West Virginia University
Information Technology Services
16-001 Acceptable Use Policy

Effective: August 13th, 2016
Updated / Revised: August 13th, 2016
Next Scheduled Review: (every 3 years from the date of approval)
Contact: Chief Information Security Officer, Information Technology Services

Purpose

The purpose of this policy is to establish the acceptable use of West Virginia University (WVU) technology and data resources, which are provided to faculty, staff, students, and third parties to advance the mission of academics, research, and community outreach.

Scope

This policy applies to all faculty, staff, students and third parties who store, use, transfer, transport, produce, or dispose of technology and data resources owned or managed by WVU.

Definitions

Personally Identifiable Information (PII) – information that can be used on its own or with other information to identify a single person, or multiple persons.

Credit Card information – in addition to the credit card number this can include the card holder's name, address, Social Security Numbers (SSN), and any other PII stored on the credit card.

FERPA – The Family Educational Rights and Privacy Act of 1974 is the federal law that governs access to educational information records.

HIPAA – The Health Insurance Portability and Accountability Act of 1996, under Title 2, requires the establishment of policies, and guidelines for maintaining the privacy and security of individually identifiable health information.

PCI-DSS – Payment Card Industry Data Security Standards are the standards developed by the major credit card issuers (Visa, MasterCard, American express, Discover and JCB) on merchant responsibilities for processing credit card transactions.

Policy

Acceptable use is conducting activities on WVU data and technology resources by authorized individuals for the purpose for which access was granted and does not disrupt operations and is not otherwise prohibited or considered unacceptable use under this policy. Users of WVU data and technology should also consider the following:

1. Users of WVU data and technology resources must adhere to all applicable WVU policies, standards, procedures, contracts and licenses, as well as applicable federal, state, and local laws and regulations.

2. WVU data and technology resources shall only be used by authorized individuals for the purpose for which access was granted.

3. Incidental personal use of technology resources, not including data resources, is permitted; however, users of WVU technology resources are advised that they should have no expectation of privacy or confidentiality in connection with the personal use of these resources. Personal use is only permissible if the use does not:

   a. Consume more than a trivial amount of resources that could be otherwise used for business purposes.
   b. Interfere with worker productivity.
   c. Preempt any business activity.
   d. Promote or result in a hostile work or academic environment.

4. The University reserves the right to monitor technology resources and the use of technology resources for operational needs and to ensure compliance with applicable laws and WVU policies and standards. To that end, users have no expectation of privacy in anything they create, store, send, or receive on WVU data and technology resources.

5. When the University receives a Freedom of Information Act request, subpoena, litigation or other similar request for information or documents, the University will take necessary measures to access WVU data and technology resources in order to comply with its legal obligations.

Unacceptable use is any unauthorized use of WVU data and technology resources or any use that disrupts or endangers WVU data and technology. The following constitutes unacceptable use

1. Exposing University data and technology resources to unauthorized access through means that include, but are not limited to, the following:

   a. Leaving the means of authentication in a location where it can be readily obtained by another individual (Example: writing one's password on a note affixed to one's monitor or keyboard.)
   b. Stepping away from a computer without securing it in some fashion (Examples: locking it with a screen saver or logging out.)
   c. Sharing a personal password or other means of authentication with another individual.
   d. Providing another person access to University technology and data resources under your authentication.
   e. Failing to secure files containing Social Security Numbers or credit card information as explained in the Sensitive Data Protection policy (http://it.wvu.edu/security/governance.)
   f. Failing to secure files containing confidential or limited access data resources. Such files might include, but are not limited to; personally identifiable information (PII); credit cardholder data; and any information associated with a federal, state, or third party mandate such as FERPA, HIPAA or PCI-DSS.

g. Failing to secure media containing confidential or limited access data. (Examples: flash drives or other portable devices, CDs, DVDs, or paper.)

h. Failing to destroy media containing confidential or limited access data resources when it is no longer needed. (Examples: printouts of such data should be shredded and data on magnetic media should be erased.)

2. Unauthorized access to or use of data or technology resources through means that include, but are not limited to, the following:

a. Using another person's credentials to gain access to University technology or data resources.

b. Using University technology and data resources to gain unauthorized access to resources of other institutions, organizations, or individuals. This includes the unauthorized downloading of copyrighted materials.

c. Accessing confidential or limited access data resources for reasons unrelated to one's job.

d. Using false or misleading information to acquire access to University technology or data resources.

e. Bypassing, subverting, or otherwise rendering ineffective the security or access control measures for any University technology or data resource.

3. Unauthorized destruction, damage, disruption, or impairment of University technology or data resources through means that include, but are not limited to:

a. Intentionally, recklessly, or negligently damaging any technology or data resource by any means. (Example: introducing malicious software into a computer system.)

b. Altering, moving, or removing software, system logs, configuration files, or other files needed for the proper operation of a computer system without prior authorization.

c. Using any technology or data resource in a manner that adversely affects the work of others.

4. Unauthorized commercial activities, including, but not limited to, the following:

a. Using University technology or data resources for one's own commercial gain, or for other commercial purposes not expressly approved by the University.

b. Using University technology or data resources to operate or support a personal or other non-University-related business.

c. Use of University resources in a manner inconsistent with the University's contractual obligations to suppliers of those resources or with any published University policy.

5. Unauthorized activity by WVU employees (administrators, faculty and staff), includes, but is not limited to:

    a. Inappropriate use of WVU-owned or operated technology systems to transmit, retrieve, access, print; or store any communication or content of a defamatory, discriminatory, harassing, obscene, or sexually explicit nature. Enforcement of this unauthorized activity must be followed in conjunction with other WVU policies, procedures or guidelines that govern appropriate workplace conduct and behavior.

Rights and Responsibilities

1. All users of WVU data and technology resources are expected to use good judgment and exercise decency and common sense. This includes, but is not limited to:

    a. Using WVU data and technology resources in a lawful and appropriate manner.
    b. Respecting the rights and privacy of others.
    c. Maintaining WVU data and technology resources in an appropriate manner. (Examples; maintaining anti-virus software, patching operating systems and applications, and using authentication for all technology resources.)
    d. Using the University's marks (e.g., trademarks, logos) only as authorized and not representing personal comments as being those of the University.

Enforcement

WVU's Chief Information Officer and Chief Information Security Officer will coordinate with appropriate University entities on the implementation of this policy.

Violation or non-compliance of this policy will be addressed in accordance with established WVU disciplinary policies and procedures, as issued and enforced by the appropriate authorities. Failure to comply with this or other related standards may result in disciplinary action up to and including termination of employment or studies.

Relevant Documents

Links

- Family Educational Rights and Privacy Act (FERPA) – http://www2.ed.gov/**ferpa**/
- Health Information Portability and Accountability Act (HIPAA) - http://www.hhs.gov/hipaa
- Payment Card Industry Data Security Standards (PCI-DSS) - https://www.pcisecuritystandards.org/pci_security/

Policies

- WVU FERPA – http://ferpa.wvu.edu
- ITS Information Security - http://it.wvu.edu/security/governance
- WVU Human Resources - http://www.hr.wvu.edu/policies
- WVU ResNet Acceptable Use - http://www.resnet.wvu.edu/policy/resnet.html
- WVU Student Conduct Code - http://campuslife.wvu.edu/r/download/180235