# COMMONWEALTH OF VIRGINIA


# Department of General Services
# Information Technology Acceptable Use Policy
# v 1.3

Approved by: _____

Joe Damico, DGS Agency Head

**Effective Date: 1/29/2018**

# *PREFACE*

### *Publication Designation*
Information Technology Security

### *Subject*
DGS Information Technology Acceptable Use Policy

### *Effective Date*
1/29/2018

### *Compliance Date*
1/29/2018

### *Supersedes*
DGS Technology Acceptable Use Policy
Date: 11/15/2016

### *Scheduled Review*
One (1) year from effective date

### *Authority*
**Code of Virginia § 2.2-603**
(Authority of Agency Directors)

**Code of Virginia, §2.2-2009**
(Additional Powers of the CIO relating to security)

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

**Code of Virginia §2.2-3803**
(Administration of systems including personal information; Internet privacy policy; exception)

**COV ITRM Policy SEC519-00**

**DGS Policy IS-2**

**COV ITRM Standard SEC501**

**DHRM Policy 1.75 –** Use of Electronic Communication and Social Media

## *Regulatory References*

1. Health Insurance Portability and Accountability Act.
2. Privacy Act of 1974.
3. Children's Online Privacy Protection Act.
4. Family Educational Rights and Privacy Act.
5. Executive Order 13231 of Critical Infrastructure Protection.

6. Federal Child Pornography Statute: 18 U.S.C. & 2252.
7. FDA CFR 21, Part 11.
8. USA Patriot Act of 2001.
9. Bank Secrecy Act.
10. Virginia Computer Crime Act, *Code of Virginia*, §18.2-152.3.,4., 5., and 6.
11. Library of Virginia Records Management Program, *Code of Virginia*, Title 42.1, Chapter 7, sec 42.1-85.
12. California Database Breach Notification Act.
13. Federal Information Security Management Act (FISMA).
14. Notification of Risk to Personal Data.
15. Office of Management and Budget (OMB) Circular A-130.
16. Sarbanes-Oxley Act (SOX).
17. Electronic Communications Privacy Act of 1986: 18 USC Part I, Ch.119, §2510 - §2522

## *International Standards*

ISO 15408, Common Criteria for Information
Technology Security Evaluation, 2009
ISO/IEC 27002: .2013, International Policy, Information technology – code of practice for information security management.

## *Acronyms and definitions*

COV: Commonwealth of Virginia
DGS: Department of General Services
ISO: Information Security Officer
ISS: Information System & Services
IT: Information Technology
ITRM: Information Technology Resource Management

Information technology (IT) resources: All COV and/or DGS provided servers, desktop computers, laptop computers, handheld devices, mobile devices, network devices or services, software, data files, facilities, fax and copiers machines, paper files and related supplies; made available to DGS Users for business and authorized personal use at the discretion of the Division Director.

DGS Users: All DGS staff and personnel including, but not limited to: full time employees, part time employees, wage employees, contractors, vendors, business partners, third party providers with direct access to IT resources, interns, visitors and any other person granted authorized use of IT resources, applications, telecommunication networks, data, and related resources that may belong to or be managed by COV and/or DGS.

Business Use: Means use that is work-related of any IT resources to facilitate the effective and efficient conduct of DGS business activities and to assist DGS staff in the performance of their job-related duties.

Personal Use: Means use that is not work-related of any IT resources. In general, incidental and occasional use of IT resources is permitted at the discretion of the Division Director or his/her designee.

Sensitive Data: is any data of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on COV and/or DGS interests, the conduct of agency programs, or the privacy to which individuals are entitled.

Personal Identifiable Information (PII): refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single person.

The following roles are defined in the COV ITRM Standard SEC501-09.1. Additionally, further outlined in the DGS TRAINING OVERVIEW AND EMPLOYEE ACKNOWLEDGEMENT OF SECURITY ROLES Information Security Office (ISO): The ISO is responsible for developing and managing the agency's information security program.

Data Owner: The Data Owner is the most senior agency manager within a Business Unit responsible for the policy and practice decisions regarding data.

Data Custodian: Data Custodians are individuals or organizations in physical or logical possession of data for Data Owners. This could be Northrop Grumman or other 3rd party vendors that Host agency data.

## Scope

In accordance with the COV ITRM SEC501-09.1 standard, this Acceptable Use Policy defines acceptable and permitted general use of COV, DGS IT resources. More restrictive policies and/or standards specific to devices, for example USB external devices for data storage or mobile devices, will be provided separately to complement this policy.

## Purpose

DGS users share DGS Information Technology (IT) resources. Everyone must use these resources responsibly since misuse by even a few individuals has the potential to disrupt DGS business mission or the work of others. Therefore, exercise ethical and appropriate behavior when using these resources.

State Law (Chapter 5 of Title 18.2 of the Code of Virginia) classifies damage to computer hardware or software (§18.2-152.4 Computer trespass; penalty), invasion of privacy (§18.2-152.5 Computer invasion of privacy; penalties), and theft of computer services (§18.2-152.6 Theft of computer services; penalties) of computer systems as (misdemeanor) crimes.
Computer fraud (§ 18.2-152.3. Computer fraud; penalty) and use of a computer as an instrument of forgery (§18.2-152.14 Computer as instrument of forgery) can be felonies.

The DGS internal procedures for enforcement of its policy are independent of possible prosecution under the law.

## Applicability

The DGS Information Technology Acceptable Use Policy as well as any other agreements, standards or policies specific to a Division or Department are applicable to all DGS Users. All DGS Users must agree and sign this policy.

## Acceptable General Use

1. All DGS users of IT resources must adhere to Virginia Department of Human Resource Management Policy number: 1.75 - Use of the Internet and Electronic Communications Systems as well as to this policy.
2. Only use IT resources that you have been authorized to.
3. Take all reasonable precautions to prevent use of your account by unauthorized person. Precautions include (but not limited to): changing passwords on a routine basis, changing default passwords and protecting files.
4. Use IT resources only for DGS authorized purposes.

5. Any DGS employee witnessing an information security incident or equipment theft must report it immediately to their supervisor and the ISO.
6. Compromised Commonwealth passwords must be reported immediately to the ISO and your supervisor - reset as quickly as possible.
7. Use of external networks connected to any COV and/or DGS IT resource must comply with the policies of acceptable use promulgated by the organizations responsible for those networks.
8. The data owner, data custodian, and/or designee may grant authorization to use data classified as sensitive and electronically stored in IT resources according with the Division policies and procedures.
9. Any DGS User of IT resources employing the Commonwealth's Internet or electronic communication systems for authorized personal use must present their communications in such a way as to be clear that the communication is personal and is not a communication of DGS or the Commonwealth.

## Prohibited General Use

1. Do not:
    a. Provide false or misleading information to gain access to IT resources. DGS may regard these actions as criminal acts and may treat them accordingly.
    b. Use Commonwealth resources to gain unauthorized access to other institutions, organizations and individuals IT resources.
    c. Share IT resource accounts or passwords with anyone. Users are responsible for all use of their accounts.
    d. Use IT resources for private consulting or to support a personal business venture, for unlawful purposes, such as the installation of fraudulently or illegally obtained software.
    e. Distribute or make available third party proprietary software without prior authorization from the licenser.
    f. Install any software on COV and/or DGS IT resources without proper authorization from Agency ISO or ISS Director.
2. Other than material known to be available to all DGS Users without restrictions, do not access, alter, copy, move or remove information, proprietary software or other files (including programs, members of subroutine libraries, data and electronic mail) from IT resources without prior authorization from Agency ISO or ISS Director.
3. You must not use the Commonwealth's Internet access or electronic communication in cases where it:
    a. Interferes with the DGS User's productivity or work performance, or with any other employee's productivity or work performance;
    b. Adversely affects the efficient operation of IT resources;
    c. Results in any personal gain or profit to the DGS User

d. Violates any provision of this policy, any supplemental policy adopted by the agency supplying the Internet or electronic communication systems, or any other policy, regulation, law or guideline as set forth by local, State or Federal law. (See Code of Virginia §2.1-804-805; §2.2-2827 as of October 1, 2001.)

## Acceptable Use – Desktop and Laptops

This policy applies to all IT resources to include, but not limited to: desktops, laptops, tablets, printer, mobile devices, and any other electronic equipment.

1. DGS Users must lock their screen when leaving their work systems unattended. To lock, press the Windows and, "L" key simultaneously.
2. DGS Users must guard Commonwealth information from unauthorized access or use. Any confidentiality agreements fully apply to COV information accessed.
3. Managers are responsible to ensure that their employees are adequately trained on appropriate use of IT equipment and that they adhere to this policy.
4. DGS Users who access IT resources from remote locations must adhere to this policy. This includes but is not limited to webmail, Citrix, VPN, eVA and DGS web-based applications.
5. Windows-based workstations used to remotely access DGS systems must be secure and running updated patches and antivirus protection.
6. Network resources and shared network drives should be used to store all DGS information. DGS Users should avoid storing DGS information or files on their desktop or laptop local hard drives (for example C: or D: drives). DGS ISS will not be held responsible for hard drive data lost due to hardware failure.
7. DGS Users are solely responsible for backing up files stored on their desktop or laptops local hard drives (for example C: or D: drives). DGS does not provide backups at the local desktop/laptop level.

## Prohibited Use – Desktop and Laptops

Activities, actions, or practices prohibited for all DGS Users concerning desktops, laptops or mobile devices include, but are not limited to, the following:

1. Connecting equipment to the network not issued by COV or DGS without first getting permission from the ISO or ISS Director.
2. Any activity, action or lack of action on the part of a user that damages or compromises DGS security.
3. Upgrading, updating or adding peripheral equipment without prior approval by the Agency ISO or ISS Director.
4. Using unlicensed software
5. Downloading and/or installing programs that are not specifically approved by ISO or ISS Director.

6. Using COV provided IT resources whether for used at DGS facilities or tele-work for un-authorized non-work related reasons or for personal gain.
7. Unauthorized access to DGS or other COV files, programs, databases or confidential information.
8. Sending confidential information to unauthorized persons without management and ISO approval.
9. Granting access to IT resources to non-DGS employees, unauthorized users to include contractors or vendors without the appropriate approval from Agency ISO or ISS Director.
10. Failing to fully cooperate with IT Security investigations when needed.
11. Allowing co-workers or other users to use the IT resources designated to you without approval from the division manager.
12. Leaving workstation unattended and unlocked for any period of time that would enable unauthorized use of the workstation.
13. Sharing logon IDs and passwords.
14. Tampering with security controls configured on IT resources.
15. Using programs or Internet web sites that compromise the privacy of DGS employees or customers by providing personal identifiable information (PII).
16. Storing sensitive data on laptops, desktops, USB drives or any other external device without first getting explicit approval from the ISO.

## Acceptable Use – Email

Acceptable use of DGS email services applies equally to on-site usage as well as remote usage of DGS email.

1. DGS email shall be used to conduct DGS business communications.
2. DGS Users shall not expect any privacy rights when using DGS email services or any other IT resources for electronic communications, even if those communications are of a personal nature.
3. Web based email is allowed on a trusted, secure personal device within your control.
4. DGS Users understand that transmitting or receiving sensitive data must be done using ISO or ISS Director approved methods and adheres to all DGS policies.

## Prohibited Email Use

Prohibited email activities, actions, or practices for all DGS Users concerning email usage include, but are not limited to, the following:

1. Sending:
    a. Sensitive information over email (unless using an ISO or ISS Director approved secure method).

b. Emails for solicitation of charitable purpose without appropriate written approval from the user's division manager.
c. Excessive amounts of data or large attachments that will affect the performance of email services. The size limit for attachments is restricted per COV Standards.
d. Spam or phishing emails to any individual or group email address.

2. Opening email attachments or clicking links from unknown sources.
3. Responding to spam or phishing emails. Phishing or threatening email must be reported to the ISO and VCCC then deleted immediately.
4. Using DGS email services for inappropriate purposes that violate legal or any DGS policy (i.e. gambling, hate or pornography).
5. The use of Google Drive is not authorized as a storage service offering and should not be used. Use of this drive is logged and monitored by VITA.

## Internet Use

Acceptable use of DGS Internet services applies equally to internet access made from DGS facilities or while tele-working.

1. DGS Internet service shall be only used for DGS business purposes.
2. Occasional and incidental personal use of internet services is allowed at the discretion of the Division Director and/or designee. Occasional and incidental use is generally limited to the employee's lunch break or before/after the work day, and must not violate any agency or Commonwealth of Virginia policies and procedures; interfere with the conduct of state business or job performance; involve solicitation or illegal activities; adversely affect the efficient operations of the agency's computer system; or harm the agency or the Commonwealth.
3. DGS Users shall not expect any privacy rights when using DGS networks.
4. DGS will limit access and use controls that prevent access to sites deemed inappropriate to include but not limited to gambling, pornographic, violence web sites. DGS has the right to monitor and control internet usage at its sole discretion and without notice provided to DGS Users.

## Prohibited Internet Use

Activities, actions, or practices prohibited for all DGS Users concerning Internet usage include, but are not limited to, the following:

1. Using DGS:
    a. Email address to register to a non-work related web site or one that does not have a clear policy for protecting privacy.
    b. Services to stream non-work related radio or video

c. Internet services for purposes that violate legal laws or any COV or DGS policy regarding gambling, hate, hacking, pornography or any other inappropriate purpose.

2. Downloading unauthorized software or inappropriate images, unless there is a business need and appropriate approval from user's manager or Division Director is obtained.
3. Accessing websites with explicit content (for example vocabulary related to sexually transmitted diseases or anatomical body parts) is only acceptable if the user's job duty requires it to fulfill the business mission. Approval from the Division Director is required.

## Compliance

1. Violation of this policy shall be reported immediately to the user's manager, who in turn will report the incident to the Agency ISO.
2. The ISO will investigate and collect facts related to the reported violation. According to the severity of a violation, disciplinary actions may include but not be limited to:
    a. Temporary restriction of computer resources access for a fixed period of time according to the seriousness of the offense.
    b. Disciplinary actions in accordance with the guidelines established in Policy 1.60 Standards of Conduct Policy.
    c. Reporting to state and federal law enforcement when necessary.
3. All formal disciplinary actions taken under this policy are subject to the Commonwealth's personnel guidelines and are executed by the Human Resources Department.

## Publication Revision Control

| Version | Date | Purpose of Revision |
|---|---|---|
| Original | 7/15/2011 | Base Document |
| 1.1 | 12/18/2014 | Updated references and the responsibilities outlined in the VITA security standard |
| 1.2 | 11/15/2016 | Added more content and updated references |
| 1.3 | 1/29/2018 | Updated policy content and references. |