COMMONWEALTH OF VIRGINIA

Information Technology Resource Management

Information Technology Standard
Use of Non-Commonwealth Computing Devices to Telework

Virginia Information Technologies Agency (VITA)

ITRM PUBLICATION VERSION CONTROL

ITRM Publication Version Control: It is the User's responsibility to ensure they have the latest version of this ITRM publication. Questions should be directed to ~~Director for Policy Practice and~~ *Manager of Enterprise* Architecture ~~(PPA)~~ *(EA)* within the ~~Information Technology Investments and Enterprise Solutions~~ *Relationship, Management and Governance* Directorate. ~~PPA~~ *EA* will issue a Change Notice Alert and post on the VITA Web site, provide an email announcement to the Agency Information Technology Resources (AITRs) and Information Security Officers (ISOs) at all state agencies and institutions *of higher education* as well as other parties ~~PPA~~ *EA* considers being interested in the change.

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

Version	Date	Purpose of Revision
Original	07/01/2007	Base Document
v 00.1	*November 15, 2016*	*This administrative update is necessitated by changes in the Code of Virginia and organizational changes in VITA. No substantive changes were made to this document.*

Review Process

~~Technology Strategy and Solutions~~ *Relationship, Management and Governance* Directorate Review

~~N.Jerry Smirnoff,~~ The VITA ~~Director of Information Technology Investment and Enterprise Solutions (ITIES), and Chuck Tyger, Director for Policy, Practices, and~~ *Manager of the Enterprise* Architecture Division, provided the initial review of the report.

Identifying Changes in This Document

- See the latest entry in the table above
- Vertical lines in the left margin indicate that the paragraph has changes or additions.
- Specific changes in wording are noted using italics and underlines; with italics only indicating new/added language and italics that is underlined indicating language that has changed.

The following examples demonstrate how the reader may identify updates and changes:

Example with no change to text – The text is the same. The text is the same. The text is the same.

Example with revised text – This text is the same. *A wording change, update or clarification has been made in this text.*

Example of new section – *This section of text is new.*

Agency Online Review

The report was posted on VITA's Online Review and Comment Application (ORCA) for 30 days. All agencies, stakeholders, and the public were encouraged to provide their comments through ORCA. All comments were carefully evaluated and the individual commenters were notified of the action taken.

PREFACE

Publication Designation

ITRM Standard SEC511-00.1

Subject

Information Technology Standard
Using Non-Commonwealth Owned Computing Devices to Telework

Effective Date

~~July 1, 2007~~ *December 8, 2016*

Compliance Date

~~July 1, 2007~~ *December 8, 2016*

Supersedes
TRM Standard SEC511-00

Scheduled Review

One (1) year from effective date

Authority

~~Code of Virginia § 2.2-603(G)~~
~~(Authority of Agency Directors)~~

Code of Virginia, §§ 2.2-2005 – 2.2-2032 (Creation of the Virginia Information Technologies Agency; "VITA;" Appointment of Chief Information Officer (CIO))

~~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 personnel information; Internet privacy policy)~~

Scope

In accordance with § 2.2-603, § 2.2-2009 and § 2.2-2005, all State Agencies are responsible for complying with all Commonwealth ITRM policies and standards, and considering Commonwealth ITRM guidelines issued by the Chief Information Officer of the Commonwealth. In addition*: "The director of every department in the executive branch of state government shall report to the Chief Information Officer as described in § 2.2-2005, all known incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws, or other incidents compromising the security of the Commonwealth's information technology systems with the potential to cause major disruption to normal Agency activities. Such reports shall be made to the Chief Information Officer within 24 hours from when the department discovered or should have discovered their occurrence."*

~~This *Standard* is applicable to all the Commonwealth's executive, legislative, and judicial branches, and independent agencies and institutions of higher education (collectively referred to as "Agency"). Academic "instruction or research" systems, however, are exempt from this *Standard*. This exemption, does not, however, relieve these Academic "instruction or research" systems from meeting the requirements of any other state or federal Law or Act to which they are subject. This *Standard* is offered only as guidance to local government entities. Exemptions from the applicability of this *Standard* are defined in detail in Section 1.6.of ITRM Standard 501-01.~~

Purpose

To define the minimum acceptable level of security controls necessary for eligible employees to use computers, computing devices, or related electronic equipment not owned or leased by the Commonwealth to telework.

General Responsibilities

(Italics indicate quote from the Code of Virginia requirements)

Chief Information Officer

In accordance with *Code of Virginia* § 2.2-2009, the Chief Information Officer (CIO) is assigned the following duties: *"the CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of electronic information"*

Chief Information Security Officer

The Chief Information Officer (CIO) has designated the Chief Information Security Officer (CISO) to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of the Commonwealth of Virginia's information technology systems and data.

~~**Council on Technology Services**~~

~~In accordance with the *Code of Virginia* §2.2-2009, the Council on Technology Services is assigned the following duties: "*In developing and updating such policies, procedures and standards, the CIO shall consider, at a minimum, the advice and recommendations of the Council on Technology Services.*"~~

Information Technology Advisory Council (ITAC)

Advises the CIO and Secretary of Technology on the development, adoption and update of statewide technical and data policies,

standards and guidelines for information technology and related systems.

~~**Information Technology Investments and Enterprise Solutions Directorate**~~

~~In accordance with the *Code of Virginia* § 2.2-2010, the CIO has assigned the Information Technology Investments and Enterprise Solutions Directorate the following duties: *Develop and adopt policies, standards, and guidelines for managing information technology by state agencies and institutions.*"~~

Virginia Information Technologies Agency (VITA)

At the direction of the CIO, VITA leads efforts that draft, review and update technical and data policies, standards, and guidelines for information technology and related systems. VITA uses requirements in IT technical and data related policies and standards when establishing contracts, reviewing procurement requests, agency IT projects, budget requests and strategic plans, and when developing and managing IT related services.

All State Agencies

In accordance with § 2.2-603, § 2.2-2009 and § 2.2-2005, all State Agencies are responsible for complying with all Commonwealth ITRM policies and standards, and considering Commonwealth ITRM guidelines issued by the Chief Information Officer of the Commonwealth. In addition*: "The director of every department in the state government shall report to the Chief Information Officer as described in § 2.2-2005, all known incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws, or other incidents compromising the security of the Commonwealth's information technology systems with the potential to cause major disruption to normal Agency activities. Such reports shall be made to the Chief Information Officer within 24 hours from when the department discovered or should have discovered their occurrence."*

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 of Critical Infrastructure Protection
6. Federal Child Pornography Statute: 18 U.S.C. & 2252
7. Federal Rehabilitation Act of 1973, § 508
8. Bank Secrecy Act
9. Virginia Computer Crime Act, *Code of Virginia*, §18.2-152.3.,4., 5., and 6
10. Library of Virginia Records Management Program, *Code of Virginia*, Title 42.1, Chapter 7, sec 42.1-85
11. Federal Information Security Management Act (FISMA)
12. Office of Management and Budget (OMB) Circular A-130

International Standards

1. International Standard, Information Technology – code of practice for information security management, BS ISO/IEC 17799:2005.

Definitions

See Glossary

Related ITRM Policy

ITRM Policy ~~SEC500-02:~~ Information Security Policy SEC 519-01 ~~(Revised 07/01/2007)~~

TABLE OF CONTENTS

1 Introduction

The use of Commonwealth owned or leased information technology assets is strongly encouraged for teleworking and most especially where it involves remote access to COV (Commonwealth of Virginia) computing resources. If desired, the agency head may allow the use of information technology assets not owned or leased by the COV when such use meets the provisions of this standard. Exceptions to this standard may be requested using the Exception Request form.

The intent of this standard is to protect COV information technology assets and the data they process and store while assisting to meet the COV's teleworking objectives. Because of the less structured and uncontrolled environment typical of personally owned or leased computing devices, the probability of a risk actually occurring is increased. These risks include, but are not limited to:

- Data leakage due to temporary internet files stored on personally owned or leased devices,
- Unauthorized capture of account names and passwords by malicious code installed on devices.

2 Use of Non-Commonwealth Owned or Leased Computing devices

2.1 Purpose

There are circumstances where it is acceptable for employees to use non-Commonwealth owned or leased computing devices to telework. While other solutions may be viable and will be considered on an exception basis, acceptable solutions under this standard include:

- Use of standalone devices,
- Internet access to web-based applications, and
- Internet access to remote desktop applications.

2.2 General Requirements

In order to perform Commonwealth business in a secure manner while teleworking from non-COV owned or leased computing devices, the following requirements must be met:

1. If an internet connection is necessary, then the internet connection must be reliable and provide sufficient bandwidth to allow for acceptable work productivity. Remote users are also responsible for maintaining compliance with the terms-of-service contract or acceptable use policy of their Internet Service Provider.

2. Storing of any Commonwealth data on non-COV owned or leased computing devices is prohibited due to records retention and Freedom of Information Act (FOIA) complexities, as well as the associated information security risks.

3. Any network traffic between the non-COV device and Commonwealth applications containing sensitive information must use an acceptable level of encryption, such as SSL (Secure Sockets layer), TLS (Transport Layer Security) or equivalent methodology that supports a minimum of 3DES (Triple Data Encryption Standard) or AES (Advanced Encryption Standard) with a minimal key length of 128 bits.

4. The Agency must provide training and instruction to IT system users on Agency remote access policies, standards, procedures and guidelines prior to the users' receiving remote access capabilities.

2.3 Solution Specific Requirements

2.3.1 Standalone Computing devices

Telework is acceptable using non-COV owned devices with a standalone device as this is a device that makes no network connection to Commonwealth resources. This may be a personal device that is used for web based work research, or for standard local applications that require no network connections, such as word processing.

2.3.2 Internet Access to Web-based Applications

Telework is acceptable using non-COV owned devices for Internet access to Web-based applications as these enable the secure use of applications via managing security of the connection at the application or host when the following controls at a minimum are in place:

1. Access to the application is supported by standard internet browsers and does not include client software to be installed on the user's device.
2. Access, authorization and authentication is controlled by the application.

2.3.3 Internet Access to COV Information Resources Using Remote Desktop

Telework is acceptable using non-COV owned devices to access COV Information resources such as network drives, email, and applications if using a remote desktop or terminal server application when the following controls, at a minimum are in place:

1. Applications are run from a remote desktop server or terminal server that is secured within the COV infrastructure.
2. The remote desktop or terminal server controls access, authorization and authentication to the terminal services or remote desktop service.
3. The COV application controls access, authorization and authentication as per normal internal usage.

3 Security Incident Response Regarding Non-Commonwealth Owned Computing Devices

3.1 Purpose

IT security incidents may occur while using non-Commonwealth owned or leased computing devices to perform Commonwealth business.

3.2 Requirements

Eligible employees using non-Commonwealth owned or leased computing devices to telework must be aware of the following requirements:

1. In the event a non-Commonwealth owned or leased computing device used for Commonwealth business is involved in the investigation of a security incident, the employee may be required to release the device to law enforcement or the COV Computer Security Incident Response Team (CIRT) for forensic purposes.

2. The COV CIRT is obligated to report any illegal activity uncovered during a security incident investigation, whether the activity is related to the incident being investigated or not.

3. While all investigations are confidential, the remote user concedes any expectation of privacy related to information stored on a personally owned computing device involved in a security incident.

Glossary of IT Security Definitions

Academic Instruction and Research Systems: Those systems used by institutions of higher education for the purpose of providing instruction to students and/or by students and/or faculty for the purpose of conducting research.

Access: Access: The ability to use, modify or affect an IT system or to gain entry to a physical area or location.

Access Controls: Access controls: A set of security procedures that monitor access and either allow or prohibit users from accessing IT systems and data. The purpose of access controls is to prevent unauthorized access to IT systems.

Accountability: The association of each log-on ID with one and only one user, so that the user can always be tracked while using an IT system, providing the ability to know which user performed what system activities.
Alert: Advance notification that an emergency or disaster situation may occur.

Application: A computer program or set of programs that meet a defined set of business needs. See also *Application System.*

Application System: An interconnected set of IT resources under the same direct management control that meets a defined set of business needs. See also *Application*, *Support System*, and *Information Technology (IT) System.*

Asset: Any software, data, hardware, administrative, physical, communications, or personnel resource.

Audit: An independent review and examination of records and activities to test for adequacy of controls, measure compliance with established policies and operational procedures, and recommend changes to controls, policies, or procedures.

Authenticate: To determine that something is genuine. To reliably determine the identity of a communicating party or device.

Authentication: The process of verifying an identity of a user to determine the right to access specific types of data or IT system.

Authorization: The process of granting access to data or IT system by designated authority after proper identification and authentication.
Availability: Protection of IT systems and data so that they are accessible to authorized users when needed without interference or obstruction.

Chief Information Officer of the Commonwealth (CIO): The CIO oversees the operation of the Virginia Information Technologies Agency (VITA) and, under the direction and control of the Virginia Information Technology Investment Board (the Board), exercises the powers and performs the duties conferred or imposed upon him by law and performs such other duties as may be required by the Board.

Chief Information Security Officer of the Commonwealth (CISO): The CISO is the senior management official designated by the CIO of the Commonwealth to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of COV IT systems and data.

Commonwealth of Virginia (COV): The government of the Commonwealth of Virginia, and its agencies and departments.

Commonwealth of Virginia Computer Incident Response Team (COV CIRT): a function of the Incident Management division of the COV Security Services directorate. The COV CIRT operates under the direction of the Incident Management Director, and is primarily comprised of the Incident Management engineers, with additional resources to be drawn as needed on a per incident basis from IT Partnership technical, legal and human resources staff.

Computing Devices: A *c*omputing device is a hardware component or system of components that allows a user to interact with a computer, a telephone system, or other electronic information system.

Confidentiality: The protection of data from unauthorized disclosure to individuals or IT systems.

Data: An arrangement of numbers, characters, and/or images that represent concepts symbolically.

Database: A collection of logically related data (and a description of this data), designed to meet the information needs of an organization.

Data Security: Data Security refers to those practices, technologies, and/or services used to apply security appropriately to data.

Data Storage Media: A device used to store IT data. Examples of data storage media include floppy disks, fixed disks, CD-ROMs, and USB flash drives.

Eligible Employees: Classified, appointed and hourly employees of the Commonwealth as well as Commonwealth vendors, contractors and consultants.

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

Firewall: Traffic-controlling gateway that controls access, traffic, and services between two networks or network segments, one trusted and the other untrusted.

Identification: The process of associating a user with a unique user ID or login ID.

Incident Response Capability (IRC):): The follow-up to an incident including reporting, responding and recovery procedures.

Incident Response Team: An organization within an Agency constituted to monitor IT security threats and prepare for and respond to cyber attacks.

Information Security Officer (ISO): The individual designated by the Agency Head to be responsible for the development, implementation, oversight, and maintenance of the agency's IT security program.

Information Technology (IT): Telecommunications, automated data processing, databases, the Internet, management information systems, and related information, equipment, goods, and services.

Information Technology (IT) Security: The protection afforded to IT systems and data in order to preserve their availability, integrity, and confidentiality.

Information Technology (IT) Security Architecture: The logical and physical security infrastructure made up of products, functions, locations, resources, protocols, formats, operational sequences, administrative and technical security controls, etc., designed to provide the appropriate level of protection for IT systems and data.

Information Technology (IT) Security Audit: The examination and assessment of the adequacy of IT system controls and compliance with established IT security policy and procedures.

Information Technology (IT) Security Breach: The violation of an explicit or implied security policy that compromises the integrity, availability, or confidentiality of an IT system.

Information Technology (IT) Security Controls: The protection mechanisms prescribed to meet the security requirements specified for an IT system.

Information Technology (IT) Security Incident: An adverse event or situation, whether intentional or accidental, that poses a threat to the integrity, availability, or confidentiality of an IT system.

Information Technology (IT) Security Requirements: The types and levels of protection necessary to adequately secure an IT system.

Information Technology (IT) System: An interconnected set of IT resources under the same direct management control. See also *Application System* and *Support System.*

Information Technology (IT) As used in this document, a term that includes COV employees, contractors, vendors, third-party providers, and any other authorized users of IT systems, applications, telecommunication networks, data, and related resources.

Internet: An external worldwide public data network using Internet protocols to which COV can establish connections..

Malicious Code: Harmful code (such as viruses and worms) introduced into a program or file for the purpose of contaminating, damaging, or destroying IT systems and/or data. Malicious code includes viruses, trojan horses, trap doors, worms, spyware, and counterfeit computer instructions (executables)..

Malicious Software: See Malicious Code.

Operational Risk: The possibility of a loss from events related to technology and infrastructure failure, from business interruptions, from staff related problems and from external events such as regulatory changes.

Password: A unique string of characters that, in conjunction with a logon ID, authenticates a user's identity.

Personal Digital Assistant (PDA): A digital device, which can include the functionality of a computer, a cellular telephone, a music player and a camera

Personnel: All COV employees, contractors, and subcontractors, both permanent and temporary.

Privacy: The rights and desires of an individual to limit the disclosure of individual information to others.

Privacy Officer: The privacy officer, if required by statute (such as HIPPA) provides guidance on the requirements of state and federal Privacy laws; disclosure of and access to sensitive data; and security and protection requirements in conjunction with the IT system when there is some overlap among sensitivity, disclosure, privacy, and security issues.

Remote Access: Remote access is the ability to get access to a computer or a network from a remote distance.

Remote Control: Remote Control is a technology or protocol that displays the screen of another computer (via Internet or network) on the remote user's own screen. The program allows the remote user to use a mouse and keyboard to control the other computer remotely.

Remote User: A user who accesses a computer or a network from a remote distance

Repudiation: Denial that one did or said something.

Risk: The possibility of loss or injury based on the likelihood that an event will occur and the amount of harm that could result.

Secure: A state that provides adequate protection of IT systems and data against compromise, commensurate with sensitivity and risk.

Sensitive: See Sensitivity.

Sensitivity: A measurement of adverse affect on COV interests, the conduct of agency programs, or the privacy to which individuals are entitled that compromise of IT systems and data with respect to confidentiality, integrity, and/or availability could cause.. IT systems and data are sensitive in direct proportion to the materiality of the adverse effect caused by their compromise.

Sensitivity Classification: The process of determining whether and to what degree IT systems and data are sensitive.

Session: A session is a series of interactions between two communication end points (typically a client and a server) that occur during the span of a single connection.

Threat: Any circumstance or event (human, physical, or environmental) with the potential to cause harm to an IT system in the form of destruction, disclosure, adverse modification of data, and/or denial of service by exploiting vulnerability.

Universal Serial Bus (USB): A standard for connecting devices.

USB Flash Drive: A small, lightweight, removable and rewritable data storage device.

Virus: See Malicious Code.

VPN: A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or remote users with secure access to their organization's network.

Web Application: A web application is an application that is accessed with a Web browser over a network such as the Internet or an intranet.

Workstation: A terminal, computer, or other discrete resource that allows personnel to access and use IT resources.

IT Security ACRONYMS

AITR: Agency Information Technology Representative

ANSI: American National Standards Institute

BIA: Business Impact Analysis

CAP: Corrective Action Plan

CIO: Chief Information Officer

CISO: Chief Information Security Officer

CIRT Commonwealth of Virginia Computer Incident Response Team

COOP: Continuity of Operations Plan

COPPA: Children's Online Privacy Protection Act

COTS: Council on Technology Services

DHRM: Department of Human Resource Management

DRP: Disaster Recovery Plan

FIPS: Federal Information Processing Standards

FISMA: Federal Information Security Management Act

FTP: File Transfer Protocol

HIPAA: Health Insurance Portability and Accountability Act

IDS: Intrusion Detection Systems

IPS: Intrusion Prevention Systems

IRC: Incident Response Capability

ISA: Interconnection Security Agreement

ISO: Information Security Officer

ITRM: Information Technology Resource Management

MOU: Memorandum of Understanding

OMB: Office of Management and Budget

PDA: Personal Digital Assistant

PIA: Privacy Impact Assessment

PII: Personally Identifiable Information

PIN: Personal Identification Number

RA: Risk Assessment

RBD: Risk-Based Decisions

RTO: Recovery Time Objective

SLA: Service Level Agreement

SDLC: Systems Development Life Cycle

SNMP: Simple Network Management Protocol

SOP: Standard Operating Procedure

SSID: Service Set Identifier

SSP: Security Program Plan

ST&E: Security Test & Evaluation

ITIES: Information Technology Investment and Enterprise Solutions Directorate (VITA)

USCERT: Computer Emergency Response Team

VDEM: Virginia Department of Emergency Management

VITA: Virginia Information Technologies Agency

APPENDIX

IT SECURITY POLICY AND STANDARD EXCEPTION REQUEST FORM

The form an Agency must submit to request an exception to any requirement of this Standard is on the following page.

COV IT Security Policy & Standard Exception Request Form

Agency: _____ Contact for Additional Information:_____

Requirement to which an exception is requested:

_____

1. Provide the **Business or Technical Justification:**

2. Describe the scope including quantification and requested duration (not to exceed one (1) year):

3. Describe all associated risks:

4. Identify the controls to mitigate the risks:

5. Identify any unmitigated risks:

I have evaluated the business issues associated with this request and I accept any and all associated risks as being reasonable under the circumstances.

_____ _____
Agency Head **Date**

Chief Information Security Officer of the Commonwealth (CISO) Use Only

Approved_____ Denied_____ Comments:

_____ _____
CISO Date

Agency Request for Appeal Use Only

Approved_____ Comments:

_____ _____
Agency Head Date

Chief Information Officer of the Commonwealth (CIO) Office Use Only (Appeal)

Appeal Approved_____ Appeal Denied_____ Comments:

_____ _____
CIO Date