Information Resource Acceptable Use Policy

EFFECTIVE DATE: 07/01/2014

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 Virginia Information Technologies Agency (VITA) 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 VITA employees (classified, hourly, or business partners) as well as all VITA systems

ACRONYMS

CIO:	Chief Information Officer
COV:	Commonwealth of Virginia
CSRM:	Commonwealth Security and Risk Management
DHRM:	Department of Human Resource Management
ISO:	Information Security Officer
IT:	Information Technology
ITRM:	Information Technology Resource Management
LAN:	Local Area Network
PC:	Personal Computer
SEC501:	Information Security Standard 501
VCCC:	VITA Customer Care Center
VITA:	Virginia Information Technologies Agency
VPN:	Virtual Private Network

DEFINITIONS

See COV ITRM Glossary

BACKGROUND

The Information Resource Acceptable Use Policy at VITA is intended to facilitate the effective implementation of the processes necessary meet the Information Resource Acceptable Use requirements as stipulated by the COV ITRM Security Standard SEC501 and security best practices. This policy directs that VITA 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 / Tasks	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 VITA's network.

Since inappropriate use of VITA's systems exposes VITA to risk, this policy explains responsibilities for use of VITA information technology resources (including but not limited to computer systems, mobile devices, voice mail, email, the network, and VITA's 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 VITA 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 and VITA Standards of Conduct Special Provisions.

All VITA 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 VITA 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.

B. INTERNET USE

1. Acceptable use of the Internet consists of activities necessary to support the purpose, goals, and mission of the Virginia Information Technologies Agency and each user's authorized job functions.
2. Tools are implemented by VITA to:

    a. Log Internet access.

    b. Monitor the Internet access and usage by individuals.

NOTE: The Internet is a network of interconnected computers over which VITA 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.

3. 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 VITA business matters or publish material that shows VITA 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 VITA websites is business related and has been approved by the department publishing the information.

    g. Do not make offensive or harassing material available through VITA's websites.

    h. Do not post personal commercial advertising on the VITA's websites.

i. Do not use VITA Internet access for personal financial gain or for personal solicitations.

j. Do not make data available on VITA's 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. Do not setup or configure any wireless access points. VITA has setup a network of wireless access points throughout the building to provide VITA users this type of access while also providing enhanced levels of security.

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

        iii. Gamble

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

        v. Knowingly send sensitive data unencrypted through email.

        vi. Tamper with or otherwise attempt to circumvent security controls.

            1. Understand that tools to inventory the hardware and software will be installed by VITA on each VITA PC and that removing, tampering or disrupting these tools in any capacity is not allowed.

            2. Understand that image and operating system integrity standards will be kept on all PC's. Non-standard applications or operating systems that are needed for business functions will be installed by VITA. These requests should be submitted to the VCCC for dispatch to VITA.

            3. PC anti-virus software will be installed on all devices connected to the VITA network. Periodic scans of all devices will be conducted and employees are prohibited from canceling these scans. Canceling of these scans can result in the immediate loss of network access for the user, until VITA can ensure that the networked device is free from viruses.

vii. Use for product advertisement.

viii. Install unauthorized encryption hardware or software on VITA systems.

ix. Add hardware to, remove hardware from, or modify hardware on a VITA system.

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

xi. Sending large numbers of messages to an individual or a group (Mail bombing).

xii. Attempting to subscribe anyone else to mailing lists.

xiii. Perform activities that might cause embarrassment, loss of reputation, or other harm to VITA.

xiv. Send out defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene, or otherwise inappropriate messages or media.

xv. Perform activities that cause an invasion of privacy.

xvi. Perform activities that cause disruption to users, services, or equipment or create a hostile workplace.

1. 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.

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

xviii. Download, install or distribute, without the authorization of the Agency Head, ISO or the agency designee:

1. Games.

2. Screen Savers.

3. Peer-to-peer file-sharing programs

4. Non-VITA supported software

If there are any questions about allowable programs or materials on the VITA network, please contact your supervisor or the ISO.

xix. Reveal personal or network passwords to others, including coworkers, family, friends, or other members of the household, when working from home or remote locations.

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 the agency'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 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

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

G. REMOTE ACCESS

1. VITA employees and business partners who remotely access agency network resources will use only VITA provided equipment configured, set up and maintained by Customer Support Services or the seat management vendor without modification. Access to network resources, including the Internet, will be via broadband or modem dial-in and Virtual Private Networking (VPN). This does not apply to users accessing Microsoft Outlook Web Access from a remote location.
2. VITA employees and business partners must only use approved remote access processes and procedures when connecting remotely.

H. EMAIL USAGE

1. Using any outbound email sent from a VITA agency email account is to be considered as equivalent to a message sent on agency 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 an email using another's identity, an assumed name or anonymously;

b. Use email for the propagation of viruses, computer worms, Trojan Horses, and other malicious software.

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 30 minutes.

   b. Use IT-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.

   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 VITA's 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.

J. PROTECTING DATA

1. Store all data files and other critical information on a network share, such as the "X:\" or "F:\" 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 VITA network under any circumstances.

L. BANDWIDTH USAGE

1. Excessive use of VITA 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 VITA IT resources provided by the agency is permitted, providing such use does not violate any agency 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 the agency's computer systems, harm the agency 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 VITA-owned or VITA-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 VITA's network.

P. SOFTWARE INSTALLATION

1. Installation of non-company-supplied programs is prohibited. Numerous security threats can pretend to be safe software; malware, spyware, and Trojans can all be installed without user knowledge through games or other programs. Additionally, software can cause conflicts or have a negative impact on system performance.

Q. IT EQUIPMENT AND SOFTWARE PURCHASES

1. All IT hardware and software purchases needed to conduct internal VITA business must be done by VITA. The VITA will review agency PC requests and coordinate the purchase and/or placement or seat management service assets to ensure compatibility with established PC and LAN system configuration standards.

R. POLICY COMPLIANCE

1. All VITA 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 VITA CSRM Information Resource Acceptable Use Policy may change from time to time and agree to abide by current and subsequent revisions of the policy.
2. This acknowledgement will be made by VITA employees and business partners by signing the "Acknowledgement of Information Resource Acceptable Use Policy" (See: Attachment A) and signing the "Information Security Access Agreement" (See: Attachment B) prior to their being granted Internet, email and other electronic communication and IT systems access.
3. Known instances of non-compliance with this policy should be reported to the user's supervisor/manager and the ISO.
4. Violations of this Policy will be handled in accordance with DHRM's Standards of Conduct Policy 1.60. Disciplinary action will be determined on a case-by-case basis by the Chief Information Officer or designee, in concert with VITA's Human Resources Office, with sanctions up to/or including termination depending on the severity of the offense.

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)

COV ITRM *IT 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)

VITA Internal Website Policies and Procedures

VITA Remote and Wireless Access Control Policy

VITA IT Configuration Management Policy

VITA IT Identification and Authentication Policy

VITA IT Media Protection Policy

VITA IT System and Services Acquisition Policy

VITA IT System and Communications Protection Policy

VITA IT System and Information Integrity Policy

ATTACHMENT A: Acknowledgement of Information Resource Acceptable Use Policy

ATTACHMENT B: Information Security Access Agreement

Version History		
Version	Date	Change Summary
1	07/01/2014	Supersedes VITA CSRM Acceptable Use IT Resources Policy and VITA CSRM PC LAN Policy

ATTACHMENT A

Virginia Information Technologies Agency

ACKNOWLEDGEMENT OF ACCEPTABLE USE OF IT RESOURCES

I understand and agree to abide by current and subsequent revisions to the VITA CSRM Information Resource Acceptable Use Policy and the Code of Virginia, Section 2.2-2827.

I understand that VITA 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 VITA management for all computer equipment provided by VITA. I further understand that 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 VITA CSRM Information Resource Acceptable Use Policy.

Employee / Business Partner Name (Print) _____ **Date**_____

Employee / Business Partner Signature _____

Division / Branch: _____

ATTACHMENT B

Information Security Access Agreement

Commonwealth of Virginia

Virginia Information Technologies Agency

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 VITA 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 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): _____

Virginia Information Technologies Agency _____
Division Name