Policy Name: **V.4 Telephone/Cell Phone Use Policy**	**Section:** V Technology	**Programs: All**
	Standard/Area:	**Review Date: 11/10/25**
File: Employee Portal; Technology V.4 Telephone/Cell Phone Use Policy.doc	**Effective Date: 8/25 (moved from Employee Handbook)**	**Revision Date: 11/10/25**

Section I: Intent

This policy establishes acceptable and responsible use of telephone and cell phone resources by MVCS employees to protect data, ensure safety, maintain productivity, and comply with applicable laws and organizational risk management practices.

Section II: Policy

MVCS-issued devices are property of MVCS and should be used primarily for MVCS business. Personal use should be incidental and not interfere with work responsibilities. Users must always protect MVCS data and device security. Loss or theft must be reported immediately per incident reporting procedures. All usage should comply with applicable laws, organizational standards, and industry best practices, including privacy, confidentiality, and data security.

This policy applies to all MVCS employees, contractors, interns, volunteers, and temporary staff who use MVCS-issued or personal devices for MVCS business (collectively referred to as “users”). The policy covers all telephone lines, mobile phones, smartphones, tablets with telephony capabilities, and related applications (voice, video, messaging, and data services) used for MVCS work.

Nothing in this policy is intended to prevent employees from engaging in protected concerted activity under the NLRA.

Section III: Procedures

Definitions

MVCS-issued device: Any phone or cellular device provided by MVCS for business use.

- Personal device (BYOD): A personal device used to access MVCS data or perform MVCS duties.

- PII/PHI: Personally identifiable information or protected health information (as applicable). All such data must be handled per MVCS data protection guidelines.

- Restricted use: Uses prohibited by policy (e.g., unlawful activities, harassment, sharing confidential information inappropriately).

- Safe driving: Operating a motor vehicle in a manner that prioritizes safety; hands-free operation where possible.

5. Acceptable Use of MVCS Telephones and Cell Phones
- Business use: Use for MVCS operations, communications with clients, suppliers, colleagues, and partners, scheduling, coordinating services, and other work-related activities.
- Professional conduct: Communicate respectfully and professionally. Do not engage in harassment, discrimination, or unlawful activity.
- Documentation and data handling: When discussing or transmitting MVCS information, ensure proper channels, encryption, and access controls as required by policy.
- Compliance with driving safety: Do not use a handheld device while operating a motor vehicle except in a legally permissible, hands-free manner. If driving, pull over safely to use a device when necessary and safe.

6. Eligibility for a company provided cell phone
An employee must have a legitimate business need for a cell phone/mobile device based on services provided and an assessment made by their supervisor that is approved by their Program Director. The issuance of same to the employee must be approved by the employee's Supervisor. MVCS owns and remains entitled to all company-issued cell phone/mobile devices, including all passwords controlling access to them. At the time of employment termination, all such equipment and passwords must be returned to Human Resources in operable condition.

6. Prohibited Uses
- Unauthorized disclosure of confidential or sensitive MVCS information.
- Sharing login credentials or device access with unauthorized individuals.
- Using MVCS devices for illegal activity, political campaigning, or other non-work-related activities in violation of MVCS policy.
- Installation or use of unapproved apps or software that pose security risks.
- Recording conversations or taking photos in restricted areas or where prohibited by policy or law.
- Texting, emailing, or messaging in a manner that creates safety or legal risk (e.g., while driving, or when prohibited by law).

7) Personal Use and BYOD (Bring Your Own Device)
- Personal use should be limited and should not interfere with work responsibilities or MVCS data security.
- BOYD Risk Management If allowed, to use personal devices for MVCS work, users must comply with the following requirements: In order to access MVCS data, personal devices must be kept updated and secure. Securing your personal devices involves the following:

- Requiring a passcode, Fingerprint or Face ID to unlock the device.
- Requiring the device locks after periods of inactivity.
- Ensuring the device is not regularly used by people other then yourself.
- Making sure to install the latest security updates and recent operating system updates.
- When possible, using the Company Portal (or similar app) to ensure the installation and security of

MVCS data.

- MVCS reserves the right to revoke access or require device compliance at any time.
- The use of the Company Portal App should be used (where possible) to separate MVCS data from personal data.

While MVCS permits employees to bring personal cell phones and other mobile devices (i.e. smart phones, PDAs, tablets, laptops) into the workplace, employees must not permit the use of such devices to interfere with their job duties or impact workplace safety and health.

Use of personal cell phones and mobile devices at work can be distracting and disruptive and cause a loss of employee productivity. As a result, employees should primarily use such personal devices during nonworking time, such as breaks and meal periods. During this time, employees should use their device in a manner that is courteous to those around them. Outside of nonworking time, use of such devices should be kept at a minimum and limited to emergency use only.

Employees with devices that have a camera and/or audio/video recording capability are restricted from using those functions on MVCS property unless authorized in advance by their Supervisor and with proper consent of the subjects being videotaped or photographed.

Employees are expected to comply with Agency policies regarding the protection of the employer's confidential and proprietary information when using personal devices.

While operating a vehicle on Agency time, the Agency requires that the driver's personal cell phone/mobile device be turned off. An employee who needs to make or receive a phone call should pull off the road to a safe location unless he or she has the correct hands-free equipment for the device that is in compliance with applicable state laws.

8. Security and Privacy
- Device security: Use strong passwords or biometric authentication; lock devices when not in use; enable auto-lock and device encryption where supported.
- Data protection: Do not store or transmit MVCS data on unsecured networks without approved security controls (e.g., VPN, approved apps).
- Remote access: Access to MVCS systems may require VPN, MFA, or other authentication methods as defined by MVCS IT security policies.
- Monitoring: MVCS reserves the right to monitor, audit, and review device usage and data access in accordance with applicable laws and organizational policies to ensure security and compliance.
- Incident reporting: Report suspected data breaches, loss/theft, or policy violations to the designated security or HR/administration contact immediately.

9. Use of MVCS Communications Systems
- MVCS communications systems (phones, VOIP, messaging apps) may be used to conduct MVCS business. Users must comply with MVCS policies for appropriate use, storage, retention, and destruction of communications data.

10. Safety and Driving
- use of handheld devices while operating a vehicle is prohibited unless it is being used in hands-free mode. If necessary, pull over safely to conduct business calls.
- If driving is required as part of duties, plan calls in advance and use approved, hands-free devices or alternatives (voicemail, scheduling, or delegation).

11. Data Retention, Records, and Privacy
- Communications may be subject to MVCS retention schedules and legal discovery. Do not delete or destroy records in violation of policy.
- Personal communications not related to MVCS business should be kept separate where possible.
- For projects involving PII/PHI or other sensitive data, follow specific MVCS data handling and retention policies.

12. Compliance and Enforcement
- Compliance: All users must comply with this policy as well as related MVCS policies (IT security, data protection, privacy, acceptable use, and safety).
- Violations: Violations may result in disciplinary action up to and including termination, legal action, and reimbursement of costs or damages, depending on the severity and nature of the violation.
- Investigation: MVCS reserves the right to investigate suspected violations. Unauthorized access, misuse, or disclosure may be reported to appropriate authorities.

13. Roles and Responsibilities
- Employees: Use devices responsibly, protect data, report security incidents, and follow this policy.
- Supervisors/Managers: Ensure team awareness, monitor compliance within the bounds of policy and law, and address incidents with appropriate corrective actions.
- IT and Security: Enforce security controls, manage device configurations, provide training, monitor for policy violations, and respond to incidents.
- HR/Compliance: Provide guidance on policy applicability, manage disciplinary actions, and maintain policy documentation.

14. Training and Awareness
- All users must complete annual training on appropriate phone use, data protection, security practices, and policy updates.
- New hires must acknowledge understanding of this policy as part of onboarding.

15. Monitoring, Auditing, and Change Management
- MVCS may monitor device usage, network access, and data activity to ensure policy compliance and protect MVCS resources.
- This policy will be reviewed and updated as needed to reflect changes in technology, law, and organizational needs.

16. Procedures and Resources
- Reporting incidents: reporting lost devices, suspected data breaches, or policy violations should be made to the IT department immediately. IT personnel will inform the Chief Operating Officer of any suspected data breaches or policy violations and submit an official incident report through the MVCS incident reporting system.

- Approval and exceptions: All requests for exceptions to the policy (e.g., BYOD exceptions, app restrictions) should be communicated to the IT manager for review.

Section IV: Distribution and Training

The Policy and associated attachments are distributed on the MVCS shared Drive (P) and also on the 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