Electronic Systems and Equipment

Policy Type: Local
Responsible Office: Chief John Venuti, Virginia Commonwealth University Police Department
Initial Policy Approved: 6/16/2014
Current Revision Approved: 6/2/2017

General

Electronic systems and equipment provides the VCU Police Department with enhanced communication abilities for both routine and emergency situations. The Administrative and Business Operations Division is responsible for the procurement, operation, maintenance and security of the Department's computers and computer systems. This policy is designed to supplement existing Commonwealth of Virginia and VCU computer, network use and electronic systems policies which are applicable to all employees upon hire. VCU reserves the right to monitor any of its electronic systems, including email messages and any other known messages, documents, spreadsheets or files.

Accountability Statement

All employees are expected to fully comply with the guidelines and timelines set forth in this written directive. Failure to comply will result in appropriate corrective action. Responsibility rests with the division commander to ensure that any violations of policy are investigated and appropriate training, counseling and/or disciplinary action is initiated.

Definitions

A. CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) SECURITY POLICY – A federal policy to provide appropriate controls to protect the full lifecycle of criminal justice information, whether at rest or in transit.

B. ELECTRONIC SYSTEMS – All hardware, software, and tools owned by VCU that are available for official use by VCU employees, including but not limited to, electronic mail, voice mail, calendaring and systems such as internet, etc.

C. INTERNET SYSTEM – A global information system of interconnected computers and computer networks used to receive and transmit information and electronic messages.
D. **INTRANET SYSTEM** – A local information system used to receive and transmit information and electronic documents among authorized users.

E. **MOBILE DATA COMPUTER (MDC)** – The hardware device used by officers in the field to run communications, NCIC/VCIN inquiries, and other software applications. The term MDC shall apply to both the fixed mounted and laptop versions.

F. **DIGITAL MOBILE VIDEO RECORDER SYSTEM (ARBITRATOR)** – Equipment installed in patrol vehicles which is used to record a video/audio account of events.

G. **WIRELESS COMMUNICATION DEVICES** – Wireless communication devices shall be defined as cellular telephones, iPhone/iPad units, or any other electronic communication devices and services.

H. **ROLES AND RESPONSIBILITIES** – For all systems with criminal justice information, the following table shows the designated roles and responsibilities over the applicable system:

<table>
<thead>
<tr>
<th>System</th>
<th>Data Steward</th>
<th>Owner/Admin</th>
<th>Data Custodian</th>
<th>System Owner</th>
<th>Department Tech</th>
<th>System Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arbitrator - vehicle camera system</td>
<td>Chief</td>
<td>IT Manager</td>
<td>Officers</td>
<td>Chief</td>
<td>IT Manager</td>
<td>IT Manager</td>
</tr>
<tr>
<td>Evidence.com/Sync - body camera software</td>
<td>Chief</td>
<td>IT Manager</td>
<td>Officers</td>
<td>Chief</td>
<td>IT Manager</td>
<td>IT Manager</td>
</tr>
<tr>
<td>Treds/Report Beam - vehicle accident reporting system</td>
<td>Chief</td>
<td>IT Manager</td>
<td>Officers</td>
<td>Chief</td>
<td>IT Manager</td>
<td>Accreditation &amp; Compliance Coordinator</td>
</tr>
<tr>
<td>Campus Camera System</td>
<td>Chief</td>
<td>IT Manager</td>
<td>Officers</td>
<td>Chief</td>
<td>IT Manager</td>
<td>IT Manager</td>
</tr>
<tr>
<td>LinX - law enforcement info exchange</td>
<td>Chief</td>
<td>Admin Director</td>
<td>Officers</td>
<td>Chief</td>
<td>IT Manager</td>
<td>IT Manager</td>
</tr>
<tr>
<td>AS400 - legacy incident report system</td>
<td>Chief</td>
<td>Admin Director</td>
<td>Officers</td>
<td>Chief</td>
<td>IT Manager</td>
<td>Admin Director</td>
</tr>
<tr>
<td>RMS/Moblan/MFR - incident report system</td>
<td>Chief</td>
<td>Admin Director</td>
<td>Officers</td>
<td>Chief</td>
<td>IT Manager</td>
<td>Admin Director</td>
</tr>
<tr>
<td>LiveScan - fingerprinting system</td>
<td>Chief</td>
<td>IT Manager</td>
<td>Officers</td>
<td>Chief</td>
<td>IT Manager</td>
<td>IT Manager</td>
</tr>
<tr>
<td>VCIN - Virginia criminal info network</td>
<td>Chief</td>
<td>ECC Manager</td>
<td>Officers</td>
<td>Chief</td>
<td>IT Manager</td>
<td>ECC Manager</td>
</tr>
<tr>
<td>NICE - ECC phone recording system</td>
<td>Chief</td>
<td>ECC Manager</td>
<td>Officers</td>
<td>Chief</td>
<td>IT Manager</td>
<td>IT Manager</td>
</tr>
<tr>
<td>LiveSafe - campus safety app</td>
<td>Chief</td>
<td>ECC Manager</td>
<td>Officers</td>
<td>Chief</td>
<td>IT Manager</td>
<td>ECC Manager</td>
</tr>
<tr>
<td>Tipsoft - text-a-tip system</td>
<td>Chief</td>
<td>ECC Manager</td>
<td>Officers</td>
<td>Chief</td>
<td>IT Manager</td>
<td>ECC Manager</td>
</tr>
<tr>
<td>Tracker - property &amp; evidence bar code tracking system</td>
<td>Chief</td>
<td>Captain, Support Services</td>
<td>Officers</td>
<td>Chief</td>
<td>IT Manager</td>
<td>Property Manager</td>
</tr>
<tr>
<td>CAD - software system for dispatching/ monitoring ECC calls</td>
<td>Chief</td>
<td>ECC Manager</td>
<td>Officers</td>
<td>Chief</td>
<td>IT Manager</td>
<td>ECC Manager</td>
</tr>
<tr>
<td>TruVision - legacy campus camera system</td>
<td>Chief</td>
<td>ECC Manager</td>
<td>Officers</td>
<td>Chief</td>
<td>IT Manager</td>
<td>ECC Manager</td>
</tr>
<tr>
<td>Crystal Reports - statistical data extraction software</td>
<td>Chief</td>
<td>Accreditation &amp; Compliance Coordinator</td>
<td>Officers</td>
<td>Chief</td>
<td>IT Manager</td>
<td>Accreditation &amp; Compliance Coordinator</td>
</tr>
<tr>
<td>NetViewer - web access to CAD data</td>
<td>Chief</td>
<td>ECC Manager</td>
<td>Officers</td>
<td>Chief</td>
<td>IT Manager</td>
<td>ECC Manager</td>
</tr>
</tbody>
</table>

3-3 Computer Systems and Equipment
Approved: 6/2/2017
Access

A. New department members and all department members annually thereafter, sign the Confidentiality and Compliance Statement included in their Employee Work Profile. A member's signature indicates agreement to abide by the department, state, and university policies and procedures concerning confidentiality and information processing. The new employee checklist initiated by the supervisor indicates appropriate access to the department's computers and/or systems, based on the employee's new role.

B. Violations to these policies will result in access removal and/or disciplinary action in accordance with the Commonwealth of Virginia 1.60 Standards of Conduct.

C. Approved applicants will be given a user ID along with system and application passwords.

D. The system (sign-on) password must be changed the first time a new user signs onto a system. This new password shall be unique to the individual and shall not be shared with others or written down in a conspicuous location.

E. Periodic changing of passwords is required by the systems. VCU IT makes users aware of any required password changes.

F. Personal devices cannot be utilized to extract, house, transfer or copy VCUPD data.

Security

A. The computer server room shall remain locked at all times. Only authorized personnel are permitted in the server room.

B. Generally, the department's computer programs are password protected, and other applications of a confidential nature are protected by user ID access and restrictions.

C. Only individuals authorized to run a particular application may do so. No department member shall make a deliberate attempt to bypass system or resource security.

D. While actively logged onto a VCUPD computer, no computer shall be left unattended. Only one active session per system is allowed per use; do not open multiple sessions of the same program. VCUPD system users are required to log out of computer sessions when access is no longer needed. The IT Manager will make periodic security checks to enforce the department's computer security policies.

E. Systems administrator for various electronic and network systems will assign individual levels of security. These levels will determine access to system objects, programs and functions. Specific access restrictions for security levels are based on the applicability of each system.

F. VCUIT/Information Security must conduct and complete a security review of any proposed external party access to VCUPD data. Third-party data transmission or storage is prohibited unless approved by the Chief.

G. Only VCUPD provided equipment is to be utilized to access and/or print VCUPD email and/or records that include criminal information. Dual Factor Authentication (DUO)/Virtual Private
Network (VPN) is the only approved method to remotely access VCUPD data or records. VPN access must be approved by the Chief or their designee. Department issued computers must be used in order to access VCUPD systems from home.

H. Removal or reissuance of equipment containing VCUPD data or records must be in compliance with record retention policies or approved by the Chief or their designee, which includes hard drives or memory in all electronics (computers, cameras, copiers, USB drives, etc.).

I. Non-VCUPD personnel accessing VCUPD computers must log-in with their own credentials; VCUPD personnel will not allow non-VCUPD personnel to access computers using the VCUPD personnel’s credentials.

J. In the event of a system crash, only designated VCUIT personnel are permitted to work on resolving the issues and systems.

K. In the event of a data breach or other data security event involving VCUPD data, VCUPD personnel should immediately notify the Chief and the VCUPD IT Manager, who will immediately notify VCUIT/Security.

L. Per the Gramm-Leach-Bliley Act and CJIS, documents containing personal or criminal information data must be secured when it is not needed.

Information Backup

A. Backups are performed nightly for all VCU-owned or controlled systems by VCUIT.
B. The RMS system backups are conducted by the Richmond Police Department.
C. A complete system backup is performed whenever a system change is implemented by VCUIT.

Application Documentation and Training

A. Application programs are purchased for departmental use, and user documentation is provided as part of the program purchase.
B. User training for application documentation will be provided as needed to department members for programs specific to a member’s job responsibilities. Certain positions within the department require extensive training related to computer use.
C. The System Administrator is responsible for ensuring that adequate training of personnel is accomplished.
Email

A. Electronic mail is a department resource and is provided as a business tool. It shall be used to augment other types of communication already in the workplace, such as the telephone, fax machine, voice mail, written memorandum, and the like.

B. Email messages shall be treated like paper memos, faxes and the like, with regard to privacy. When a paper memo, fax, or email has left the sender, they relinquish control over it.

NOTE: Confidentiality/Privacy – All departmental electronic systems are considered public records and are subject to inspection and disclosure. Employees have no expectation of privacy in their use of electronic mail.

C. Email users shall exercise caution when logging in and out of the electronic system so as to prevent someone else from utilizing their password to send or retrieve messages.

Revision History

This policy supersedes the following archived policies:

6/16/2014  3-3 Computer Systems and Equipment