1. PURPOSE & SCOPE:

1.1 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.

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

2. POLICY:

2.1 Acceptable Use. 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 is considered acceptable use.

2.1.1 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.

2.1.2 WVU data and technology resources shall only be used by authorized individuals for the purpose for which access was granted. Access to WVU data and technology resources must be based on least privilege or on a need-to-know basis depending on the individual’s job responsibilities.

2.1.3 Incidental personal use of technology resources, not including data resources, is permitted; however, users of WVU technology resources are advised that they should
ITS Policy 1.0
Acceptable Use of Data and Technology Resources

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:

2.1.3.1 Consume more than a trivial amount of resources that could be otherwise used for business purposes;

2.1.3.2 Interfere with worker productivity;

2.1.3.3 Preempt any business activity; or,

2.1.3.4 Promote or result in a hostile work or academic environment.

2.1.4 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 should have no expectation of privacy in anything they create, store, send or receive on WVU data and technology resources.

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

2.2 Unacceptable Use. 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:

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

2.2.1.1 Leaving the means of authentication in a location where it can be readily obtained by another individual (e.g., writing one’s password on a note affixed to one’s monitor or keyboard).

2.2.1.2 Stepping away from a computer without securing it in some fashion (e.g., locking it with a screen saver or logging out).
ITS Policy 1.0
Acceptable Use of Data and Technology Resources

Category: Acceptable Use of Technology
Title: Acceptable Use of Data and Technology Policy
Responsible Unit: Information Technology Services
Effective: August 13, 2016
Revision History: March 27, 2017
Review Date: March 2020

2.2.1.3 Sharing a personal password or other means of authentication with another individual.

2.2.1.4 Providing another person access to University technology and data resources under your authentication.

2.2.1.5 Failing to secure files containing Social Security numbers or credit card information as outlined in the Sensitive Data Protection Policy.

2.2.1.6 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 card holder data; and any information associated with a federal, state or third party mandate such as FERPA, HIPAA or PCI-DSS.

2.2.1.7 Failing to secure media containing confidential or limited access data resources when it is no longer needed (e.g., shredding printouts or erasing magnetic media).

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

2.2.2.1 Using another person’s credentials to gain access to University technology or data resources.

2.2.2.2 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 as outlined in the Digital Millennium Copyright Act.

2.2.2.3 Accessing confidential or limited access data resources for reasons unrelated to one’s job.

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

2.2.2.5 Bypassing, subverting or otherwise rendering ineffective, the security or access control measures for any University technology or data resource.
ITS Policy 1.0
Acceptable Use of Data and Technology Resources

Category: Acceptable Use of Technology
Title: Acceptable Use of Data and Technology Policy
Responsible Unit: Information Technology Services
Effective: August 13, 2016
Revision History: March 27, 2017
Review Date: March 2020

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

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

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

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

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

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

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

2.2.4.3 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.

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

2.3 All users of WVU data and technology resources are expected to use good judgement and exercise decency and common sense. This includes, but is not limited to, the following:
ITS Policy 1.0
Acceptable Use of Data and Technology Resources

Category: Acceptable Use of Technology
Title: Acceptable Use of Data and Technology Policy
Responsible Unit: Information Technology Services
Effective: August 13, 2016
Revision History: March 27, 2017
Review Date: March 2020

2.3.1 Using WVU data and technology resources in a lawful and appropriate manner.

2.3.2 Respecting the rights and privacy of others.

2.3.3 Maintaining WVU data and technology resources in an appropriate manner (e.g., using anti-virus software, patching operating systems and applications and using authentication for all technology resources).

2.3.4 Using the University’s marks (e.g., trademarks, logo) only as authorized and not representing personal comments as being those of the University.

3. DEFINITIONS:

3.1 **Authorized individuals:** Faculty, staff, students and third-parties who have assigned WVU Login credentials which provide access to WVU data and technology resources.

3.2 **Credit card information:** In addition to the credit card number, this data can also include the card holder’s name, address, Social Security number (SSN) or any other PII stored on the credit card.

3.3 **FERPA:** The Family Educational Rights and Privacy act of 1974 is the federal law that governs access to educational information records.

3.4 **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.

3.5 **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.

3.6 **Personally identifiable information (PII):** Data that identifies the individual including, but not limited to, Social Security numbers, driver’s license numbers, credit card numbers,
bank account information, employee performance or salary information, student grades, disciplinary information or account passwords.

3.7 **WVU third-party:** An individual or an entity that has an affiliation with WVU (e.g., retirees, consultants, presenters, camp attendees, vendors).

## 4. ENFORCEMENT:

4.1 WVU’s Chief Information Officer, supported by the Chief Information Security and Privacy Officer, will coordinate with appropriate University entities on the implementation and enforcement of this policy.

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

## 5. CROSS REFERENCES:

5.1 All other University policies are also applicable to the electronic environment. Relevant institutional policies include, but are not limited to:


5.1.2 [WVU FERPA Policies](https://www.wvu.edu/services/records/cas/casinfo/ferpa)

5.1.3 ITS Policy 3.2 [Sensitive Data Protection](https://www.wvu.edu/services/techservices/its/policy/3.2)

5.1.4 [Digital Millennium Copyright Act (DMCA)](https://www.copyright.gov/dmca/)

5.1.5 [Health Information Portability and Accountability Act (HIPAA)](https://www.hhs.gov/hipaa/)

5.1.6 [Payment Card Industry Data Security Standards (PCI-DSS)](https://www.pcisecuritystandards.org/)

---

**ITS Policy 1.0**  
Acceptable Use of Data and Technology Resources

**Category:** Acceptable Use of Technology  
**Title:** Acceptable Use of Data and Technology Policy  
**Responsible Unit:** Information Technology Services  
**Effective:** August 13, 2016  
**Revision History:** March 27, 2017  
**Review Date:** March 2020
ITS Policy 1.0
Acceptable Use of Data and Technology Resources

Category: Acceptable Use of Technology
Title: Acceptable Use of Data and Technology Policy
Responsible Unit: Information Technology Services
Effective: August 13, 2016
Revision History: March 27, 2017
Review Date: March 2020

5.1.7 Faculty Handbook
5.1.8 Code of Student Rights and Responsibilities (Code of Conduct)
5.1.9 WVU Division of Administration, Finance and Human Resources Policies
5.1.10 WV Higher Education Policy Commission Rules and Policies