Purposely engaging in activity that may;
    - degrade the performance of information systems;
    - deprive an authorized RRAR user access to a RRAR resource;
    - obtain extra resources beyond those allocated; or
    - circumvent RRAR computer security measures.

- Downloading, installing, or running security programs or utilities that reveal passwords, private information, or exploit weaknesses in the security of a system. For example, RRAR users must not run spyware, adware, password cracking programs, packet sniffers, port scanners, or any other non- approved programs on RRAR information systems.
- Circumventing user authentication or security of any host, network, or account.
- Interfering with, or denying service to, any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

Access to the Internet at home, from a RRAR-owned computer, must adhere to all the same policies that apply to use from within RRAR facilities. Authorized users must not allow family members or other non-authorized users to access RRAR computer systems.

RRAR information systems must not be used for personal benefit.

Incidental Use

As a convenience to the RRAR user community, incidental use of information systems is permitted.
The following restrictions apply:

- Authorized Users are responsible for exercising good judgment regarding the reasonableness of personal use. Immediate supervisors are responsible for supervising their employees regarding excessive use.
- Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, and so on, is restricted to RRAR-approved users; it does not extend to family members or other acquaintances.
- Incidental use must not result in direct costs to RRAR without prior approval of management.
- Incidental use must not interfere with the normal performance of an employee's work duties.
- No files or documents may be sent or received that may cause legal action against, or embarrassment to, RRAR.
- Storage of personal email messages, voice messages, files, and documents within RRAR's information systems must be nominal.
- All messages, files, and documents — including personal messages, files, and documents — located on RRAR information systems are owned by RRAR, may be subject to open records requests, and may be accessed in accordance with this policy.

Review and Acceptance

All RRAR staff is responsible for review and acceptance of *Policy 1: Acceptable Use* upon starting work at RRAR (see Exhibit A).

New employee onboarding and training shall include this Policy 1 at a minimum, and in addition to all other applicable training and orientation material, and instructions for acceptance shall be provided at that time. Signed acceptance will be received and retained by RRAR.

RRAR Acceptable Use of Information Systems Policy

Exhibit A

[This exhibit is a copy of the current Acceptable Use of Information Systems receipt.]

Receipt of Acceptable Use of Information Systems
Please sign this form and return it to Information Systems

I have received a copy of the RRAR Acceptable Use of Information Systems Policy.
I understand the information in the Acceptable Use of Information Systems policy is a summary only, and it is my responsibility to review and become familiar with all of the material contained in the Comprehensive IT Policy.

I understand the most updated policies and Bylaws will always be located on the intranet for my reference, and it will be my responsibility to review the policies and Bylaws as they are updated.

I further understand the content of the Comprehensive IT Policy supersedes all policies previously issued. I also understand that RRAR may supersede, change, eliminate, or add to any policies or practices described in the Comprehensive IT Policy.

My signature below indicates that I have received my personal copy of the Acceptable Use of Information Systems Policy and it will be my responsibility to review the Comprehensive IT policies as they are updated.

User Signature_____
User Name (printed)_____
Date_____

***Retain one copy of this Receipt for your records and return the other copy to Information Systems.*

RRAR Privacy Policy

We recognize the importance of protecting the personal information you provide at Web sites owned or controlled by the NATIONAL ASSOCIATION OF REALTORS® (NAR).

1. RRAR gathers the following types of information needed to process your transactions, fulfill your requests, and maintain our membership records:

- Contact information you provide (for example, your personal and business addresses, phone and fax numbers, firm affiliations and titles).
- Tracking information which our Web server automatically recognizes each time you visit one of our sites or communicate with us by email (for example, your domain name, your email address, and what pages you visit).
- Information you volunteer, via applications or surveys.

2. RRAR uses this information to:

- Improve and customize the content and layout of our sites and other communications tools.
- Notify you of updates to our sites.
- Notify you of relevant products and services.
- Notify you of upcoming events and programs.
- Track usage of our sites.
- Assist the state REALTOR® associations and the National Association of REALTORS® in membership tracking and for their use for purposes similar to those listed above.

3. Email contact information. RRAR does not share, sell, or trade email addresses. RRAR may use your email address to directly send you information and may provide you with online informational or marketing messages with other communications to which you have subscribed.

4. Other forms of contact information. Forms of contact information other than email address (for example, street address) may be listed in the membership directories. RRAR will not share, sell or otherwise provide this contact information about you.

5. Credit information that you and credit authorizers provide when you make payments by credit card or electronic check for products, dues or other services via the REALTOR® Electronic Commerce Network or Autobooks will only be used to process the transactions you request. This information will be provided to and maintained by reputable credit reporting databases, but will never be sold, shared or provided to other third parties.

6. RRAR follows generally accepted standards to protect the information it collects and makes available via its Web sites. RRAR tests their security procedures and modifies them as new technologies become feasible.

7. You may request to edit your personal contact information by contacting RRAR.

8. Do-Not-Track Disclosure: Some browsers have a "Do Not Track" feature that allows you to communicate to websites that you do not want to have your online activities tracked. Our system does not respond to Do Not Track requests or headers from some or all browsers at this time.