Department of Juvenile Justice
Administrative Procedure

Administrative Procedure #: **VOL I-1.3-7**	**Statutory Authority:** *Code of Virginia, §2.2-2005, et seq. (*Powers and duties of the Chief Information Officer "CIO" Virginia Information Technologies Agency; "VITA") *(http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-2005)* *Code of Virginia, §2.2-2827* (Restrictions on state employee access to information infrastructure) (http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-2827) *Code of Virginia, §2.2-1201, (13)* (Duties of the Department) (http://leg1.state.va.us/000/cod/2.2-1201.HTM)
Subject: Information Resource Acceptable Use	**Regulations:** 6VAC35-160 Regulations Governing Juvenile Record Information and the Virginia Juvenile Justice Information System
	COV ITRM Information Security Policy (SEC 519) (http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/Security_Policy_519_00_Final_0709.pdf) COV ITRM *IT Security Standard* (SEC501) (http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/Information_Security_Standard_SEC501_06_Eff04042011.pdf) *IT Standard Use of Non-Commonwealth Computing Devices to Telework* (ITRM SEC511-00) (http://www.vita.virginia.gov/uploadedFiles/Library/SEC511-00UseofNonCOVAssetstoTelework.pdf) DHRM Policy Use of Electronic Communications and Social Media. (http://www.dhrm.state.va.us/hrpolicy/pol175UseOfInternet.pdf)

I. PURPOSE

The purpose of this procedure is to create a prescriptive set of processes and procedures, aligned with applicable Commonwealth of Virginia (COV) Information Technology (IT) security policy and standards, to ensure the Department of Juvenile Justice (DJJ) develops, disseminates, and updates the Information Resource Acceptable Use Administrative Procedure requirements as stipulated by the COV Information Technology Resource Management (ITRM) Security Standard SEC501 and security best practices. This procedure explains responsibilities for use of DJJ information technology resources (including but not limited to computer systems, mobile devices, voicemail, electronic mail (email), Local Area Network LAN, and Internet connection on DJJ devices), specifies the actions that are prohibited, and establishes the minimum requirements for the Information Resource Acceptable Use Procedure.

II. SCOPE

This procedure applies to all DJJ IT Users to whom a COV network account has been assigned, as well as all DJJ systems (including but not limited to computers, mobile devices,

electronic email, etc.). This procedure not only addresses data, but also the computer systems, software, and hardware resources used to process the electronic information.

III. DEFINITIONS

Access Control Mechanism – For the purpose of this procedure is defined as any login identifiers, passwords, terminal identifiers, user identifiers, digital certificates, IP addresses, logon IDs granted to the DJJ IT Users.

DJJ personnel –Individuals employed by, volunteering, or contracted with DJJ, including but not limited to full-time, part-time, and wage positions, contractors, volunteers, and interns.

DJJ IT Users - All individuals to whom a Commonwealth of Virginia (COV) network account has been assigned. This includes, but is not limited to, classified, hourly, and part-time employees, service providers, business partners, interns, and volunteers.

Email Bombing - Users repeatedly sending an email message to a particular address (es) at a specific victim site. In many instances, the messages are large and constructed with meaningless data in an effort to consume additional system and network resources.

Email Spamming – Users sending emails to a list of many users with the intent of having the users reply to the emails and causing all the original recipients to also receive the reply overflowing the email mailbox.

Encryption - The process or the means of converting original data to an unintelligible form so it cannot be read by unauthorized users.

IT Resources – For the purpose of this procedure IT Resources are defined as computer systems (desktops, laptops, tablets), any other electronic device (including but not limited to mobile devices), software (ex. Microsoft Office applications, Adobe reader, etc.), LAN, electronic mail (email), Internet access, hardware (ex. Printers, copiers, etc.), electronic information (data).

Keystroke Logging - The action of recording the keys struck on a keyboard in a covert manner so that the person using the keyboard is unaware that these actions are being monitored.

Local Area Network (LAN) – A private computer network generally on a DJJ IT User's premises and operated within a limited geographical area.

Network Sniffing - A tool that monitors data flowing over the network making a copy of the data but without redirecting or altering it.

Port Scanning – Users sending out a request to connect to each computer on each port sequentially and notes which ports respond or seem open to more in-depth probing. It is similar to a thief going through a neighborhood and checking every door and window on each house to see which ones are open and which ones are locked.

Virtual Private Network (VPN) - A communications service that affords various levels of privacy over public or private infrastructure.

IV. PROCEDURE

A. General Information for Account Use, Internet Use, and Network Access

1. DJJ IT Users shall acknowledge the following regarding account use, Internet use, and network access:

    a. Acceptable use and access consists of activities necessary to support the purpose, goals, and mission of DJJ and each DJJ IT User's authorized job functions or assigned tasks.

    b. Use and access are monitored by VITA/NG Partnership and there shall be no expectation of privacy.

    c. Access and use for the purpose of harassment, conducting illegal activity, personal profit, and gambling are strictly prohibited.

2. All software shall be approved by the IT Director prior to purchase and installation.

3. While this procedure is as complete as possible, no procedure can cover every situation. When there is a question regarding what constitutes acceptable use, DJJ IT Users shall consult with their supervisors, and if additional assistance is required supervisors shall consult with the Information Security Officer (ISO) (iso@djj.virginia.gov).

4. All DJJ IT Users shall safeguard IT resources from unauthorized use, intrusion, destruction, or theft. Failure to comply with this procedure may result in disciplinary action under the Department of Human Resource Management (DHRM) Standards of Conduct Policy 1.60 and DJJ Staff Code of Conduct, Administrative Procedure Vol. 1-1.2-01.

5. All DJJ IT Users shall abide by the (DHRM) Policy 1.75, Use of Electronic Communications, and Social Media (http://www.dhrm.state.va.us/hrpolicy/pol175UseOfInternet.pdf) and the requirements provided in this Administrative Procedure.

B. Account Use

1. DJJ IT Users shall not use any access control mechanism that has not been expressly assigned to them and shall not disclose or modify any assigned or entrusted access control mechanism for any purpose other than those required to perform any authorized employment functions unless properly authorized to do so in writing by the Director or the Information Security Officer (ISO).
2. DJJ IT Users agree that login IDs and passwords shall never be shared or disclosed. This includes revealing personal or network passwords to others such as coworkers, family, friends, or other members of the household, when working from home or remote locations. DJJ IT Users are accountable for any activity on the system performed with the use of their account.

C. Internet Use

1. DJJ IT Users shall adhere to the following Internet use guidelines:

   a. Accessing online games, including games found on social websites shall be prohibited.

   b. Streaming media (music or movie streaming) unless its use is business related shall be prohibited.

   c. DJJ personnel shall only use software that is part of the IT standard software suite or that has been approved by the IT Director.

   d. If using a non-COV computer, ensure that all files are scanned for viruses before introducing the files to the DJJ network (network drives and/or email). For example, if you download a research article onto your personal computer prior to

emailing it to your COV email account, scan the file for viruses using anti-virus software (e.g. McAfee, Symantec).

e. Only material and content approved through the DJJ Public Information Officer may be posted to the DJJ website. Approved content shall be posted by DJJ IT personnel.

2. Supervisors may monitor internet access:

   a. The Supervisor shall send a written request (via email or memorandum) to the DJJ ISO with the approval of the Unit Head when requesting to review a DJJ IT User's internet access.

   b. The request shall include the full name of the DJJ IT User for which the report has been requested, the nature and justification for the request, and the period to be reviewed.

D. Network Access

1. Avoid intentionally accessing network data, files, and information not directly related to your job. Existence of access capabilities does not imply permission to use this access.

2. DJJ IT Users shall only access wireless networks set up by Department of General Services or DJJ IT staff while on DJJ premises to ensure a secure connection.

3. Only authorized DJJ personnel shall set up or configure any wireless access points within DJJ premises.

4. All network traffic including, but not limited to, email, Internet, and Local Area Network (LAN) communications shall be subject to electronic monitoring.

E. Remote Access

DJJ personnel who remotely access network resources (excluding BADGE) shall use only DJJ-provided equipment configured, set up, and maintained by VITA/NG Customer Support Services without modification. Remote access to network resources, will be via broadband or Virtual Private Networking (VPN). Although, DJJ IT Users are permitted to access BADGE from non-COV devices via broadband, users shall not download any data to non-COV devices. This shall not apply to DJJ IT Users accessing Microsoft Outlook Web Access from a remote location.

Department of Juvenile Justice
Administrative Procedure

F. Unacceptable Use

1. In addition to unacceptable uses as defined in DHRM's Policy 1.75, Use of Electronic Communications and Social Media, the following statements, although not inclusive, define specific unacceptable uses for DJJ's network and systems. DJJ personnel shall not:

   a. Access data or programs to seek information on, obtain copies of, or modify files, other data, or passwords belonging to other DJJ IT Users unless authorized by the IT Director.

   b. Access, download, print, or store sexually explicit material in violation of § 2.2-2827 (http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-2827) of the Code of Virginia.

   c. Gamble.

   d. Perform activities that are illegal under local, state, federal, or international law.

   e. Knowingly send sensitive data unencrypted through email.

   f. Tamper with or otherwise attempt to circumvent security controls e.g. hardware, software, image, operating system integrity standards, and anti-virus software.

      i. Non-standard applications or operating systems that are needed for business functions will be installed by VITA/NG partnership after approval has been obtained. These requests should be submitted to DJJ's IT Director for approval (see section M of this procedure, "IT Equipment and Software Purchases and Installation," for additional information).

      ii. Periodic virus scans of all devices shall be conducted and DJJ IT Users shall not cancel these scans. Canceling of these scans increases the risk and vulnerability of the equipment and may result in the loss of the DJJ IT User's data.

   g. Advertise products.

   h. Install unauthorized hardware or software on DJJ systems.

   i. Add hardware to, remove hardware from, or modify hardware on a DJJ system.

j. Connect non-COV-owned devices such as personal computers, laptops, flash devices (USB thumb drives/memories), or hand held devices to a COV/DJJ IT system or network, except in accordance with the VITA Commonwealth Security and Risk Management Remote and Wireless Access Control Policy (VITA CSRM IT Remote and Wireless Access Controls Policy v1_0) and the COV IT Standard Use of Non-Commonwealth Computing Devices to Telework (COV ITRM SEC511).

k. Send large numbers of messages to an individual or a group (email bombing or email spamming) except to conduct DJJ business.

l. Subscribe anyone else to mailing lists.

m. Perform the following activities without the authorization of the IT Director or the ISO.

   i. Reading personal notes that someone else wrote;

   ii. Reading personal emails;

   iii. Reading personal text messages;

   iv. Posting videos of someone on the internet without their permission;

   v. Posting videos of under aged children on the internet without the permission of their parents or legal guardians; and

   vi. Going through personal items.

n. Perform activities that cause disruption to users, services, or equipment or create a hostile workplace. Disruptions include, but are not limited to, distribution of advertisements, intentional propagation of computer viruses, and using the network to gain unauthorized entry to any other machine accessible through the network.

o. Perform port scanning, network sniffing, keystroke logging, or other IT information gathering techniques when they are not part of your job responsibilities.

p. Download, install, or distribute, without the authorization of the Director, ISO, or designee:

   i. Games.

ii. Screen Savers programs.

iii. Peer-to-peer file-sharing programs.

iv. Non-VITA supported software.

q. Leave workstation unattended and unlocked for any period of time that would enable unauthorized use of the workstation.

2. Questions regarding allowable programs or materials on the DJJ network shall be directed to a supervisor or the ISO.

G. Copyright Infringement

1. DJJ IT Users shall be prohibited from using the DJJ's computer systems and networks to download, upload, or otherwise handle illegal or unauthorized copyrighted content.

2. All of the following activities constitute violations of this Administrative Procedure if done without permission of the copyright owner:

   a. Copying and sharing images, music, movies, or other copyrighted material using Peer to Peer (P2P) file sharing or unlicensed CDs or DVDs.

   b. Posting or plagiarizing copyrighted material.

   c. Downloading copyrighted files that have not been legally procured.

3. This list does not include all violations; copyright law applies to many more activities than those listed above.

H. Email Usage

1. Using any outbound email sent from a DJJ email account is to be considered equivalent to a message sent on agency letterhead, therefore:

   a. The content and tone of any such message shall reflect the official responsibilities of the author.

   b. DJJ email shall be used primarily to conduct DJJ business communications. Sending or distributing non-work related email communications using DJJ's email services is permitted as long as the personal use does not interfere with the user's productivity or work performance, does not interfere with any other

employee's productivity or work performance, and does not adversely affect the efficient operation of the Commonwealth's systems and networks.

c. Any untrue, prejudicial, misleading, obscene, racist, sexist, or other unprofessional remarks may make the organization liable for legal action and shall be considered a breach of DHRM's Standards of Conduct Policy 1.60.

d. DJJ IT Users shall not expect any privacy rights when using DJJ's email services or any other type of IT resources for electronic communication, even if those communications are of a personal nature.

e. DJJ IT Users shall adhere to the COV ITRM SEC501-08 security requirements regarding transmitting or receiving confidential juvenile information as defined in 16.1-300 of the *Code of Virginia*.

2. It shall be prohibited to:

a. Send an email using another's identity or an assumed name.

b. Use email for the propagation of viruses, computer worms, Trojan Horses (a destructive program that masquerades as a legitimate application), and other malicious software.

c. Open email attachments that are from unsolicited emails.

d. Respond to spam or suspicious email. These emails shall be deleted immediately.

e. Send attachments larger than 10 MB that will affect the performance of email service. The size limit per attachment is 10MB as per COV ITRM SEC501-08.

f. Send emails for non-work related solicitation of charitable purposes without appropriate written approval from the DJJ IT User's direct supervisor or manager.

I. Protecting Electronic Devices

1. Password-protect all computers, laptops, portable computing devices, and workstations, with the automatic screen saver or session lock up feature set for a maximum of 30 minutes.

2. Ensure unattended portable computing devices are secured from unauthorized access. For example, make sure these devices are locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

Department of Juvenile Justice
Administrative Procedure

J. Protecting Data

1. Although DJJ IT Users have access to data, they shall not read, disclose, provide, or otherwise make available, in whole or in part, such information unless disclosure is authorized by §16.1-300 of the *Code of Virginia*, the *Virginia Administrative Code*, and Virginia Department of Human Resource Management (DHRM) or DJJ Administrative Procedure VOL. I-1.9-01 Responding to Requests for Information and for purposes specifically related to the business of DJJ and the Commonwealth of Virginia.

2. DJJ IT Users acknowledge that the data contained in and accessed using DJJ's information systems and the Commonwealth's network are the property of the Commonwealth of Virginia.

3. All data files and other critical information shall be stored on a network share, such as the "U:\" drive. Network drives are backed up nightly by the VITA/NG partnership and backups are sent off-site for disaster recovery purposes. All confidential or sensitive data shall be stored on network drives or encrypted devices. No confidential or sensitive data shall be stored on a desktop or laptop unless encrypted and approved by the Information Security Officer (ISO) or the IT Director.

4. COV-issued removable media (diskettes, tapes, USB memory, and CD-ROM) shall be stored in a secure location away from extreme temperature and sunlight.

5. All obligations with respect to the confidentiality and security of all information disclosed to DJJ IT Users shall survive the termination of any agreement or relationship with DJJ.

K. Bandwidth Usage

DJJ IT Users should be aware of excessive use of DJJ bandwidth and other computer resources. Performing large file downloads and other bandwidth-intensive tasks can degrade network capacity and performance.

L. Incidental Use

1. Occasional and incidental personal use of DJJ IT resources provided by DJJ is permitted, providing such use does not violate any DJJ or Commonwealth of Virginia policies and procedures, interfere with the conduct of state business or job performance (based on volume or frequency), involve unapproved solicitation or

illegal activities, adversely affect the efficient operations of the DJJ's computer systems, harm DJJ or the Commonwealth, or involve for-profit personal business.

2. Incidental personal use of electronic mail (email), Internet access, fax machines, printers, copiers, etc., is restricted to approved DJJ IT Users; it does not extend to family members or other acquaintances.

   Note: This procedure does not attempt to define all acceptable or unacceptable personal use. The above information is provided as a guideline. If the employee is unclear about acceptable personal use, he/she shall seek the advice of his/her supervisor or Unit Head.

M. IT Software Purchases and Installation

1. All IT software purchases needed to conduct internal DJJ business shall be processed through the DJJ Procurement Department. The IT Director will review the request and coordinate the purchase to ensure compatibility with established computer and LAN system configuration standards.

2. All non-partnership supported software shall be approved by the DJJ IT Director before installation.

3. All new software requests shall be processed by submitting the "Software Installation Request Form" located on the S: / drive under the "Security SOP Forms" folder. All new software requests may take up to three (3) weeks for DJJ IT to process. Please keep in mind that final installation may take longer depending on VITA/NG Partnership availability.

N. Procedure Compliance

1. All DJJ personnel and business partners shall acknowledge acceptance of and continuing compliance with this Administrative Procedure and the requirements provided for in § 2.2-2827 of the *Code of Virginia*.

2. This acknowledgement shall be made by DJJ personnel and business partners by signing the "Acknowledgement of Information Resource Acceptable Use Procedure" (See: Attachment A) and signing the "VOL I-1 3-2 Information Security Agreement Form" prior to being granted Internet, email, and other electronic communication and IT systems access.

3. Known instances of non-compliance with this administrative procedure shall be reported to the DJJ IT User's supervisor/manager who in turn shall report the incident to the DJJ ISO (ISO@djj.virginia.gov).

4. Violations of this administrative procedure shall be handled in accordance with DHRM's Standards of Conduct Policy 1.60 and DJJ's Code of Conduct. All disciplinary actions taken under this procedure shall be determined on a case-by-case basis by the Human Resource Director or designee, in concert with DJJ's ISO, with sanctions up to or including termination, depending on the severity of the offense.

5. DJJ IT Users agree to abide by all applicable DJJ procedures, regulations, and directives that relate to the security of DJJ's computer systems and the data contained therein.

6. DJJ IT Users shall take all appropriate action to ensure the protection, confidentiality, and security of information and automated systems. DJJ IT Users shall perform their duties with quality and integrity, in a professional manner, and in keeping with established procedures. DJJ IT Users shall report all violations of information security immediately to DJJ's Information Security Officer.

V. RESPONSIBILITY

The DJJ Director, Unit Head, CSU Directors, and JCC Superintendents are responsible for the enforcement of this administrative procedure.

The Information Security Officer is responsible for reviewing and updating the Acceptable Use Administrative Procedure.

All DJJ IT Users are responsible for reading and adhering to the requirements of the Acceptable Use Administrative Procedure.

DJJ Human Resources Department is responsible for ensuring that all new hires are provided with a copy of this administrative procedure.

VI. INTERPRETATION

The IT Director or the ISO shall be responsible for granting exceptions and interpreting this procedure.

Department of Juvenile Justice
Administrative Procedure

VII. OTHER REFERENCES

- DHRM Policy 1.75, Use of Electronic Communications and Social Media (http://www.dhrm.state.va.us/hrpolicy/pol175UseOfInternet.pdf) and Standards of Conduct Policy 1.60 (http://www.dhrm.state.va.us/hrpolicy/web/pol1_60.pdf)
- Freedom of Information Act (http://foiacouncil.dls.virginia.gov/2010law.pdf)
- Commonwealth Policies, Standards, and Guidelines (http://www.vita.virginia.gov/library/default.aspx?id=537#securityPSGs)

VIII. CONFIDENTIALITY

All procedures are DJJ property and shall only be used for legitimate business purposes. Any redistribution of the documents or information contained in the procedures or bulletins shall be in accordance with applicable state and federal statutes and regulations and all other DJJ procedures. Any unauthorized use or distribution may result in disciplinary and/or criminal action, as appropriate and applicable.

Approved by: Angela Valentine	**Date:** 7/17/2017
Effective Date: August 21, 2017	**Office of Primary Responsibility:** Information Technology Services
Supersedes: Administrative Procedure ITS VOL I-1.3-7 Internet Access and Computer Utilization and Information Security	**Forms:** Attachment A: Acknowledgement of Acceptable Use of IT Resources Attachment B: Information Security Access Agreement

Department of Juvenile Justice
Administrative Procedure

ATTACHMENT A

ACKNOWLEDGEMENT OF ACCEPTABLE USE OF IT RESOURCES

I understand and agree to abide by current and subsequent revisions to the DJJ Information Resource Acceptable Use Procedure and the Code of Virginia, Section 2.2-2827 (http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-2827).

I understand that DJJ has the right to monitor any and all aspects of their computer systems and networks, Internet access, and Email usage and that this information is a matter of public record and subject to inspection by the public and DJJ management for all computer equipment provided by DJJ. I further understand that DJJ IT Users should have no expectation of privacy regarding Internet usage and sites visited or emails sent or received in such circumstances, even if the usage was for purely personal purposes.

My signature below acknowledges receipt of the DJJ "VOL. I-1.3-7 Information Resource Acceptable Use Procedure."

Employee/Business Partner Name (Print)

_____**Date**_____

Employee/Business Partner (Signature)

_____

Division/Branch:

_____