Title: Acceptable Use Policy Policy: 6115

Purpose

The purpose of the Acceptable Use policy is to identify and provide all users, including system owners, data owners, system administrators, and data custodians with awareness of their responsibilities for acceptable use of VSU computer systems and data.

Authority, Responsibility, and Duties

1. The IT Security program roles and responsibilities are assigned to individuals and may differ from the actual role title or working title of the individual's position. Individuals may be assigned multiple roles, as long as, the multiple role assignments provide adequate separation of duties, provide adequate protection against the possibility of fraud, and do not lead to a conflict of interests. Refer to Information Security Policy 6110 for roles and responsibilities.
2. All users of electronic resources and systems are expected to use the University's electronic resources and IT systems in a professional manner that demonstrates respect for confidentiality, integrity and availability of data, and intellectual property rights. All users also accept personal responsibility for any actions that constitute a violation of this policy.

Definitions

The IT security definitions and terms can be found in the COV ITRM IT Glossary. It is referenced on the ITRM Policies, Standards, and Guidelines web page on www.vita.virginia.govllibrary.

Policy Statements

1. This policy applies to all University employees (permanent, temporary, contractual, faculty, administrators, and interns) who are responsible for the development, coordination, and execution and use of VSU information technology resources to conduct University business and to transmit sensitive data in the performance of their jobs.
2. All members of the University community are expected to use the University's electronic resources and IT systems in a professional manner that demonstrates respect for confidentiality, integrity and availability of data, and intellectual property rights.
3. All uses of electronic resources and systems must be for their intended use and such use must comply with applicable local, state, and federal laws, copyright laws, and University policies.
4. Users of the University's electronic resources and systems accept personal responsibility for any actions that constitute a violation of this policy.
5. Personal use of the University's electronic resources and systems is permitted only when such use is incidental and occasional. Personal use is prohibited when:

a. It interferes with the user's productivity or work performance, or with any other employee's productivity or work performance;
b. I t adversely affects the efficient operation of the computer system; or,
c. It violates any provision of this policy.

6. In making acceptable use of University IT systems and resources, IT system users are prohibited from, and NOT allowed to:
   a. Install or use proprietary encryption hardware/software on University's IT computers.
   b. Tamper with or disable security controls configured on the University's computers, workstations or mobile devices.
   c. Install personal software on the University's computers including workstations and mobile devices or make or use illegal copies of copyright materials or software, store such copies on University systems, or transmit them over the University network.
   d. Add hardware to, remove hardware from, or modify hardware on the University's IT computers including workstations or mobile devices.
   e. The use of USB thumb drives or any other storage device on any University owned asset. If this needs to be saved on a removable drive, staff should use an encrypted drive for sensitive or proprietary and file an exception with the ISO for a regular thumb drive for non-sensitive or non-proprietary file removal.
   f. Connect non-University owned devices to the University intranet network (private network), such as personal computers, laptops, or hand held devices except in accordance with then-current COV ITRM of Non-Commonwealth Computing Devices to Telework Standard.
   g. Access, download, print, or store information with sexually explicit content as prohibited by law (see Code of Virginia §2.1-804-805; §2.2-2827 as of October 1, 2001).
   h. Download or transmit fraudulent, threatening, obscene, intimidating, defamatory, harassing, discriminatory, or otherwise unlawful messages or images.
   1. Send e-mail using another's identity, an assumed name, or anonymously.
   J. Forward proprietary or confidential VSU email to any personal email address.
   k. Store or forward any proprietary or confidential VSU in any non-VSU cloud storage service such as iCloud, Drive, etc.
   l. Use another person's system, user id, password, files, or data.
   m. Engage in any activity that might be purposefully harmful to systems, or to any information thereon such as creating or propagating viruses, disrupting services, or damaging files or making unauthorized modification to University data.

7. Privacy Statement
   a. There is no expectation of privacy in any message, file, image, or data created, sent, retrieved, or received by use of the University's electronic resources and systems.
   b. All messages transmitted by facsimile, e-mail, or the Internet shall be treated as job-related or academic material to carry out Virginia State University's educational mission.

c. At any time, the Technology Services department shall reserve the right (with or without cause) to monitor, access, and disclose all data created, sent, received, processed, or stored on University computers, laptops, hand held devices, computer equipment, University network, or electronic communications and report any suspicious activity to the appropriate authorities.

8. Exceptions to this Policy

Exceptions to this policy will require a documented request that details the business case for the exception, specifically what requirement the exception is for, and what mitigating controls will be implemented to protect the University. Refer to Information Security Policy 6110 for the requirements and process to file an exception.

9. Violations of Policy

Violation of this policy may result in disciplinary action under the Virginia Department of Human Resources Policy 1.60, Standards of Conduct (4116/08, 6/1/11).

References

Virginia Department of Human Resources Management:

Policy 1.60 Standards of Conduct (4/16/08, 611/11)
Policy 1.75 Uses of Electronic Communication and Social Media (8/01101, 3117/11)

Virginia Information Technology Agency (VITA):

Information Security Standards (SEC501-09) (02/20/2015)

Approval By: _____ Date: 5/10/16
President