COMMONWEALTH OF VIRGINIA

Information Technology Resource Management (ITRM)

USE OF NON-COMMONWEALTH COMPUTING DEVICES TO TELEWORK STANDARD

Virginia Information Technologies Agency (VITA)

ITRM PUBLICATION VERSION CONTROL

Reviews

This publication was reviewed and approved by the VITA Enterprise Architecture Division.

Publication Version Control

Questions related to this publication shall be directed to VITA's Enterprise Architecture Division (EA) at ea@vita.virginia.gov. EA notifies the Agency Information Technology Resources (AITRs) at all state agencies, institutions and other interested parties of proposed revisions to this document.

The following table contains a history of the revisions to this publication.

Version	Date	Purpose of Revision
Original	07/01/2007	Base Document
v. 00.1	11/15/2016	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.
v. 00.2	03/31/2021	This is an administrative update to update the document format and clarify the wording in Section 2.2.2. No substantive changes were made to this document.
Revision 1	8/10/2021	Updated Preface to reflect changes in the Code of Virginia. Removed and added verbiage in sections 2.1, . Added a new bullet to section 2.1. Removed and added verbiage in section 2.2. Added verbiage to 2.3.2. Removed and added verbiage in section 2.3.3. Added section 2.3.4 (Use of Non-COV Peripheral Devices).

Identifying Changes in This Document

- See the latest entry in the table above
  - EXA-R-01 Standard Language Example with No Change – The text is the same.
  - EXA-R-02 Technology Standard Example with Revision – The text is the same. *A wording change, update or clarification is made in this text. See italics and underlined words.*
  - EXA-R-03 Technology Standard Example of New Standard – *This standard is new.*
  - EXA-R-04 Technology Standard Example of deleted text – ~~This text was deleted.~~

PREFACE

Publication Designation
ITRM Standard SEC511-1

Subject
Using Non-Commonwealth Owned Computing Devices to Telework Standard

Effective Date
August 10, 2021

Compliance Date
November 10, 2021

Supersedes
ITRM Standard SEC511-00.2

Scheduled Review
One (1) year from effective date

Authority

Code of Virginia, §§ 2.2-2005 –2.2-2024
(Creation of the Virginia Information Technologies Agency; "VITA;" Appointment of Chief Information Officer (CIO))

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.

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.

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 Executive Branch 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."

Related ITRM Policy, Regulatory References, and Other Standards

ITRM Policy Information Security Policy SEC 519
VITA EA Smart Device Use
Health Insurance Portability and Accountability Act
Privacy Act of 1974
Children's Online Privacy Protection Act
Family Educational Rights and Privacy Act
Executive Order of Critical Infrastructure Protection
Federal Child Pornography Statute: 18 U.S.C. & 2252
Federal Rehabilitation Act of 1973, § 508
Bank Secrecy Act
Virginia Computer Crime Act, Code of Virginia, §18.2-152.3., 4., 5., and 6
Library of Virginia Records Management Program, Code of Virginia, Title 42.1, Chapter 7, sec 42.1-85
Federal Information Security Management Act (FISMA)
Office of Management and Budget (OMB) Circular A-130
International Standard, Information Technology – code of practice for information security management, BS ISO/IEC 17799:2005

Definitions
Definitions are found in the single comprehensive glossary that supports Commonwealth Information Technology Resource Management (ITRM) documents (COV ITRM Glossary).

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,
- Internet access to *COV information resources using virtual desktop infrastructure* ~~remote desktop applications~~,
- *Use of non-COV peripheral devices*

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 the associated security risks. Agencies dealing with questions in this area should also consult as appropriate with the Library of Virginia (see https://www.lva.virginia.gov/agencies/records/use-of-private.htm), the FOIA Council, and their counsel. *The following non-COV owned or leased devices have internal memory or*

storage and are prohibited from being directly connected to COV devices. These include, but are not limited to:

- *non-COV USB flash drives*
- *external hard drives*
- *smartphones*
- *digital cameras*
- *tablets*
- *personal computer*
- *e-readers*

3. Any network traffic between the non-COV device and Commonwealth applications containing sensitive information must use an acceptable level of encryption *utilizing cryptography approved per Federal Information Processing Standards (FIPS) 140-2. FIPS 140-2 specifies the security requirements that must be satisfied by a cryptographic solution.* ~~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 *or a COV approved authentication process*.

2.3.3 Internet Access to COV Information Resources Using ~~Remote Desktop~~ Virtual Desktop Infrastructure

Telework is acceptable using non-COV owned devices to access COV Information resources such as network drives, email, and applications if using an approved Virtual Desktop

Infrastructure (VDI) solution. VDI solutions host desktop environments on a central server, allowing employees to work remotely using various devices.

2.3.4 Use of Non-COV Peripheral Devices

Telework is acceptable using certain non-COV peripheral devices to connect to COV managed computers. A peripheral device is any auxiliary device that connects to and works with a computer in some way. Acceptable peripheral devices include, but are not limited to:

- *monitor*
- *mouse*
- *printer*
- *keyboard*
- *webcam*
- *speaker*
- *microphone*

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.