OCS

Office of Children’s Services

Empowering communities to serve youth

5.0 Information Resource Acceptable Use Policy

Prepared By: **Information Security**

Date Document Approved: **November 1, 2016**

Publication Version Control

Publication Version Control: It is the user's responsibility to ensure they have the latest version of this publication. Questions should be directed to the Office of Children's Services Information Security Officer (ISO) within the Information Technology Office. The OCS ISO will issue an agency-wide Broadcast and post the revised publication version on the agency Intranet, and provide an email announcement to parties the OCS ISO considers being interested in the change.

This chart contains a history of this publication's revisions.

Version	**Date**	**Comments**
Original	February 17, 2016	Base Document
Revision 1	October 26, 2016	Revision to modify format
Revision 2	May 20, 2019	Revised Statement of Policy Sections B, D, H, P Added Statement of Policy Section S Modified attachment A and B with OCS logo
Revision 3	August 28, 2020	No modifications
Revision 4	October 22, 2021	No modifications

Table of Contents

PURPOSE

The purpose of this policy is to create a prescriptive set of process and procedures, aligned with applicable COV IT security policy and standards, to ensure the Office of Children's Services (OCS) develops, disseminates, and updates the Information Resource Acceptable Use Policy. This policy and procedure establishes the minimum requirements for the Information Resource Acceptable Use Policy.

SCOPE

All OCS employees (classified, hourly, or business partners) as well as all OCS systems

ACRONYMS

COV:	Commonwealth of Virginia
DHRM:	Department of Human Resource Management
ISO:	Information Security Officer
IT:	Information Technology
ITRM:	Information Technology Resource Management
LAN:	Local Area Network
OCS:	Office of Children's Services
PC:	Personal Computer
SEC501:	Information Security Standard 501
VDSS:	Virginia Department of Social Services
VITA:	Virginia Information Technologies Agency
AITR:	Agency IT Resource

DEFINITIONS

See COV ITRM Glossary

BACKGROUND

The Information Resource Acceptable Use Policy at OCS is intended to facilitate the effective implementation of the processes necessary to meet the Information Resource Acceptable Use requirements as stipulated by the COV ITRM Security Standard SEC501 and security best practices. This policy directs that OCS meet these requirements for all IT systems.

ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibilities as described in the Statement of Policy section. The following Roles and Responsibility Matrix describe 4 activities:

1) Responsible (R) – Person working on activity
2) Accountable (A) – Person with decision authority and one who delegates the work
3) Consulted (C) – Key stakeholder or subject matter expert who should be included in decision or work activity
4) Informed (I) – Person who needs to know of decision or action

Roles	Agency Head	Information Security Officer	Human Resources	IT System User
Tasks				
REVIEW AND UPDATE ACCEPTABLE USE	I	A		
ENFORCE ACCEPTABLE USE		A	R	
ADHERE TO REQUIREMENTS IN ACCEPTABLE USE POLICY				A

STATEMENT OF POLICY

Though there are a number of reasons to provide network access, by far the most common is to perform job duties. This access carries responsibilities and obligations concerning acceptable use of OCS network.

Since inappropriate use of OCS systems exposes OCS to risk, this policy explains responsibilities for use of OCS information technology resources (including but not limited to computer systems, mobile devices, voice mail, email, the network, and OCS Internet connection) and specifies the actions that are prohibited.

While this policy is as complete as possible, no policy can cover every situation, so use common sense when using OCS resources. Supervisors should be consulted for any questions regarding what constitutes acceptable use.

All IT users have the responsibility for safeguarding IT resources from unauthorized use, intrusion, destruction or theft. This policy not only includes data, but also the computer systems, software, and hardware resources used to process the electronic information. Failure to comply with this policy may result in a disciplinary action under the DHRM Standards of Conduct Policy 1.60.

All OCS IT users will abide by the Department of Human Resource Management (DHRM) Policy 1.75, Use of Electronic Communications and Social Media and the following requirements.

A. ACCOUNT USE

1. Network accounts must be implemented in a standard fashion and used consistently across the organization.
2. Users of OCS IT resources are prohibited from knowingly disclosing or modifying any assigned or entrusted access control mechanism (such as: log-in identifiers, passwords, terminal identifiers, user identifiers, digital certificates, IP addresses, etc.) for any purpose other than those required to perform any authorized employment functions.
3. Accounts within the OCS organization require proper signed Access Account Request forms with specific designated access justifications. An access justification describes the specific job duties that require access to the system(s) being requested.
4. All account access should be reviewed yearly.
5. Only the director may submit a request for an Administrative Account.
6. Accounts lock if not used in 90 days and are removed after 180 days of inactivity.
7. Shared accounts are NOT permitted.
8. Use concept of Least Privilege when setting up account access.
9. The ISO or designee should suspend the worker's accounts any time they will be gone for more than 30 work days. Requests to suspend the COV email account should be sent to the ISO or designee to process. For the worker with 90 to 179 days between work dates, an email to reset the account must come from the person(s) who approved the original access request. For the worker with 180 days or more between work dates, the account must be terminated, and new access request forms must be submitted to re-establish the account access.

B. INTERNET USE

1. Acceptable use of the Internet consists of activities necessary to support the purpose, goals, and mission of the Office of Children's Services and each user's authorized job functions.
2. Tools are implemented by OCS which:
    a. Log Internet access.
    b. Monitor the Internet access and usage by individuals.
    c. Enterprise Audit Log (EAL) for access to certain sensitive systems
3. Occasional and incidental personal use of the Internet services provided by OCS is permitted during established lunch periods (less than 15 minutes in any continuous hour), break periods (less than 5 minutes), before and after established work schedule (less than 15 minutes in any continuous hour), provided such use does not violate OCS or COV policies, procedures, or practices. This use can be further limited if it is determined to be detrimental to business use of the Internet.
4. OCS users should avoid unnecessary use of Internet resources. With the implementation of web IT applications, OCS has become much more reliant on the network infrastructure

to handle client applications for core public assistance services. Excessive use of Internet resources has been linked to network/system slowdowns, lockups, lockouts, and other issues related to various system operations.

5. Accessing personal email through personal Internet Service Providers (e.g., AOL, Hotmail, Excitemail, Yahoo, Google, etc.) is also allowable (similar to personal calls on business phones). No attachments should be downloaded.
6. OCS users are prohibited from using social media including Facebook, Twitter, Instagram, and LinkedIn to conduct agency business involving sensitive case information.

NOTE: The Internet is a network of interconnected computers over which OCS has little control. The user should recognize this when using the Internet and understand that it is a public domain; the user might come into contact with information, even inadvertently, that may be considered offensive, sexually explicit, or inappropriate. The users should understand this risk during use of the Internet.

7. Following are Internet Use guidelines:
    a. Do not access online games, including games found on social websites.
    b. Do not use streaming media unless its use is business related.
    c. To access the Internet, use only software that is part of the IT standard software suite or that has been approved by IT. This software must incorporate all vendor-provided security patches required by IT.
    d. If using blogs or websites, do not discuss OCS business matters or publish material that shows OCS in a negative light. The user assumes all risks associated with blogging and social networking.
    e. Make sure all files downloaded from the Internet are scanned for viruses using the approved IT-distributed software suite and current virus detection software.
    f. Make sure content on all OCS websites is business related and has been approved by the department publishing the information.
    g. Do not make offensive or harassing material available through OCS websites.
    h. Do not post personal commercial advertising on OCS websites.
    i. Do not use OCS Internet access for personal financial gain or for personal solicitations.
    j. Do not make data available on OCS websites without ensuring that the material is accessible to only those groups and individuals who are authorized.

C. NETWORK ACCESS

1. Avoid 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. Wireless transmissions of any data are extremely vulnerable to improper recovery or inadvertent access. Due to the relative ease in recovering these transmissions, specific security requirements are necessary. Any access not specifically addressed in the OCS Information Security Policy is prohibited unless explicit permission is granted from the ISO. OCS users need to ensure when accessing external wireless connections, that the session is encrypted and appropriately secured.

D. 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.

   a. Users cannot use the OCS network or systems to:

      i. Access data or programs to seek information on, obtain copies of, or modify files, other data or passwords belonging to other users.

      ii. Access sports, and TV/video streams and audio/video clips – related to music, TV, and movies.

      iii. Access, download, print or store sexually explicit material in violation of the Code of Virginia, *§2.2-2827*.

      iv. Knowingly upload or download commercial software in violation of its copyright and/or licensing agreement.

      v. Knowingly send sensitive data unencrypted through email.

      vi. Forward a chain mail.

      vii. Gamble.

      viii. Use for product or service advertisement.

      ix. Access data or programs to seek information on, obtain copies of, or modify files, other data or passwords belonging to other users.

      x. Interfere with or disrupt network users, services or equipment. Disruptions include, but are not limited to: distribution of unsolicited advertising; intentional propagation of computer viruses; and using the network to gain unauthorized entry to any other machine accessible through the network.

      xi. Listen to radio, TV and other types of broadcasts (e.g., Webcasts, Streaming Video) that are not related to the employee's job duties and do not have prior supervisory approval. (Written approval required for Streaming Video.)

      xii. Download or install any of the following without written authorization from the ISO:

         1. Copyrighted materials (e.g., music and movie files);
         2. Games to include playing games over the Internet;
         3. Screen Savers;
         4. Peer-to-Peer (P2P) file-sharing programs; and/or
         5. Non-OCS supplied software.

      xiii. If such use interferes with the conduct of OCS business or job performance (based on volume or frequency), involves solicitation or illegal activities or adversely impacts the efficient operations of OCS computer systems, the employee's access may be limited.

      xiv. At no time should personal use of the Commonwealth's provided Internet services harm OCS, the Commonwealth or involve for-profit personal business.

      xv. The following are provided as examples of unacceptable use: routinely visiting social networking sites such as dating sites and Twitter accounts during established work periods for personal use. At times specific sites are blocked due to misuse; for example, Facebook and sports as a category. Please see B.3.

xvi. This policy does not attempt to define all unacceptable personal use. The above information is provided as a guideline. If the employee is unclear about acceptable personal use, they should seek the advice of their supervisor, Director or contact the ISO for clarification.

E. OVERUSE

1. Users should not knowingly perform actions that negatively affect the computer network or other corporate resources or that negatively affect job performance.

F. COPYRIGHT INFRINGEMENT

1. Users are prohibited from using OCS 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 Acceptable Use Policy if done without permission of the copyright owner:
    a. Copying and sharing images, music, movies, or other copyrighted material using 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.

G. REMOTE ACCESS

1. OCS employees and business partners must only use approved remote access processes and procedures when connecting remotely.

H. EMAIL USAGE

1. Any outbound email sent from an OCS email account is to be considered as equivalent to a message sent on OCS letterhead, therefore:
    a. The content and tone of any such message must reflect the official responsibilities of the author;
    b. Any untrue, prejudicial, misleading, obscene, racist, sexist, or other unprofessional remarks may make the organization liable for legal action and will be considered a breach of DHRM's Standards of Conduct Policy 1.60.
2. It is prohibited to:
    a. Send sensitive information in an email without taking steps to encrypt the sensitive information
    b. List a state email address for personal endeavors or personal business use;
    c. Send an email using another's identity, an assumed name or anonymously;
    d. Use email for the propagation of viruses, computer worms, Trojan Horses, and other malicious software.

e. Use any outside email accounts to conduct official agency business.

3. If a suspicious email is received, delete it without opening it and then empty the deleted mail folder.
4. Users may access their COV-provided email from any personal computer, smart phone, tablet, or other devices, using the Internet. Users who remotely access any other OCS resources will use only OCS-provided equipment that is configured, set up and maintained by VITA or Northrop Grumman (NG) technicians without modification or similar equipment provided by a locality that is not supported by the Commonwealth's partnership with NG.
5. If an abusive, harassing or threatening email is received, do not respond to it and report the incident to the ISO.

I. PROTECTING ELECTRONIC DEVICES

1. To protect electronic devices:
   a. Password-protect all PCs, laptops, portable computing devices, and workstations, with the automatic activation feature set for a maximum of 15 minutes.
   b. Use COV-provided encryption or other security measures to protect information stored on laptops and portable computing devices and to protect such devices from theft.
   c. Make sure all PCs, laptops, and workstations contain approved virus-scanning software with a current virus database.
   d. If a portable device supports virus-scanning software, make sure the software is active and that available anti-virus patches for the installed software are up-to-date.
   e. If it is determined that required security-related software is not installed or that a remote computer has a virus, is party to a cyber-attack, or in some way endangers the security of the OCS network, disable the account and network connection. Access will be re-established once IT determines the computer or device to be safe.
   f. Make sure 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. Logical security options include screensaver passwords and automatic session timeouts.
   g. Always lock your computer when you step away from your desk. (Ctrl + Alt + Del or Windows key + "L")
   h. Use of personally-owned equipment or storage media such as scanners, USB thumb drives, compact disks, portable hard drives, smart phones, and computers to store and/or process information that has been determined to be sensitive is strictly prohibited and not allowed according to COV Standards. If users are unsure of the sensitivity, they should not process personally-owned devices. This requirement may be waived by OCS during emergency situations. Any personally-owned electronic devices used (in violations of this policy) to store sensitive data are subject to being wiped of all data or software.
   i. To this end, non-COV owned devices cannot be directly connected to a COV network or a COV device, such as a desktop or laptop computer. Additionally, locality-owned devices cannot be used to directly access a COV network or OCS information system of record, including those systems which contain sensitive information.

J. PROTECTING DATA

1. Store all data files and other critical information on a network share, such as the "W:\" or "H:\" drive. These drives are backed up nightly and backups are sent off-site for disaster recovery purposes. All sensitive data must be stored on network drives. No sensitive data is to be stored on a desktop or laptop unless encrypted and approved by the Information Security Officer (ISO) and the agency head.
2. Store media (diskettes, tapes and CD-ROM) in a secure location away from extreme temperature and sunlight.

K. PEER-TO-PEER FILE SHARING

1. Peer-to-Peer (P2P) networking is not allowed on the OCS network under any circumstances.

L. BANDWIDTH USAGE

1. Excessive use of OCS bandwidth and other computer resources is not permitted. Perform large file downloads and other bandwidth-intensive tasks that can degrade network capacity or performance only during times of low usage.

M. INCIDENTAL USE

1. Occasional and incidental personal use of OCS IT resources provided by OCS is permitted, providing such use does not violate any OCS or Commonwealth of Virginia policies and procedures, interfere with the conduct of state business or job performance (based on volume or frequency), involve solicitation or illegal activities, adversely affect the efficient operations of OCS computer systems, harm OCS or the Commonwealth, or involve for-profit personal business.
2. Incidental personal use of electronic mail, Internet access, fax machines, printers, copiers, etc., is restricted to approved users; it does not extend to family members or other acquaintances.

Note: This policy 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 should seek the advice of his/her supervisor or division director.

N. USE FOR ILLEGAL ACTIVITIES

1. Users must not knowingly use OCS-owned or OCS-provided computer systems for activities that are considered illegal under local, state, federal, or international law.
2. Such actions include, but are not limited to:
   a. Unauthorized Port Scanning
   b. Unauthorized Network Hacking
   c. Unauthorized Packet Sniffing
   d. Unauthorized Packet Spoofing
   e. Unauthorized Denial of Service
   f. Unauthorized Wireless Hacking

g. Any act that might be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system

h. Acts of Terrorism

i. Identity Theft

j. Spying

k. Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statutes

l. Downloading, storing, or distributing copyrighted material

O. PERSONAL STORAGE MEDIA

1. Personal storage devices represent a serious threat to data security and are prohibited on the OCS network. Examples: Thumb drives, personal cloud storage, or external hard drives.

P. FLASH DRIVES

1. A COV-purchased flash drive can be used to connect to a non-COV device as well as a COV device.

    a. This practice would be appropriate with the following requirements:

    - None of the work being performed on the home computer involves the use of sensitive data in an unencrypted manner. Sensitive data, regardless if encrypted or not, cannot be stored on the local computer's C: drive. Work performed must be accessed from and saved to the COV flash drive.
    - Sensitive data on the flash drive must be encrypted.
    - Non-sensitive data on the flash drive does not need to be encrypted.
    - Work-related data stored on a COV purchased flash drive can be stored on or migrated to a COV device, such as a desktop or laptop computer.

    b. Lost flash drives need to be reported. Include a description of the information on the drive.

Q. SOFTWARE INSTALLATION

1. OCS computers are set up with a standard software suite that addresses the needs of OCS users. If additional software needs to be installed to perform OCS business, it must meet the following requirements:

    a. The software must be used in accordance with copyright laws and the licensing agreement;

    b. There must be sufficient proof of ownership; and

    c. The software must not impact the performance of OCS approved software or OCS hardware.

    d. The software must comply with sensitive data encryption in transit and at rest.

2. This policy applies to commercially produced software, shareware, public domain software and freeware. The installation or modification of any software on OCS IT systems is prohibited unless authorized in writing by the ISO or designee. Any modification or change to the standard device or system configuration as promulgated by the VITA/NG Partnership

is prohibited unless authorized in writing by the ISO or designee. The software may be analyzed by VITA/NG to ensure the integrity of our network is maintained.

R. IT EQUIPMENT AND SOFTWARE PURCHASES

1. All hardware purchases shall be done by VDSS. The hardware request is sent to the VDSS AITR by the OCS IT Manager or designee. VDSS will review agency requests and coordinate the purchase and/or placement or seat management service assets to ensure compatibility with established device and LAN system configuration standards. OCS shall purchase and maintain IT software in compliance with COV and OCS requirements.
2. Media including CDs, DVDs, thumb drives, portable hard drives if purchased by OCS monies are – by definition – COV-owned; therefore, these items can be connected and used on COV/OCS equipment and networks to store and/or transport COV/OCS data.

S. Inappropriate Use of OCS Information Systems and Data

1. Inappropriate use of information systems to gain access to sensitive information not required to perform your job may result in the indefinite suspension of access to the information system and possible criminal referral to the local Commonwealth Attorney if the sensitive information belongs to another person. The suspension remains in force regardless of where you are employed within DSS.

2. The following would be considered inappropriate use:
   a. Using a DSS/Federal/State information system to look up information about your family member;
   b. Using a DSS/Federal/State information system to look up your own information;
   c. Using a DSS/Federal/State information system to look up any person not part of a DSS case;
   d. Using a DSS/Federal/State information system to do any of the above for another co-worker or supervisor; and
   e. Sharing DSS data with another person/agency outside of an established Memorandum of Agreement

T. POLICY COMPLIANCE

1. All OCS employees and business partners must acknowledge acceptance of and continuing compliance with this policy, including the Code of Virginia, *§2.2-2827*. All users will further acknowledge that the OCS Information Resource Acceptable Use Policy may change from time to time and agree to abide by current and subsequent revisions of the policy.
2. Known instances of non-compliance with this policy should be reported to the user's supervisor/manager and the ISO.
3. Violations of this Policy will be handled in accordance with established disciplinary procedures. Disciplinary action will be determined on a case-by-case basis by appropriate OCS management, with sanctions up to or including termination depending on the severity of the violation.

4. Inappropriate use of information systems to gain access to information not required to perform your job may result in the indefinite suspension of access to the information system. The suspension remains in force regardless of where you are employed.
5. A user cannot be granted access to OCS IT systems, Internet, email or other electronic communications before signing the OCS Information Security Program Policy and OCS Information Resource Acceptable Use Acknowledgement Form.

ASSOCIATED PROCEDURE

None

AUTHORITY REFERENCE

Code of Virginia, §2.2-2005 et seq.
(Powers and duties of the Chief Information Officer "CIO" Virginia Information Technologies Agency; "VITA")

Code of Virginia, §2.2-2827
(Restrictions on state employee access to information infrastructure)

Code of Virginia, §2.2-1201, (13)
(Duties of the Department)

ITRM Information Security Policy (SEC 519)

ITRM Information Security Standard (SEC501)

IT Standard Use of Non-Commonwealth Computing Devices to Telework (ITRM SEC511-00)

OTHER REFERENCE

DHRM Policy 1.75, Use of Electronic Communications and Social Media and Standards of Conduct Policy 1.60

Freedom of Information Act

Commonwealth Policies, Standards, and Guidelines (PSGs)

Remote and Wireless Access Control Policy

IT Configuration Management Policy

IT Identification and Authentication Policy

IT Media Protection Policy

IT System and Services Acquisition Policy

IT System and Communications Protection Policy

IT System and Information Integrity Policy

ATTACHMENT A: Information Security Program Policy and Information Resource Acceptable Use Policy Acknowledgement Form

ATTACHMENT B: Information Security Access Agreement

ATTACHMENT A

Information Security Policy and Information Resource Acceptable Use and Rules of Engagement Policy Acknowledgement Form

The Virginia Department of Social Services (VDSS/Department) provides computers to Office of Children's Services (OCS) assist them in the performance of their jobs. The computer systems and networks belong to the Department, and the user may use the system for authorized purposes only.

I understand that it is my responsibility as a user to read and abide by the:

- VDSS Information Security Policy
- VDSS Information Resource Acceptable Use and Rules of Engagement Policy

even if I do not agree with them. If I have any questions about the program or policy, I understand that I need to ask Security Officer or Supervisor.

I understand that any and all databases and files I have access to may have ***confidential*** information. I understand that I am prohibited from making any unauthorized access or disclosure of ***confidential*** information. I understand that I must protect data processing and telecommunication equipment, network, software and data from accidents, misuse and unauthorized use or disclosure.

I understand that violation of this agreement may result in disciplinary action or prosecution if I knowingly and/or intentionally misuse any information obtained from the Department's data processing and telecommunications equipment, network, software or data.

I understand that VDSS and OCS have 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 may be subject to inspection by the public and VDSS, and OCS management. I further understand that I should have no expectation of privacy regarding Internet usage and sites visited or emails sent or received, even if the usage was for purely personal purposes. I understand that unacceptable use of the Internet, e-mail and other electronic communications may result in disciplinary action.

My signature below acknowledges my understanding of the VDSS Information Security Policy and the VDSS Information Resource Acceptable Use and Rules of Engagement Policy.

Complete this form:

Print Full Name ____
Signature ____
Date ____

This form is to be retained by the Security Officer.

ATTACHMENT B

Information Security Access Agreement

As a user of the Commonwealth of Virginia's information technology services, I understand and agree to abide by the following terms which govern my access to and use of these information technology services:

Access has been granted to me as a necessary privilege in order to perform authorized job functions for the Commonwealth. I understand and agree that I am prohibited from using or knowingly permitting use of any assigned or entrusted access control mechanisms (such as log-in IDs, passwords, terminal IDs, user IDs, file protection keys or production read/write keys) for any purpose other than those required to perform my authorized job functions;

I understand and agree that I will not disclose information concerning any access control mechanism of which I have knowledge unless properly authorized to do so, and I will not use any access mechanism which has not been expressly assigned to me;

I agree to abide by all applicable Commonwealth of Virginia policies, standards and guidelines and OCS policies and procedures, which relate to the security of Commonwealth information technology services and the information contained therein;

If I observe any incidents of non-compliance with the terms of this agreement, I am responsible for reporting them to the OCS Information Security Officer who is the OCS liaison personnel to the Commonwealth's Chief Information Security Officer;

By signing this agreement, I hereby certify that I understand the preceding terms and provisions and that I accept the responsibility of adhering to the same. I further acknowledge that any infractions of this agreement will result in disciplinary action, including but not limited to the termination of my access privileges.

Employee/Business Partner (Print): ___________________________ **Date:** _____________

Employee/Business Partner (Signature): ______________________________________