User IT Security Policy

Contents

PURPOSE ....................................................................................................................................................... 2

SCOPE ............................................................................................................................................................ 2

POLICY SECTIONS ...................................................................................................................................... 2

FAILURE TO COMPLY ..................................................................................................................................... 2

USE OF VRS TECHNOLOGY RESOURCES ........................................................................................................ 2

VRS Technology Resources are for VRS Use Only .......................................................................................... 2

Security Awareness Training is Required .................................................................................................. 2

Incidental Personal Use is Allowed ........................................................................................................... 2

Software Restrictions ................................................................................................................................ 2

Certain Activities Are Prohibited ............................................................................................................... 3

All VRS Technology Use is Monitored ....................................................................................................... 4

SAFEGUARDING SENSITIVE INFORMATION ................................................................................................. 4

Sensitive Information ................................................................................................................................ 4

Disclosure .................................................................................................................................................. 4

Employees Must Safeguard Sensitive Information ....................................................................................... 5

Sensitive Data Must Be Stored In a Secure Manner ....................................................................................... 5

CONTROLLING ACCESS TO SENSITIVE INFORMATION .................................................................................. 6

Access Is Limited To the Minimum Necessary for the Position ................................................................. 6

Access Privileges Cannot Be Shared .......................................................................................................... 6

Personal Device Usage Is Allowed ............................................................................................................. 6

Identification and Authentication Is Required ............................................................................................. 7

Wireless Access ......................................................................................................................................... 7

REPORTING SECURITY INCIDENTS ............................................................................................................. 8
PURPOSE
The purpose of this policy is to define the technology controls applicable to system users. In addition to this end user policy, all technology staff are responsible for adhering to all provisions in the current revision of VRS ITRM SEC501. VRS data, software, hardware, information and telecommunications are important resources and must be protected. The day-to-day security and protection of the agency’s information technology resources starts with system users.

SCOPE
The scope of this policy includes all VRS staff (full-time, part-time, wage, temporary or contractual) and agents (third-party administrators, subcontractors) who have access to VRS technology resources and assets.

POLICY SECTIONS
This policy consists of four sections:
  1. Use of VRS Technology Resources
  2. Safeguarding Sensitive Information
  3. Controlling Access to Sensitive Information
  4. Reporting Security Incidents

FAILURE TO COMPLY
Violations of this policy may lead to disciplinary action, up to and including termination.

USE OF VRS TECHNOLOGY RESOURCES
VRS Technology Resources are for VRS Use Only
VRS provides employees with access to its computer systems, applications and networks including, email and internet, for use in conducting VRS' business. Employees should exercise professional judgment when using VRS' networks and computer systems, and restrict activities to those that are business related.

Security Awareness Training is Required
All technology users are required to undergo security awareness training annually. When appropriate, the training may be specialized for different user roles and duties. Security training is required before access rights are given (or as soon as practicable thereafter).

Incidental Personal Use is Allowed
Employee’s use of email and the internet should generally be limited to VRS business. Limited, occasional, or incidental use of certain technology resources (such as phones, pc, printers, internet, etc.) for personal, non-business purposes is allowed. (See the HR Use of VRS Resources Policy for more information.) Employees are encouraged to use a personal device and the VRS Guest Wi-Fi Network when accessing the internet for non-business reasons.

Software Restrictions
Storing, using or transmitting copyrighted material and/or licensed or open source software on VRS systems is only allowed if VRS owns the software or has otherwise complied with licensing and copyright
laws governing the software. Users are not allowed to make, acquire, or use unauthorized copies of
copyrighted material, computer software, programs, executable files or documentation.

To ensure the appropriate software is available to meet VRS business needs and that the use of all
software is consistent with the software license, VRS Technology Services will provide software required
to meet business needs. The use of software that is not approved could present security and legal
threats to VRS, and such use is prohibited. Prior to acquisition, all software requests will undergo a
security risk review. To request new software see the VRS Security Review and Scan Procedures.

VRS users are prohibited from intentionally developing or experimenting with malicious programs. VRS
users are also not permitted to knowingly propagate malicious programs including opening attachments
from unknown sources or known malicious sources.

**Certain Activities Are Prohibited**

Certain activities are prohibited:

- Using electronic communications or Internet access to:
  - Harass, discriminate, stalk or act in a manner that may be construed by others as
    harassment or discrimination based on race, national origin, sex, sexual preference, age,
    disability, religious beliefs or any other characteristic protected by federal, state or local
    law;
  - Spread rumors, engage in gossip, or disparage VRS or its employees;
  - Post information or send electronic communications such as email using someone else’s
    identity;
  - Access, upload, download, transmit, print, post or store information with sexually
    explicit content as prohibited by law (see Code of Virginia §2.2-2827);
  - Access, upload, download, transmit, print, post or store threatening, obscene,
    intimidating, defamatory, harassing, discriminatory, or otherwise unlawful messages or
    images;
  - Visit game rooms, chat rooms, entertainment sites, or adult sites.

- Modifying a VRS technology asset, such as
  - Installing or using non-authorized or proprietary encryption hardware/software on VRS
    systems;
  - Tampering with security controls configured on any VRS device;
  - Adding hardware to, removing hardware from, or modifying hardware on any VRS
    device, such as removing or adding a new hard drive to a desktop computer. The
    connection of VRS-approved peripherals (monitor, mouse, speakers) is not a violation of
    this policy.

- Using VRS or Commonwealth information systems or the information contained therein to
  locate or otherwise obtain information on employees, members or other agency customers for
  personal reasons.

- Auto-forwarding of emails to external email accounts.

- Connecting non-VRS-owned devices (such as personal computers, laptops or hand held devices)
  to a VRS IT system or network, except in accordance with the current approved mobility
  solutions at VRS. See https://vrsmobility for more information.

- Any other use that is in violation of applicable local, state and federal law or is designated as
  prohibited by VRS.
All VRS Technology Use is Monitored
By using or connecting to a VRS or Commonwealth of VA (COV) owned network or computer system, employees consent to having their activity and information accessed, monitored, reviewed, recorded and stored without notice. All information transmitted, received or stored on VRS networks or systems is VRS property and may be monitored, logged, subject to Freedom Of Information Act (FOIA) or disclosed to ensure appropriate use. The Code of Virginia makes it a crime for anyone to use or examine a computer or a computer network when they know or should know they do not have the authority to view the information displayed. See § 18.2-152.5. “Virginia Computer Crimes Act” for more information.

SAFEGUARDING SENSITIVE INFORMATION
Employees may have access to sensitive information. Employees are expected to safeguard this information and such information may not be disclosed, shared, revealed to any individual or entity (including other internal VRS staff) or acted upon except in accordance with approved business processes.

Sensitive Information
Any compromise of the confidentiality, integrity and/or availability of sensitive information could have a material adverse effect on VRS or the privacy to which individuals are entitled. Examples of sensitive information include:

- Social Security Number(s)
- Data containing two or more of the following:
  - Driver’s License or state ID number
  - Credit card or Debit card number with identifying information such as pin number
  - Employee ID number
  - Any Portion of Name (First Name, Last Name)
  - Medical History (operations, full date of birth, etc.)
  - Mental Health History
  - Health Policy Number or information about application, claims, or appeals
- Any data or information containing non-public information where the release would have a negative impact on the agency, its programs and/or its stakeholders, such as:
  - Network drawings
  - Source code
  - Investment protected data such as investment strategies and non-VRS owned data
  - IT security and architectural documentation
  - Database framework or specifications
  - Any privileged information from internal or external legal counsel
  - Personnel Records
  - Vendor proprietary information
- Data protected from being released under FOIA (§ 2.2-3705.7)

Disclosure
Disclosure is defined as the act of directly or indirectly releasing, communicating or furnishing any sensitive VRS data to any individual or entity in an unauthorized manner.

Authorized Disclosure Examples:
- Two users discussing data as part of a business process when they both have access privileges to the data
- Discussing member’s data with the member after verifying the identity of that member
- Mailing member information to the member’s address on file
Unauthorized Disclosure Examples:

- Discussing data with a user or entity that does not have access privileges to the data
- Browsing VRS data for personal curiosity
- Sending sensitive information via email

Employees Must Safeguard Sensitive Information

Employees are not permitted to disclose or use at any time any VRS sensitive information except as specifically authorized by the employees’ job duties and approved business processes.

- The employee must safeguard all confidential information and data and not use or divulge the same or any part thereof directly or indirectly to anyone outside of an approved VRS business process.
- The employee must not remove any confidential or sensitive information from VRS' premises without prior permission and, upon request from VRS, must return to VRS all confidential material, property and documents in their possession.
- Employees are prohibited from accessing any sensitive information for which they have not been formally granted the necessary access privileges. Employees cannot delegate their access privileges to other employees. In other words, sensitive information can only be shared or discussed with employees who also have been formally granted the necessary access privileges.
- All requests for access to or release of confidential information that are outside of an employee’s access privileges or outside of the approved privileges of the requestor (such as requests for access and release of sensitive information to an outside entity or access to an employee’s computer or access logs) must be made by the appropriate agency authority (Director, FOIA manager, Legal Counsel, Human Resources (HR) Director, Director’s Executive Committee (DEC) member, etc.) and must be forwarded to the Information Security Office (ISO) or Chief Technology Security Officer (CTSO). No access of such information should occur without the prior approval of the ISO or CTSO.
- Email is not a secure form of communication and must not be used to send unencrypted sensitive information. Users are highly discouraged from using their VRS email account for personal reasons that could result in unwanted SPAM or targeted Phishing, such as registering at online retailers, social media, etc. Auto-forwarding of emails to external accounts is prohibited. An email sent from a VRS system may constitute a public record of the Commonwealth of Virginia, and may be subject to FOIA requests.
- Employees should limit their use of personal or contractor email accounts to conduct VRS business.
- Non-VRS owned mobile devices (phone, tablet, laptop, etc.) are prohibited from sending, receiving or storing sensitive VRS information.
- Employees are not permitted to use sensitive information or proprietary information for their own benefit, the benefit of another VRS employee or the benefit of others outside of VRS.

This duty of confidentiality extends even after the employee's employment relationship with the VRS ends and continues in perpetuity.

Sensitive Data Must Be Stored In a Secure Manner

- Employees should not leave documents containing sensitive data where unauthorized persons could view their contents or otherwise allow access by unauthorized persons.
- Electronic media containing confidential information must be stored in a locked filing cabinet or under strict password protection.
- Only VRS-owned devices and VRS-owned data storage media are allowed.
- Sensitive data is prohibited from being stored on any non-network storage device or media unless the data is encrypted and there is a written exception approved by the ISO or CTSO and the Agency Head. Examples of prohibited locations include laptop or desktop hard drives, USB thumb drives, CD or DVD media, etc.
- Any storage of VRS data on devices that are not under actual or contractual control of the VRS is prohibited. This includes, but is not limited to, Google Drive, Dropbox, iCloud or personal email/voicemail.
- Any device or data storage media that is not owned or leased by VRS is prohibited from connecting to any VRS system including servers or PCs. An exception can be made at the discretion of the ISO or CTSO.
- VRS users shall not use or store sensitive data in non-production environments. For example, sensitive data cannot be stored on a development or test environment that does not have security controls equivalent to the production environment.

CONTROLLING ACCESS TO SENSITIVE INFORMATION
Access to sensitive information in electronic systems is managed and controlled. All additions or changes to network access must be requested by a Manager or Supervisor through the Security Request System (SRS).

Access Is Limited To the Minimum Necessary for the Position
Access is based upon the principal of least privilege and granted based on a position and assigned user roles. Least privilege can be defined as the minimum access needed to accomplish assigned tasks based on the position description and assigned user roles. Local administrator rights are generally only granted to authorized staff in technology roles and require a documented exception annually from the Agency Head.

Staff that undergo changes in their work-related responsibilities are fully responsible in conjunction with their VRS management for determining any required changes to their access privileges. Access changes must be requested through established security procedures. VRS managers must request access termination immediately upon the separation of an employee.

Access Privileges Cannot Be Shared
Sharing of individual accounts is not permitted. Users are accountable for any activity performed on the system with the use of their account.

Shared accounts are not allowed on any VRS IT system. An account is considered shared whenever multiple users know the login credentials or multiple users log into the account to work. In all cases, staff granted access to an account are considered the owner of that account and are responsible for its proper use.

Personal Device Usage Is Allowed
The VRS Personal Device Program (PDP) Policy allows some employees to use their personal computing devices (smart phones, PDA, tablets) to access VRS IT systems such as email and data to facilitate VRS business. The General Polices for All Smart Devices establishes basic guidelines, responsibilities, and requirements for the use of personally owned devices.
Connecting non-VRS-owned devices to a VRS IT system or network, such as personal computers, laptops or hand held devices is prohibited, except in accordance with the current approved mobility solutions at VRS. See https://vrsmobility for more information.

**Identification and Authentication Is Required**

Access to VRS IT resources requires the unique identification of an individual to the resource. Authenticators are defined as something that confirms the proof of identity of a user to a VRS system through the memory of that user or something they have in their possession. Examples of authenticators are login IDs, passwords, 2nd factor tokens, pin numbers, etc.

Authenticators must be safeguarded at all times.
- The sharing of an authenticator and account access is prohibited
- The user is required to protect their ID via a strong password
- Authenticators must not be stored in clear text (e.g. in a standard word or excel document)
- Authenticators should be encrypted prior to storing digitally
- Documenting and storing hardware passwords must be done securely
- Initial passwords must be replaced and not reused

Users must accept the system use notification message or banner before being granted access to the system. This banner is presented to you at every first logon to a VRS desktop, laptop, or server. Remote access is allowed when authorized.

The use of remote IT resources and related connections (e.g. laptops, wireless broadband service, modems, VPN, etc.) is allowed for those staff and authorized third parties with a clear business need for such access. The employee and/or authorized third party individual must take every reasonable measure to protect VRS’s assets and must immediately notify the CTSO or the ISO if they believe IT resources have been compromised. It is the responsibility of all staff and authorized third parties to ensure a remote connection to VRS (under their control) is not accessed by unauthorized individuals, does not violate agency policies and is not in any other way misused.

**Wireless Access**

The VRS wireless network consists of three different network segments. Each of these networks will address different needs and will have different controls to regulate access and allowable network traffic.

- **Guest Wireless Network** – should be used by guests of VRS, including contractors, board members, vendor representatives, other visitors and VRS employees using personal devices for occasional personal use. The Guest Wireless Network is not intended to be used by the general public. All activity is subject to logging or monitoring. Abuse of this wireless resource could result in disconnection.
- **Mobile Smart Device Wireless Network** – should be used by VRS employees using VRS-owned smartphones and tablets and employees using personal devices under the Personal Device Program (PDP).
- **Internal Wireless Network for VRS-owned Laptops** – can only be used by VRS owned wireless devices.

The VRS Wireless Network Policy can be found on The Loop.
REPORTING SECURITY INCIDENTS

A Security Incident is any event or situation, whether intentional or accidental, that poses a threat to the integrity, availability or confidentiality of a sensitive IT system, asset or data. An incident may also include the act of violating an explicit or implied security policy.

All Information Technology Security Incidents must be reported to the ISO or CTSO on the User Incident Identification and Reporting Form as soon as possible but in all cases within 24 hours. This includes, but is not limited to, lost or stolen laptop or device, damaged device, account compromise, sharing of password, unauthorized sharing or access to sensitive data, etc.

VRS employees have a responsibility to safeguard and protect VRS technology equipment under their care. Any damage or loss of VRS technology equipment must be immediately reported to the VRS Security Manager on a VRS Incident Report. Employees should contact Information Security or the VRS Service Desk immediately if they believe that malware has affected their computer.