December 16, 2022

COMMONWEALTH OF VIRGINIA

Information Technology Resource Management

Prohibited Hardware, Software and Services Policy

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 VITA's Director for Enterprise Architecture (EA) Division within the Commonwealth Security and Risk Management Directorate. 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 EA considers to be interested in the change.

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

Version	Date	Purpose of Revision
00	9/14/2021	Initial Policy
Revision 00.1	11/4/2021	Administrative Update Adding Banned Entities per Federal Register 2021-24123
Revision 00.2	12/16/2022	Administrative Update Adding TikTok and WeChat

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. Deleted language shall be noted by ~~striking it through~~.

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

EXA-R-01 Example with No Change – The text is the same.

EXA-R-02 Example with Revision – This text is the same. *A wording change, update or clarification has been made in this text.*

EXA-R-03 Example of New Text – *This language is new*.

~~**EXA-R-03 Example of Deleted Requirement –** This requirement was rescinded on mm/dd/yyy~~.

Review Process

Enterprise Architecture (EA) Review

The Enterprise Architecture team provided the initial review of the policy.

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 individuals that provided comments were notified of the action taken.

PREFACE

Publication Designation
ITRM Policy SEC528

Subject
Information Security Policy

Effective Date
9/15/2021

Compliance Date
9/15/2021

Supersedes

Scheduled Review
Two (2) years from effective date

Most Recent Review
3/1/2021

Authority
Code of Virginia, §2.2-2009 Paragraph H (Additional Powers of the CIO relating to security)
Code of Virginia, §2.2-603
(Authority of Agency Directors)

Scope
This policy is applicable to the Commonwealth's executive, legislative, and judicial branches, as well as independent and institutions of higher education (collectively referred to as "Agency"). This policy is offered only as guidance to local government entities.

Purpose
To protect the Commonwealth by notifying all agencies of any hardware, software or services that have been prohibited for use in the Commonwealth.

General Responsibilities
(Italics indicate quote from the Code of Virginia requirements)

Chief Information Officer of the Commonwealth
In accordance with Code of Virginia, § 2.2-2009, section H, The CIO shall promptly notify all public bodies as defined in § 2.2-5514 of hardware, software, or services that have been prohibited pursuant to Chapter 55.3 (§ 2.2-5514).

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's information assets.

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.

Executive Branch Agencies Provide input and review during the development, adoption and update of statewide technical and data policies, standards and guidelines for information technology and related systems.

Judicial and Legislative Branches In accordance with the Code of Virginia §2.2-2009: the: "CIO shall work with representatives of the Chief Justice of the Supreme Court and Joint Rules Committee of the General Assembly to identify their needs."

Glossary of Security Definitions
As appropriate, terms and definitions used in this document can be found in the COV ITRM IT Glossary. The COV ITRM IT Glossary may be referenced on the ITRM Policies, Standards and Guidelines web page at http://www.vita.virginia.gov/library/default.aspx?id=537.

Related ITRM Policy Current version of the COV ITRM Policy: SEC519; Standard: SEC501 Information Security Standard; SEC525 Hosted Information Security Standard; SEC520 Risk Management Standard

TABLE OF CONTENTS

1. PROHIBITED TECHNOLOGIES POLICY

1.1 Background

The Commonwealth of Virginia (COV) utilizes numerous information technology services, hardware and software to support the missions of its agencies.

The commonwealth and the federal government have identified some services, hardware and software that must be prohibited for commonwealth usage per 2.2-2009 (section H): *The CIO shall promptly notify all public bodies as defined in § 2.2-5514 of hardware, software, or services that have been prohibited pursuant to Chapter 55.3 (§ 2.2-5514).*

All agencies are prohibited from using or contracting for information technology services that are prohibited according to this policy.

1.2 Guidance

The following sources provide identification of certain prohibited services, hardware and software

- Federal Acquisition Regulation (FAR rule, Section 889 Parts A and B)
    - Per Department of Defense (DoD); General Services Administration (GSA) and National Aeronautics and Space Agency (NASA)
- Office of Management and Budget (OMB)
- Federal Acquisition Security Council (FASC)
- *Department of Commerce*
- Others as identified

1.3 Statement of Policy

It is the policy of the COV (§2.2-603.F) that each Agency Head is responsible for securing the electronic data that is held by the agency and shall comply with the requirements of §2.2-2009. Per §2.2-2009 section H, the CIO shall promptly notify all public bodies as defined in § 2.2-5514 of hardware, software, or services that have been prohibited pursuant to Chapter 55.3 (§ 2.2-5514).

This policy prohibits executive, judicial, legislative and independent agencies from entering into, or extending or renewing, a contract with an entity that utilizes any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

2. Prohibited services, hardware and software

Commonwealth aligns this prohibition with the federal government (FAR RULE SECTION 889 Part A). The federal government prohibits obtaining (through a contract or other instrument) certain telecommunications equipment (including video surveillance equipment) or services produced by the following covered entities and their subsidiaries and affiliates.

Government Contractors Cannot Use Prohibited Telecom: this prohibits the government from contracting with any entity that uses certain telecommunications equipment or services produced by the entities listed in the statute. The interim rule was effective August 13, 2020. The Department of Defense has the authority to add additional companies to this list (FAR RULE SECTION 889 Part B).

In addition, the Office of Management and Budget has released an interim regulation outlining the interagency process that will allow agencies to bar companies from federal contracting when they constitute a supply chain security risk.

The rule, authorized by the Federal Acquisition Supply Chain Security Act of 2018, offers a number of pathways to request excluding a particular vendor from contracting with the federal government. Individual member agencies or the full Federal Acquisition Security Council (FASC) can make a recommendation, outside agencies or governmental bodies can submit a written request, or the council can consider tips from "any individual or non-federal entity that the FASC determines to be credible."

The council must then conduct "due diligence" to determine if the risks are valid, including "ensuring to the extent possible, that the information is credible or that the level of confidence in the information is appropriately taken into consideration," examining "other relevant publicly available information as necessary and appropriate" and consulting with the National Institute for Standards and Technology to ensure such exclusion is in line with federal guidelines and standards.

Currently prohibited:

- Huawei Technologies Company
- ZTE Corporation
- Hytera Communications Corporation
- Hangzhou Hikvision Digital Technology Company
- Kapersky Labs
- ByteDance (TikTok)
- Tencent Holdings Limited (WeChat)

Prohibited per Department of Commerce / Bureau of Industry and Security (Federal Register: 2021-24123):
https://public-inspection.federalregister.gov/2021-24123.pdf?utm_medium=email&utm_campaign=pi+subscription+mailing+list&utm_source=federalregister.gov

- *Candiru (Israel)*
- *NSO Group (Israel)*
- *Positive Technologies (Russia)*
- *Computer Security Initiative Consultancy PTE LTD, a.k.a. COSEINC (Singapore)*

Note: The council and sources listed in section 1.2 reserve the right to add new suppliers/contractors to the prohibited list as applicable.

3. Compliance

Compliance with this document is mandatory for all executive branch, judicial, legislative and independent agencies including all executive offices and boards/councils and prohibits agencies from entering into, or extending or renewing, a contract with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services.

4. Process for Requesting Exceptions

If an Agency Head determines that compliance with the provisions of this *policy* or any related information security standards would adversely impact a business process of the agency, the Agency Head may request approval to deviate from a specific requirement by submitting an exception request to the CISO. For each exception, the requesting agency shall fully document:

- The business need;
- The scope and extent;
- Mitigating safeguards;
- Residual risks;
- The specific duration; and
- Agency Head approval.

Each request shall be approved by the Agency Head indicating acceptance of the defined residual risks prior to submission to the CISO. Requests for exception shall be evaluated and decided upon by the CISO, and the requesting party informed of the action taken. An exception cannot be processed unless all residual risks have been identified and the Agency Head has approved, indicating acceptance of these risks. Denied exception requests may be appealed to the CIO of the Commonwealth.