Acceptable Use Policy

December 8, 2021

Virginia Tax

Purpose

The purpose of this policy is to protect the citizens and businesses of the Commonwealth from information security breaches or other data disclosures by defining the secure use of Virginia Department of Taxation's (Virginia Tax) assets. This policy expands on the Virginia Tax Information Security Policy and Virginia Department of Human Resource Management (DHRM) Policy 1.75 – Use of Electronic Communications and Social Media.

Scope

Applicable to all users granted access to Virginia Tax information systems.

***Note: For supplementary guidance to this policy (i.e. during COVID-19), see Internal Policy in SharePoint Toolbox.**

Roles

This policy categorizes user roles based on use of Virginia Tax data and systems. A user may be included in multiple categories based on his/her role. The "All Users" role is any person granted access to a Virginia Tax application or system. The "Remote Users" role applies to all users not physically located at a Virginia Tax site (includes users teleworking from home where applicable). The "Virginia Tax-Provided Mobile Device Users" role applies to all users assigned a Virginia Tax-provided device (e.g. mobile phone, tablet, etc.) other than their laptop or desktop computer. The "Supervisors" (or Manager) role is any person who has been assigned the responsibility of overseeing other personnel (i.e. contractors or vendors).

All Users

All Users Must:

1. Acknowledge that:
    a. Virginia Tax issued devices are intended for business use. Personal use is not allowed except where described in this policy.
    b. Users have no expectation of privacy while using a Virginia Tax device or connecting a personal device to Virginia Tax in one of the approved methods.
    c. All use can be monitored and used in the prosecution of unlawful behavior or otherwise as Virginia Tax determines, including, but not limited to, any violation of Virginia Tax or DHRM policies.
2. Follow all security policies and standards provided by the Virginia Tax Information Security Officer (ISO), Commonwealth of Virginia (COV), Internal Revenue Service (IRS), and any other applicable policies (e.g. PCI DSS, etc.).
3. Complete Safeguard and Security Awareness training requirements
    a. Failure to do so in a timely manner will result in account lockout.

    b. User's supervisor will be required to request the user's account be unlocked to allow the user to complete the training and continue using the system.
4. Use data and systems as authorized for business purposes only.
5. Report any security incident to the VCCC (staffed 24-hours/7-days a week) immediately, but no later than 24 hours after identification of a possible issue. In addition to the VCCC, users must also notify Virginia Tax's Security Operations and the user's supervisor when next available during normal business hours (8:30AM–5:00PM). This includes:
    a. Discovery of any theft, harm or loss of Virginia Tax-provided equipment.
    b. Discovery of any unauthorized access or use of Virginia-Tax data or systems.
        i. In the event of any unauthorized disclosure or inspection of state or Federal Tax Information (FTI), the incident must also be reported verbally (in person or by phone) and by email to the Disclosure Officer immediately but no later than 24 hours after identification of a possible issue.
6. Encrypt Email when sending sensitive data to external addresses and other COV agencies.
    a. Users must use approved Email encryption method (i.e. Virtru® in VITA-provided Gmail).
    b. Users must not send or share FTI data over Email at any time.
7. Alert their supervisor if any security control or requirement is inhibiting their work.
    - Users must not attempt to bypass any security control or circumvent any security requirement.
8. Use only the computers, accounts, files and systems that the user has been authorized to use.
9. Users may not share their laptop with others who have not been authorized access to Virginia Tax networking devices.
10. Use an agency approved method for accepting large data transfers (such as Box).
11. Laptops are not to be left in vehicles where they can be visibly seen. They must be locked in the trunk or inside a secure area.

All Users May:

12. Use Virginia Tax computers for incidental and non-disruptive personal use.
    - Incidental personal use must not violate Virginia Tax Human Resources or DHRM policies during times approved by the user's supervisor.
13. Use Virginia Tax-approved message collaboration tools (i.e. Google Hangouts)and teleconferencing services (i.e. Google Meet, Webex) provided by Virginia Tax except in the case of FTI data. **FTI data must NOT be shared using these technologies.**
    - See Virginia Tax Virtual Meeting Guidance in SharePoint Toolbox for additional details
14. Use VITA-provided cloud-based business collaboration and productivity applications (e.g. G Suite Google Docs, etc.) to share non-sensitive data.
15. Use personal devices to access email.

All Users Must Not:

16. Commit any unlawful act or any act that violates current Commonwealth, IRS, or Virginia Tax policy while using a Virginia Tax asset.
17. Take any action that jeopardizes the security of Virginia Tax or Virginia Tax customers.
18. Tamper with any security controls or attempt to bypass any security controls for any reason.

19. Install personal software on a Virginia Tax system (excludes Virginia Tax-provided mobile iPhone devices as described in this policy).
20. Add hardware to, remove hardware from or modify hardware on a Virginia Tax system.
    a. This includes the use of media drives (e.g. CD, DVD, thumb drive, portable disk, etc.) not provided by Virginia Tax.
    b. This does not include media drives (e.g. CD, DVD, thumb drive, portable disk, etc.) provided by clients or partners for business purposes.
21. Connect any non-Virginia Tax computer or computing device to the Virginia Tax network.
    a. This includes personal computers, handheld devices, etc.
    b. This does not include the use of approved remote access technologies described in this policy.
22. Allow anyone to use a Virginia Tax provided device or account or share a password to any system.
23. Use any other user's account or password.
24. Use any service account (i.e. an account intended for use by an automated process or system service) to access any system.
25. Use VITA-provided cloud-based business Email, collaboration, and productivity applications (e.g. G Suite, Google Docs, etc.) to share FTI.
26. Use personal Email, collaboration, productivity applications, or personal account IDs to conduct Virginia Tax business activities.
27. Take any Virginia Tax-provided device or access the Virginia Tax network from out of the country for any reason.
28. Download any email attachment to personal devices.
29. Re-direct government email to personal email account.

Remote Users

Remote Users Must:

30. Follow "All Users" policy items and acknowledgements above.
31. Adhere to requirements set in the Minimum Wireless Network Requirements (See Contacts and Reference section in this document).

Remote Users May:

32. Use a Wireless or Wired Network under the following conditions:
    a. User owns or controls the network to which the connection is made (i.e. the user's home network).
    b. The home wireless network is secured and encrypted at the level required by Virginia Tax. See Virginia Tax Minimum Wireless Network Requirements in SharePoint Toolbox for details.
    c. Use a Wireless "Hotspot" either personally owned (i.e. personal cell phone) or provided by Virginia Tax (i.e. MiFi® device).

Remote Users Must Not:

33. Use any public wired or wireless (WiFi) Internet (i.e. network access points in hotels, libraries, airports, client sites, restaurants, or any public location), unless a VPN connection is established immediately after connecting to the wireless access point or network jack. A VPN connection is required when using public internet for:
    - Access to business Email, cloud-based collaboration, and productivity applications (e.g. G Suite, Google Docs, etc.).
34. Use any public computer, such as those available in hotels, libraries, airports, client sites, restaurants, or any public location, to access any Virginia Tax system that requires authentication (i.e. sign on with a username and password).

Virginia Tax-Provided Mobile Device Users

Mobile Device Users Must:

35. Follow "All Users" policy items and acknowledgements above.
36. Acknowledge that Virginia Tax issued phones and tablets are intended for business use.
    - While incidental personal use is allowed, routine use requires the user to apply for and pay a fee. Doing so, under the following understanding:
        i. Personal use must not violate any other Virginia Tax policy.
37. Acknowledge that Virginia Tax Security personnel may seize the device at any time for investigation.
38. Acknowledge that the device can be wiped at the discretion of Virginia Tax without warning and for any reason including those who participate in the personal use program above.
39. Update the device Operating System within seven (7) calendar days of update notification.
    - Note: Devices may be prevented from accessing Virginia Tax assets if applicable updates/patches are not applied in this time period.
40. Virginia Tax issued iPhone must use your Tax email address to create the Apple ID to activate.

Mobile Device Users May:

41. Use a Wireless Network under the conditions outlined in the Remote User section, or use the device mobile connection.
42. Connect the device to a Virginia Tax provided computer for Sync, data transfer, or charging.
43. Download applications from the Apple iTunes store as long as they do not violate any other Virginia Tax policy including this one.

Mobile Device Users Must Not:

44. Connect the device to a personal or other non-Virginia Tax provided computer for any reason.
45. Compromise the security of the device (i.e. unauthorized modification or removal of security features).
46. Make "Operator Assisted" calls or other charged activities such as 411 directory services without a valid business need.

47. Use a Virginia Tax credit card to make iTunes media or application purchases unless they are approved through standard procurement practices.

Supervisors

Note: Where it is shown that supervisors (or managers) were aware of a user playing a part in an ongoing security violation, demonstrating a disregard for safe computing practices through repeated security incidents or failing to complete assigned training, the supervisor or manager will also be subject to disciplinary action.

Supervisors Must:

48. Ensure any users reporting to the supervisor or manager:
    a. Follow all Security policies, standards, and guidance.
    b. Complete security and Safeguard training requirements.
    c. Report any security incidents in a timely manner.
49. Ensure documented procedures and technical documentation for their functional area support Security policies and standards.
50. Report any user status change which could affect security, such as:
    a. Suspensions.
    b. Transfers.
    c. Terminations.
    d. Removal of need for Tax assets, especially mobile devices.
51. Report any security incident users become aware of to the VCCC and Security Operations immediately.
52. Manage access for those they supervise within the access management system.
    a. Conduct access reviews and certifications as instructed.
    b. Ensure user access to information and resources adheres to “Least Privilege” and “Separation of Duties” requirements.
        i. Only access Virginia Tax systems at the levels authorized by Virginia Tax.
        ii. Only complete tasks specific to job function and/or as authorized by Virginia Tax.
        iii. Note: Access not authorized by Virginia Tax will be revoked. See the Enforcement section in this document.
53. Ensure contractors and temporary workers take the Virginia Tax Annual Security Awareness training prior to receiving privileged access to Virginia Tax systems. Contractors or temporary workers must abide by the directions of this policy.

Supervisors May:

54. Request guidance and assistance from the Information Security Officer if users would like specific or general security policies or requirements explained (See Contacts and Reference below).

Supervisors Must Not:

55. Allow any user to violate Virginia Tax, Commonwealth or IRS security policies and standards.

Enforcement

Any violation of this policy may result in disciplinary action as appropriate based on user employment affiliation. Virginia Tax employees may receive disciplinary action as per Human Resource policies. Disciplinary action for all other users will be considered on a case-by-case basis by the Virginia Tax Commissioner or designee and may include termination of employment or contract.

Contacts and Reference

Who to Contact in Security:

- VITA Customer Care Center (VCCC) (Email: vccc@vita.virginia.gov, Phone: 866-637-8482)
- Security Operations (Email: Security@tax.virginia.gov), Phone: 804-404-4143)
- Information Security Officer (Email: vernon.smith@tax.virginia.gov)
- Disclosure Officer (Email: Disclosureofficer@tax.virginia.gov)

Where to Find Security Policies:

- Internal Policies in SharePoint Toolbox (https://covgov.sharepoint.com/sites/Virginia-Tax/toolbox/Policy%20Library/Forms/AllItems.aspx)
- Contact the ISO (isrm@tax.virginia.gov) for any policy questions.

Revision History

Version	Date	Reviewer	Notes
Draft	12/6/2021	Andy Tang and Toni Ferrell	Draft
1.0	12/7/2021	Vernon Smith	Draft
1.0	12/8/2021	Craig Burns	Draft

Approval

Awaiting ISO Signature

_____

Vernon Smith
Information Security Officer

Awaiting Agency Head Signature

_____

Craig Burns
Commissioner of Taxation