Policy Name: V.2 Voicemail, Texting, Email and Internet Use Policy	**Section:** V Technology	**Programs: All**
	Standard/Area: Technology	**Review Date: 8.20.25**
File: Employee Portal, Human Resources V.2 Voicemail, Texting, Email and Internet Use Policy.doc	**Effective Date: 8/25 (moved from Employee Handbook)**	**Revision Date**:

Section I: Intent

This policy is intended to provide each employee, contractor, intern, volunteer and authorized third party of MVCS with guidelines associated with the use of the Agency's voicemail/texting/email and Internet system (the system).

This policy is not intended to infringe upon an employee's right to engage in protected concerted activity under 29 U.S.C. sec. 157. Employees have the right to discuss terms and conditions of employment and mutual work-related concerns.

Section II: Policy

MVCS provides voicemail, texting, email, and internet access to enable effective, secure, and compliant business operations. This policy establishes acceptable use, security controls, data handling, retention, privacy, monitoring, and enforcement for all MVCS users (employees, contractors, interns, volunteers, and approved third parties) accessing MVCS voicemail, texting, email, and internet resources. All users must use these resources responsibly, protect MVCS information, respect applicable laws and MVCS policies, and report any security or policy violations promptly.

Section III: Procedures

General Provisions/Electronic Monitoring

• The MVCS email system is intended to be a means for sharing important Agency information, thus, all employees are expected to check their email at least daily when working and are responsible for understanding any information shared via the email system.
• While conducting Agency business, all employees should use MVCS email addresses, not private, personal email addresses. All employees have access to the "webmail" system and can send and receive email if needed while away from the Agency network.

• The system, and all data transmitted or received through the system, are the exclusive property of the Agency. No individual should have any expectation of privacy in any communication over this system. Any individual permitted to have access to MVCS's system will be given a voicemail, email and/or Internet address and/or access code, and will have use of the system, consistent with this policy.
• The Agency reserves the right to monitor, intercept, and/or review all data transmitted, received, or downloaded over the system. Any individual who is given access to the system is hereby given notice that the Agency will exercise this right periodically, without prior notice and without the prior consent of the employee ***(ref. V.5 MVCS Right to Inspect Policy)***
• The Agency's interests in monitoring and intercepting data include, but are not limited to: protection of proprietary, and similar confidential commercially-sensitive information (i.e. financial or sales records/reports, marketing or business strategies/plans, consumer lists, etc) managing the use of the Agency's computer system; and/or assisting the employee in the management of electronic data during periods of absence. No individual should interpret the use of password protection as creating a right or expectation of privacy. To protect everyone involved, no one will have a right or expectation of privacy with regards to the receipt, transmission or storage of data on the Agency

Voicemail/Email/Internet system

• Agency email and text messages are not secure forms of communication for the purposes of transmitting any protected consumer information. No private information regarding employees (such as social security numbers) or consumers (such as name, social security number, or other personal information) should be transmitted over the email system or via text message without use of encryption or a secure texting platform. No employees may have email or texting communication with consumers until the consumer has signed, or a parent has signed in the event the consumer is a minor, a consent form to communicate via unsecure methods.
• Employees working under a Flexible Work Schedule or Remote Work Agreement shall include their schedule and contact information as part of their email signature.

Guidelines

a. To prevent damage to MVCS systems by computer viruses all files downloaded from the Internet are scanned automatically by virus detection software. If necessary, access to the Internet may be interrupted or incoming information blocked as needed to protect system integrity.

b. Connections to the Internet and other external resources by means other than those authorized and set-up by MVCS are not permitted unless expressly authorized by the Chief Operating Officer and properly protected by appropriate security devices.

c. MVCS provides E-mail capability to its staff for their use in conducting MVCS business. Incidental personal use is permissible, provided that such use: 1) does not affect the normal business operations of MVCS; 2) does not interfere with the performance of job responsibilities; 3) otherwise complies with relevant MVCS policies.

d. Use of a personal email account or personal messaging service (app) should not be used to communicate with clients, vendors, or MVCS employees, unless authorized to do so by the staff members' supervisor or the IT Manager. MVCS provides access to necessary communication systems (such as email, messaging, secure texting and secure voicemail) which should be used for all work-related communication purposes.

e. The E-mail system software and hardware are property of MVCS, as are all messages that are composed, sent, or received via the MVCS E-mail system. Staff members should compose electronic messages with care to protect the reputation of MVCS and to comply with all laws applicable to MVCS. Notwithstanding the right of MVCS to retrieve and read any E-mail messages, such messages should be treated as confidential by other staff members and accessed only by the intended recipient. Staff members are not authorized to retrieve or read any messages that are not sent to them unless given prior approval by the intended recipient or by any other person authorized by the intended recipient or by the IT Manager.

f. When using the Internet, staff using MVCS systems are acting as representatives *of MVCS* and any such communications may be deemed to have been made by MVCS. As such, staff members should act appropriately to protect the reputation of MVCS and to comply with any applicable laws.

g. Information sent or received over the Internet or through email, is not confidential or secure. Be aware that sensitive material may be at risk *of* unintended disclosure to third parties. Even when a message is erased, it is still possible to retrieve and read that message. Furthermore, the use of passwords for security does not guarantee confidentiality Staff members must exercise caution and care when transferring such material in any form.

h. Staff members may not use a password, access a file, or retrieve any stored information unless authorized to do so. Staff members should not attempt to gain access to another staff member's messages, files, or other stored information without that person's permission unless authorized to do so by the staff members' supervisor or the IT Manager.

i. Any unauthorized attempt to gain access to restricted computer files, systems, E-mail, voice mail, decrypt encrypted material, obtain privileges or information to which a staff member is not entitled, or otherwise tamper with any computer system is prohibited and will result in disciplinary measures up to and including termination.

j. Unless authorized by the IT Manager, staff members are prohibited from making any changes or modifications to any computer hardware or software including adding or removing software or components or modifying configurations beyond what is allowed using standard user customization features. Modification includes adding games and/or additional Internet service providers.

k. MVCS provides a branded email signature for each employee upon hire. The branded email signature must be used and may not be modified without the permission of the employee's immediate supervisor.

l. Employees must comply with all software licenses, copyrights, and all other laws governing intellectual property and online activity.

m. MVCS expressly prohibits use of the Internet, E-mail and MVCS's computer systems and equipment for the following activities:

• Sending, receiving, printing, or otherwise placing MVCS internal, confidential, or proprietary information or property, including software, on any publicly accessible Internet computer, is prohibited without prior permission from the IT Manager.
• Accessing or communicating information involving offensive or harassing statements or language, including disparagement of others based on their of age, creed, color, disability, pregnancy, national origin, race, religion, sex, or sexual orientation, or any other status or category protected by law.
• Under this policy, chain letters are considered to be such communications.
• Sending or soliciting sexually oriented messages or images
• Engaging in personal commercial activities, including offering services or merchandise for sale except as otherwise authorized by MVCS.
• Engaging in any activity in violation of local, state and federal law.

All electronic communications and computer systems and all communications and information transmitted by, received from or stored in these systems are MVCS property and are subject to the provisions under ***General Provisions/Electronic Monitoring***.

Safeguarding Accounts and Passwords

Access to computer accounts must be protected, at minimum, by a user-identification (user-id) and password. It is the responsibility of the user to safeguard their user-id and password. A user-id is not to be shared; the password is not to be divulged to others, other than to your supervisor or the IT Manager for the reason to assist in temporarily troubleshooting or upgrading your work-issued device.

Section IV: Distribution and Training

The Policy and associated attachments are distributed on the MVCS Employee Portal. Notifications related to new, amended, or reviewed policies will be communicated to MVCS leadership and program directors for dissemination to their staff as appropriate. The policy may be directly disseminated to appropriate staff and/or staff groups via email notification after initial dissemination to leadership as per direction of the CEO or designee. The dissemination will be performed by the Chief Operating Officer.

Section V: Legal, Regulatory, Accrediting, and Other Related References and Resources

V.5 MVCS Right to Inspect Policy

V.3 Software Usage Policy

29 U.S.C. sec. 157