■ Section 3 - Communications

Scope: ***Electronic Communications & Information Systems Acceptable Use Policy***

Approved by Regional Governing Board Date: 4-11-11

PRACTICE / POLICY

Region V Systems owns its information systems and the data transmitted and stored within it. Employees should have no expectation of privacy or confidentiality of data stored on the organization's owned devices. This includes all incoming and outgoing electronic messages—both e-mail and voice systems. Employees who access any organizational data on Region V's network consent to be monitored for adherence to this Electronic Communications & Information Systems Acceptable Use Policy.

Information systems and electronic communication are an integral part of business at Region V Systems. For the purposes of this policy, "electronic communication and information systems" are defined to include but are not limited to: organizational servers, computers, landlines, cell phones, smartphones, flash drives, fax machines, or other technology-related resources, and the method used to communicate data stored on these devices electronically.

"ISA" (Information Systems Administration) is defined as the staff and resources Region V employs to administer its information systems. Region V has made a substantial investment in such resources to create these systems. Policies and directives have been established in order to:

- Protect this investment.
- Safeguard the data contained within these systems and protect confidential information.
- Reduce business and legal risk.
- Protect Region V Systems' reputation.
- Maintain productivity and high levels of employee service.
- Ensure that employees abide by local, state, and federal laws.

Employees using Region V Systems' information systems are representing Region V and are responsible for ensuring that the Internet and information systems are used in an effective, ethical, and lawful manner.

Region V Systems has an affirmative duty to report any illegal activity to appropriate law enforcement personnel. If it is discovered that illegal activity is or has taken place using Region V's information systems, lawful and appropriate procedures will be followed to protect the investment and reputation of the organization.

Region V Systems' Electronic Communications & Information Systems Acceptable Use Policy is in accordance with applicable federal, state, and provincial laws.

Access to certain information systems is provided as a necessary and useful tool to complete the job functions of Region V Systems' employees. With this access comes an inherent risk as the Internet and related communication systems can be saturated with security threats and inappropriate material.

The following procedures have been established for using Region V's information systems to protect both the organization and the employee.

PROCEDURES

Management and Supervisor Responsibilities

Management and supervisors must:

- Ensure that all personnel are aware of and comply with these policies.
- Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe these policies.
- Communicate with ISA staff when these policies are believed to have been breached or compromised so appropriate measures may be taken.

General Acceptable Use

1. Being responsible for the content of all text, media, or images that employees place or send over the Internet. All communications should have the employee's name attached and should be completed using professional e-mail etiquette with proper punctuation and spelling.
2. Knowing and abiding by Region V's Electronic Communications & Information Systems Acceptable Use Policy dealing with security and confidentiality of the organization's records. If it is necessary to transmit confidential information, employees are required to take steps reasonably intended to ensure that information is delivered to the proper person who is authorized to receive such information for a legitimate use and in accordance with HIPAA requirements. Also see "Consumer Confidentiality Expectations" section below.
3. Using web browsers to obtain business information.
4. Accessing databases, servers, and websites for information as needed and required for each employee's respective job.
5. Using e-mail for business communication, contacts, scheduling, and other business-related purposes. Using Region V's standard confidentiality message on all newly composed (originating) e-mail messages.
6. Using voice systems to relay and retrieve communications from business-related contacts.
7. Using office machinery as related to the duties and scope of an employee's job (copiers, shredders, fax machines, mail machines, etc.).
8. Using the In-Out Board (also known as "The Pegboard"), on a daily basis. Employees are expected to indicate their return date in the "Description of Location" field. Initials of individual names are only to be used in this area if indicating a client's home.
9. Restarting your PC at the end of each workday. Restarting refreshes the computer's memory, closes any open network file for backup purposes, and allows for proper off-hours updating to occur.

General Unacceptable Use

Employees must not use electronic communications or Region V's information systems for purposes that are illegal, unethical, harmful to the organization, or non-productive.

Some examples, but not limited to, of unacceptable use are:

1. Excessive personal use of Region V's organizational resources (computer, phone, Internet and e-mail, voice systems etc.) during work time.
2. Participating in excessive non-work-related electronic messaging (i.e. personal e-mail, texting, web browsing, etc.).
3. Promoting disrespect of Region V's employees, customers, clients, or vendors, or other persons or entities including actions that are discriminatory, or constituting a personal attack, including ethnic jokes or slurs. Communication that is harassing or threatening, including derogatory comments based on race, national origin, marital status, sex, sexual orientation, age, disability, pregnancy, religious or political beliefs, or any other characteristic protected under local, state, or federal law is strictly forbidden.
4. Sending or forwarding chain letters / e-mail, (i.e. messages containing instructions to forward the message to others).
5. Storing non-work-related media files (i.e. music, MP3s, digital photos, movies, etc.) on network drives or the "My Documents" folder.
6. Operating a business, pursuing personal business opportunities, or soliciting anyone for commercial ventures or personal gain.
7. Transmitting any content that is fraudulent.
8. Any use violating law or government regulation.
9. Viewing, copying, or transmitting inappropriate, sexually explicit, or unethical material. If such content is accidentally viewed or transmitted using Region V's information systems, the end user is to report the incident in writing to a ISA staff and/or the employee's respective supervisor stating the detail of the incident, so appropriate preventative measures may be taken.
10. Transmitting harassing or soliciting messages.
11. Transmitting or using copyrighted materials without permission.
12. Transmitting or viewing confidential and / or unauthorized information that is not for job-related purposes.
13. The use of any removable media (flash drives, thumb drives, memory sticks, etc.) without prior consent of ISA staff.
14. Any willful or malicious attempt to undermine or breach the security of Region V's information systems.
15. Any attempt to access confidential or private information not directly related to one's job duties.
16. Utilizing Region V resources such as e-mail or portable equipment to conduct business off-site or after normal business hours and not recording time worked on time sheet (non-exempt employees only).

Social Networking / Blogging Websites

Employees are prohibited from making excessive personal use of social networking websites during work hours that interferes with the performance of their job responsibilities. This includes websites such as Facebook, MySpace, LinkedIn, Yammer, Twitter, Blogger, and other similar sites. Employees are also prohibited from excessive personal use of streaming media such as YouTube, Hulu, or other similar media sites because of the potential risks and liabilities they can create for Region V Systems.

Some of these risks are:

- Introduction of malicious code that could damage systems.
- Disparaging posts that could potentially result in liability to the organization.
- Lost productivity.
- High bandwidth usage for streaming content ultimately slowing down other network connections.

Employees are prohibited from creating websites, blogging, posting or publishing any information on any Internet websites, concerning the activities, services, or clients of Region V Systems or its contracted providers without the express consent of Region V's Regional Administrator, and may not use Region V's logo or other images in any way that disparages the reputation of Region V Systems. These prohibitions extend to employees' off-work hours and to employees' off-site activities.

Your Region V Systems e-mail address and Social Media

Employees shall not use their Region V e-mail address when utilizing personal social networking or other websites that are unrelated to their job. Listing your username in combination with a region5systems.net domain for personal use online may imply that you are acting on Region V's behalf.

Outside the workplace, you have a right to participate in social media and networks using personal e-mail addresses; however, information and communications that you publish on personal online sites should never be attributed to Region V Systems or appear to be endorsed by, or to have originated from, Region V Systems. If you choose to disclose your affiliation with Region V Systems in an online communication or social networking website, then you must treat all communications associated with the disclosure as professional communications governed by Region V's Electronic Communications & Information Systems Acceptable Use Policy.

Social Networking Relationships

Supervisor-subordinate and professional-consumer/client social networking relationships may pose ethical and legal risks. Employees are strongly discouraged from participating in these types of social networking relationships. Employees should never feel compelled to accept another employee's or client's "friend" or event request from a social networking website. It is strongly advised to wait at least two years after a professional-consumer/client relationship has ended before consideration is made to befriend an individual who applies to this scenario.

Consumer Confidentiality Expectations

Region V Systems' employees are to always respect and adhere to the rights of persons served with the utmost care for client/consumer confidentiality. Expectations are as follows:

1. It is unacceptable to attempt to access confidential consumer-related information not directly related to one's job duties.
2. It is unacceptable to transmit any unencrypted data that would jeopardize the identity of confidential consumer-related information such as Social Security Numbers, full names, addresses, or other identifying information. Employees are strictly forbidden from using personal e-mail accounts or SMS text messages to transmit any consumer-related information (i.e. Gmail, Yahoo, AOL, Windstream, Verizon, Sprint, etc). Internal exchanges of information regarding clients, if job-related, are acceptable; however, such data should not be forwarded to external parties without encryption and applicable confidentiality agreements in place.
3. It is unacceptable to utilize social networking websites to discuss, in any way, current or former clients of Region V or any individual who identifies as being a consumer through Region V's stakeholder network (e.g., Consumer Coalition, consumers associated with Region V's Provider Network).
4. Employees who are members of a social networking website and participate in discussions that pertain to Region V business or clients are responsible for the content of those discussions. If an employee who is a member of a social networking website discovers inappropriate or unauthorized discussions concerning Region V consumers, present or past, or consumers who are associated with Region V's stakeholder network, the employee must immediately report this to Region V's Corporate Compliance Officer through a written *Incident Report.*

Failure to adhere to these expectations shall put the employee at risk for discipline measures up to and including termination of employment.

Downloads / Software Modifications

Program and/or software downloads from the Internet are not permitted unless specifically authorized by ISA staff. Any software installation needs to be processed and installed by ISA staff.

Copyrights

Employees using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by Region V and/or legal action by the copyright owner.

Monitoring

All Region V employees consent to having their use of the Region's information systems and electronic communications monitored, as deemed necessary for Region V to manage its business operations and to assure compliance with applicable laws and Region V policies. Region V reserves the right to access any data created, used, or modified using Region V's resources and to monitor all IT resources to verify compliance with this Policy. Employees should not expect or assume that they have a right of privacy because they are assigned and use network account passwords.

All messages and other data created, sent, or retrieved through Region V's information systems or over the Internet are the property of Region V and may be considered public information under state law, unless they involve consumer-related information or attorney-client privileged communications.

Region V utilizes various methods to monitor network activity, which may include, but are not limited to:

- Administrative access to all employee network accounts which provides the ability to review all data created, sent, or received from these accounts.
- The ability to audit login attempts or other attempts to gain access to confidential network information.
- Automated audits of various network activities, including, but not limited to Internet, voice systems, printer, and facsimile usage.

Reasons to monitor employee network activity may include, but are not limited to:

- Suspected violations as defined under this policy.
- Employee misconduct.
- Complaint-based reports.
- Performance or productivity concerns.
- Upon notice of employee separation (voluntary or involuntary).

Computer Viruses, Malware, other Security Threats

Computer viruses are programs designed to make unauthorized changes to programs and data. Therefore, viruses can cause destruction of organizational resources. Malware is software designed to maliciously infiltrate or damage a computer system without informed consent. New security threats emerge daily and it is important to note that preventative measures are of utmost importance.

It is important to know that:

- Computer viruses and malware are much easier to prevent than to cure.
- Defenses against computer viruses, malware, and other security threats include: strong authentication techniques, using trusted technical resources for data and programs, and up-to-date virus and malware scanning software.

ISA staff shall:

- Install and maintain appropriate anti-virus / anti-malware software.
- Respond to all virus attacks, destroy any virus / malware detected, and document each incident.
- Use preventative measures which include the use of local machines security parameter updates as necessary.

Employees shall:

- Not knowingly introduce a computer virus into Region V's computer network. Common risks for this include connecting notebook computers to unauthorized wireless networks and using removable media that has not been authorized for use by ISA staff.
- Immediately power off their workstation and notify an ISA staff member if he/she suspects that his/her workstation has been infected.
- Not connect any notebook or portable computers to unauthorized wireless networks.

Access Codes & Passwords

The confidentiality and integrity of data stored on Region V's computer systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties.

ISA staff shall be responsible for the administration of access controls to all Region V company systems. ISA staff will process adds, deletions, and changes upon receipt of a written or oral request from the end user's supervisor or Management Team member as applicable. ISA staff shall maintain a list of administrative access codes and passwords and keep this list in a secure area. The Director of Operations & Human Resources shall also maintain a copy of this list for backup purposes.

Each employee shall:

1. Not use any username to log in to the network other than the username issued at the start of employment with Region V. If a different computer in the building must be used, employees should use their own username and password on that machine. ISA staff can assist in setting a profile up on that machine.
2. Be responsible and accountable for all computer transactions that are made with his/her user ID and password.
3. Not disclose passwords to others. Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords should not be recorded where they may be easily obtained.
4. Change passwords at least every 120 days.
5. Use passwords that will not be easily guessed by others. The use of strong encryption passwords is enforced on Region V's network and requires the user to have a password of at least 8 characters, using a combination of letters, numbers, capital letters and special characters.
6. Restart PC when leaving a workstation for an extended period.
7. Maintain the use of a 5-minute idle screen saver which requires a password to log back in to the session.
8. Use password protection on any Portable Digital Assistant (PDA) / smartphone or other device connecting to Region V's network.

Supervisors shall notify the HR Department promptly when an employee leaves the organization or transfers to another department so that his/her access can be revoked or modified. Involuntary separations must be reported concurrent with the separation.

Physical Security of Technology Devices

Region V shall take responsibility to protect computer hardware, software, data, and electronic documentation from misuse, theft, unauthorized access, and environmental hazards as follows:

1. Memory cards, media, or other storage devices shall be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up.
2. Memory cards media, or other storage devices shall be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
3. Critical computer equipment, i.e., file servers, must be protected by an uninterruptible power supply (UPS). Other computer equipment shall be protected by a surge suppressor.
4. Environmental hazards to hardware such as food, smoke, liquids, high or low humidity and extreme heat or cold should be avoided.
5. Disconnections, modifications, and relocations of any software or hardware are not to be performed by anyone other than ISA staff. This does not apply to temporary moves of notebook computers.
6. Employees shall not take shared portable equipment, i.e. notebook computers, camera, video camera, etc., out of the building without informed consent. If consent is granted to take equipment out of the building, staff must utilize the Operations Department's checkout procedures.
7. Employees shall exercise care to safeguard the valuable electronic equipment assigned to them.

Voice Systems (Landline and Mobile)

Voice systems at Region V include all landline phones, faxes, cell phones, smartphones, and other mobile devices. Voice systems technology continues to expand its scope in the course of daily business functions and its interaction with existing traditional network devices such as desktop computers.

Employees, while operating a Region V vehicle or driving a personal vehicle for business use, shall comply with Nebraska's "Texting While Driving Law." This law prohibits drivers from using handheld wireless communication devices to read, manually type, or send a written communication while operating a motor vehicle which is in motion. Handheld wireless communication devices include, but are not limited to, a mobile or cellular telephone, a text messaging device, a personal digital assistant/ smartphone, a pager, or a laptop computer.

The following procedures apply to all voice system devices. Failure to observe these policies may result in disciplinary action and/or require the employee to reimburse Region V for any expenses incurred from unauthorized use, depending upon the type and severity of the violation, whether it causes any liability or loss to Region V, and/or the presence of any repeated violation(s).

1. Voicemail passwords are not to be shared unless necessary for job-related duties.
2. Employees are responsible for the operation, condition, and security of any mobile device checked out. All necessary precautions shall be taken to ensure that the mobile device is not subjected to conditions that would adversely affect it or for which it was not designed.
3. Region V mobile devices are to be used primarily for Region V Systems-related business.
4. Employees are expected to retrieve voice mail messages in a timely fashion.
5. Region V Systems reserves the right to monitor and audit the use of all Region V Systems phones and devices.

6. Reasonable precautions should be made to prevent theft and vandalism. If this should occur, the employee must notify their supervisor or an IT Specialist immediately if it is lost or stolen during business hours or the next business day if it is after business hours.
7. Employees needing directory assistance must not use landline or mobile "411" service from the phone companies as this proves to be a substantial cost for Region V. Employees must use alternative directory assistance methods. Suggested methods are to utilize:
    - 1-800-FREE-411 (1-800-373-3411).
    - 1-800-GOOG-411 (1-800-466-4411) for business searches.
    - "Google" or a similar online search for the name or business.
    - A phone book.

    Failure to use an alternative method for directory assistance is considered unauthorized use and may result in disciplinary action and/or related costs being withheld from the employee's payroll check.
8. Upon separation of employment with Region V Systems, any mobile devices or peripherals assigned to the individual must be turned in to ISA staff. Failure to do so may result in the cost of the device being withheld from the employee's final paycheck.
9. Know the proper procedure for Utilizing Region V's "Virginia Code" system as well as know the proper use of the first responder's emergency number: 441-5599. This number is to be used for internal assistance when a potentially escalating situation arises and should not be used in place of 911. Proper use of this number includes: displaying the number prominently on desk or landline/IP phones, and keeping the 441-5599 number on a speed dial for mobile phones.

Mobile Device Network Synchronization

If Region V has issued a smartphone or other mobile device to staff or if staff request device synchronization with their own smartphone, staff must abide with the following:

1. Ensure the use of password protection on the device. Randomly, ISA staff may periodically check these devices to ensure the password protection has not been removed. Failure to observe this practice may result in removal of network configuration.
2. When upgrading or terminating an existing device, settings must be removed from the smart-phone prior to synchronization of the new device.
3. Upon separation of employment, the device must be brought to an IT Specialist so appropriate network configuration is removed.

Cell Phone Reimbursement

Region V has available three options to assist employees with the cost of conducting business via mobile phones. All options are subject to supervisor/management approval.

1. If an employee's position warrants, a mobile phone device is issued to the employee. The cost of the device, and its job-related features as applicable (data connection, voicemail, etc.), is paid by Region V.

2. If an employee's position warrants, a stipend reimbursement of $40 per month is given if the employee chooses to use his/her personal cell phone vs. option 1 above.
3. If an employee uses his/her personal cell phone for work-related calls, Region V will reimburse the employee at a rate of 15 cents per minute.

Data Retention

All local and network data including messages created, sent, or retrieved through Region V's information systems, or over the Internet, is considered the property of Region V. Retention of Region V's data is governed by its Information and Records Management Policy.

Administration of Policy

Information Systems Administration (ISA) staff are responsible for the administration of these policies. ISA staff must:

- Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these directives.
- Provide appropriate support and guidance to assist employees to fulfill their responsibilities under these directives.
- Appropriately report observed non-compliance of these policies to staff and formally follow up with supervisors and/or management.

Violations of this Policy

Failure to observe these policies may result in disciplinary action by Region V, depending upon the type and severity of the violation, whether it causes any liability or loss (including loss of productivity time) to Region V, and/or the presence of any repeated violation(s).