West Virginia Higher Education Policy Commission
West Virginia Community and Technical College System

Information Security and Acceptable Use Policy

1. Purpose

This policy establishes and explains the guidelines and responsibilities for individuals who use the technology resources owned or managed by the West Virginia Higher Education Policy Commission (Commission) and the West Virginia Community and Technical College System (Council). The intent of this policy is to explain the range of acceptable and unacceptable uses of Commission and Council provided information technology (IT) resources and is not necessarily all-inclusive of information security. IT resources may include anything with a processor, communications capability, or storage.

This policy is based on the State of West Virginia Office of Technology's Information Security Policy (WVOT-PO1001) and Email Use Standards Policy (WVOT-PO1005), the West Virginia Executive Branch Accountability Policy (WVEB-P101), industry standards, security best practices, and applicable state and federal laws and regulations. This policy is reviewed annually or as circumstances dictate and revised as applicable.

Related Policies and Procedures:

- Incident Response Plan
- Data Classification and Protection Policy
- Data Access and Management Policy

2. Scope

This policy applies to all employees (paid, unpaid, interns, full-time, part-time, technical, and non-technical), vendors, contractors, and all other individuals, collectively referred to as "users", who have access to or use of the IT systems, applications, and resources managed or owned by the Commission and Council. It is related to security and protection of computer systems, applications, IT resources, data and information, and networks owned or managed by the Commission and Council.

3. Principles

3.1 In order to ensure that security policies and procedures remain sound, it is important that everyone realize that security is a team effort. It is important to protect the security of all IT systems, applications, servers and the network that the Commission and Council owns or manages.

3.2 The Commission and Council realize that security is a global concern. It affects not only those assigned to administer and audit security, but also end users at every level. In order to ensure that security policies and procedures remain sound,

it is important that all users realize that security is a team effort and that everyone plays an important role.

3.3 It is vital that all users are made aware that potential threats to IT systems, networks, resources and users can come from both inside and outside of the organization. Proper training and awareness activities are an essential part of the overall IT security program.

4. Policy

4.1 All IT resources, including but not limited to hardware, software, data, and physical or virtual networks are owned by the Commission and Council and the State of West Virginia unless controlled by a contractual or vendor agreement.

4.2 All users should have no expectation of privacy while accessing or using Commission and Council provided IT systems, technology, applications, and resources.

4.3 All users of Commission and Council technology resources must adhere to agency rules, policies, procedures, as well as applicable state and federal laws and regulations.

4.4 IT systems and resources are designated for authorized purposes. The Commission and Council reserves the right to monitor and review usage as required for legal, audit, or legitimate authorized operational or management purposes.

4.4.1 Users are permitted to use these resources for limited personal use provided they have the permission of their supervisor, the personal use does not affect their job performance or responsibilities, and that such use does not conflict with this or any other policies.

4.4.2 Users must never redirect or save Commission and Council documents on personally owned equipment without prior authorization.

4.5 All users, must sign an IT Security Statement of Acknowledgement indicating that they have read, understand, and will abide by all Commission and Council policies and procedures regarding IT security and acceptable use. Users must review the policies annually for updates and may be denied the use of IT resources by refusing to sign.

4.6 All devices accessing Commission and Council owned or managed systems, applications, or networks, regardless of ownership, must be equipped with up-to-date virus protection software where applicable.

4.7 All users are responsible for securing their own computer. Users must lock computers and/or laptops when leaving them unattended or not in use. Users are responsible for any actions that can be identified to have originated from their assigned computer.

4.8 All users are required to comply to the ethical standards governing copyright, software licensing, and intellectual property.

4.9 No unauthorized software will be installed on Commission and Council systems unless expressly authorized. The Senior IT Systems Administrator will authorize all software installation as applicable.

4.10 All users will utilize, maintain, disclose, and dispose of all information resources, regardless of medium, according to law, regulation, and/or policy.

4.11 Users must not intentionally introduce a virus into a Commission and Council owned computer, use unauthorized peer-to-peer networking or peer-to-peer file sharing, or attempt to disable, defeat, or circumvent any security controls.

4.12 Users must not use any Commission and Council IT resources to promote harassment or illegal discrimination of any kind.

4.13 Users are prohibited from saving files to their local machines, unless they are saving working copies for temporary use. All users must use the secure network shares provided to them.

5. Data and Information Privacy and Security

The Executive Vice Chancellor of Administration for Commission and Council has appointed a Privacy Officer and named them as the designated authority to establish and maintain a system of data and information security and protection.

5.1 Data and information resources are designated for authorized purposes. The Commission and Council has a duty and a right to review questionable activity.

5.2 All users must familiarize themselves with the Data Classification and Protection policy. The Privacy Officer and the Division of Policy and Planning determine the classification of all data and information, and users must refer to that document when there is a question about classification.

The Data Classification and Protection policy has full details on how data is classified and how it should be protected. The policy classifies all data and information into 3 levels.

5.2.1 **Level 1 Restricted** – Data is classified as restricted when unauthorized disclosure could cause a significant level of risk, the data is protected by state, federal, and local privacy laws, and unauthorized access has the potential to cause harm. This includes sensitive, confidential, personally identifiable information (PII) such as SSN, banking and financial information, name, and address.

5.2.2 **Level 2 Sensitive** – Sensitive data is defined as data that if disclosed could result in a moderate level of risk. This includes data that is made available through open record requests or other formal or legal processes. Access is limited. Sensitive data may include most data elements in state personnel records or employment and training program data.

5.2.3 **Level 3 Public** – Public data is information that alone or in combination with other data can cannot be used by a reasonable person to identify an individual and if disclosed or shared, it would result in little or no risk to the individual or agency. This includes information such as enrollment in an institution, agency public websites, or Commission and Council policies and procedures.

5.3 Restricted and sensitive data or information is **never** to be stored on local machines, smart phones, tablets, laptops, USB or flash drives, external hard drives, digital media, or other portable devices without express prior authorization from the Privacy Officer or Division of Policy and Planning and proper encryption is used.

5.4 Restricted and sensitive data or information is **never** to be stored on cloud services without prior authorization from the Privacy Officer or Division of Policy and Planning and proper encryption is used.

5.4.1 Examples of cloud storage and services that **are not approved**, and must be approved beforehand include, but not limited to:

- Dropbox
- Microsoft One Drive (including One Drive for business)
- Google Drive
- Google Docs
- File Den

5.5 The use of personal storage, equipment, or personal storage for restricted or sensitive data or information is **strictly prohibited**. Any exception to this must have prior authorization from the Privacy Officer or Division of Policy and Planning, approved virus protection, and proper encryption.

5.6 If at any time equipment changes ownership or is ready for disposal, users must notify the Senior IT Systems Administrator to ensure that there is no restricted or sensitive data or information located on the equipment.

5.7 At no time shall any Commission and Council data or information be used or disclosed for a personal or non-work-related reason.

5.8 Users must guard against access to files and take precautions to protect the data and information they have access to.

5.8.1 Physical documents, files, folders, etc. that contain restricted or sensitive data or information must be kept in locked drawers or file cabinets when not in use.

5.8.2 Offices that have restricted or sensitive data or information should be kept secure and locked when not in use.

5.8.3 Users must log off or lock their computer every time they are away from it.

5.8.4 Restricted or sensitive data or information handled outside of secure areas must receive the same level of protection as if it were on-site.

5.9 Users working remotely or carrying laptops or tablets must use the Commission and Council supplied VPN when possible. Public WIFI and internet connections are not secure and should not be used when working on restricted or sensitive documents or when viewing restricted or sensitive data or information.

5.10 Prior to collecting, sharing or disclosing, or sending/receiving data, files, or information that contain restricted or sensitive data or information, users must consult with the Privacy Officer or the Division of Policy and Planning to ensure proper controls are in place and the sharing is in compliance with state and federal laws.

5.11 All contractors and vendors must sign a contract agreeing to abide by all Commission and Council security and data privacy policies and procedures when dealing with data or information of any kind.

5.12 All Commission and Council sponsored or run websites and applications must have annual privacy reviews conducted by the Privacy Officer and contain or point to approved privacy notices or policies.

5.13 All contracts, grant proposals, data sharing agreements, memorandum of understandings, or other agreements that include data sharing, exchange of information, or disclosure of any kind must be reviewed by the Privacy Officer prior to signature to ensure compliance.

5.14 Privacy impact assessments must be completed when a new project (grants, third-party services, cloud applications, memorandum of understandings, data sharing, etc.), webpage, or internally developed application is in the development stage or when changes are being made. Annual reviews will be completed as applicable.

5.15 The Privacy Officer or the Division of Policy and Planning shall have the right to monitor and audit the collection, use, disclosure and retention of the data collected and maintained by the Commission and Council to ensure compliance with this and other privacy related policies and procedures.

6. Privacy and Security Incidents

All users must immediately report any observation of an attempted or suspected security or privacy incident[1] or any violation of this policy. Users should review the full incident response plan for complete details.

A privacy or security incident is any event that involves the misuse or computing resources, is disruptive to normal system operations, or an attempted or successful effort to access, acquire, disclose, or use PII or other information without authorization.

6.1 Examples include but are not limited to the following:

[1] See Commission and Council Incident Response Plan for details on privacy incidents.

6.1.1 Lost, stolen, unsecured, or temporary misplaced equipment, tablets, laptops, physical records, or other portable devices such as smart phones.

6.1.2 Lost or stolen storage media, including flash drives, CDs/DVDs, external hard drives, SD cards, or other external storage that contains PII or other sensitive data.

6.1.3 Improper storage or disposal of records, whether electronic or physical.

6.1.4 Posting or exposure of student information on public facing websites, public formal or informal reports and publications, social media, or other public venue.

6.1.5 Intentional or accidental transmission of student information to unauthorized parties or to authorized parties but using unsecure methods such as emailing restricted or sensitive information.

6.1.6 Malware, computer viruses, or other malicious attacks that could compromise the security of a computer or network.

6.1.7 Violations of official security policies and procedures.

6.1.8 Compromised computers or servers, such as times where a machine or network has been hacked or accessed by an unauthorized party.

6.1.9 Sharing data without full authorization or through non-secure methods such as email, texting, or other non-secure methods.

6.1.10 Receipt of student information that an individual is not entitled to.

6.1.11 Use of student or employee information for purposes other than official institution or agency related business.

6.2 IT system security incidents should be reported to the Senior IT Systems Administrator and privacy incidents should be reported to the Privacy Officer. Incident reports should, to the extent possible, use established forms and shall include as much information as possible.

6.3 Users must immediately contact the Privacy Officer upon receiving or obtaining restricted information that they are not entitled to and notify the Senior IT Systems Administrator upon becoming aware of an inappropriate use of Commission and Council provided IT resources.

6.3.1 Users should consult an immediate supervisor if there is doubt concerning authorization to access any Commission and Council IT resource or regarding acceptable or unacceptable uses. If criminal activity is suspected or detected, reporting should occur without delay.

See the incident response plan for details on reporting.

7. Access Controls

Access to technology systems, resources, and networks owned or managed by the Commission and Council imposes certain responsibilities and obligations and is granted subject to internal security and privacy policies, and applicable state and federal laws and regulations.

Data and Information access are the responsibility of the Privacy Officer and the Division of Policy and Planning and is outlined in more detail in Section 5 of this document and in the Data Access and Management Policy.

7.1 User Management Process

7.1.1 System access is limited to authorized users, processes acting on behalf of authorized users, and devices

7.1.2 The Senior IT Systems Administrator and the Privacy Officer must be immediately notified of all new hires, terminations, transfers, or requests to modify user access. Access will be created, disabled, modified, or removed as applicable.

7.1.3 A listing of all those who are authorized to request user creation or modification is maintained and updated as required and accounts will only be created or modified if the request is from an authorized user.

7.1.4 User access is modified based on an "access replacement" strategy where the users' existing access is removed during the modification process.

7.1.5 Existing user access is reviewed every 6 months to ensure that proper security is in place, access is legitimate and consistent with current job responsibilities.

7.1.6 When users are transferred, terminated, or retire, User IDs and authorizations are locked immediately and removed where appropriate.

7.2 Passwords

7.2.1 All users are provided with a unique User ID and password. As a new user, the password must immediately be changed using appropriate Commission and Council password requirements. A secure password must meet the following minimum requirements:

- The minimum number of alphabetic characters that a password must contain is 8
- The minimum number of non-alphabetic characters that a password must contain (where non-alphabetic characters are any ASCII printable characters that are non-alphabetic and are not national language characters) is 1.
- The maximum number of times a character can be used in a password must not exceed 3.
- When converting to a new password, the minimum number of characters in the new password that was not in the old password is 3.

7.2.2 All passwords are confidential and must not be shared under any circumstances.

7.2.3 All users are required to change their password every 6 months.

7.2.4 The Commission and Council maintain appropriate controls to protect the confidentiality of passwords used for authentication.

7.2.5 All users are responsible for securing and protecting their username and User ID. Users will be held accountable for any and all actions identified to have originated from their accounts.

8. Training and Awareness

The Senior IT Systems Administrator and the Privacy Officer are responsible for ensuring that all users, and others who access computer systems, receive sufficient training in policies and procedures, security requirements, correct use of information resources, and other administrative controls.

8.1 All new employees are required to complete mandatory security and privacy training within the first week of employment.

8.2 All users are required to sign a confidentiality and non-disclosure agreement.

8.3 All users are required to complete mandatory information security awareness and data privacy and security training or refresher annually.

8.4 All users will receive additional training as policies, standards, or procedures are changed, to the extent that the changes affect their jobs.

8.5 Users are required to participate in all periodic online security and privacy training assigned to them within the time set forth in the initial training email they receive. Failure to comply could lead to loss of access or revoked privileges until required training is complete.

9. Email

9.1 All users are provided with an email address that will be used for all official communications. Use of personal e-mail to conduct Commission and Council business is strictly **prohibited**.

9.2 All user content sent and/or received by Commission and Council supplied email is to be considered owned by the state and may be considered official state records subject to legal discovery and monitoring.

9.2.1 Users should have no expectation of privacy when using email even for occasional personal use.

9.2.2 Email is permitted to be connected to personal cell phones or tablets for business purposes, however this does not in any way ensure privacy or confidentiality of Commission and Council email communications.

9.3 Restricted or sensitive information (including the users' own information) is **never** to be sent through email regardless if the recipient is internal or external.

Contact the Privacy Officer or the Division of Policy and Planning for a secure method of transferring this type of information.

9.3.1 All incoming and outgoing email will be scanned for potential violation of data privacy policies. The Privacy Officer will review any violations and handle appropriately.

9.3.2 Users must immediately contact the privacy officer upon receiving or obtaining confidential information to which the user is not entitled.

9.4 Email is not to be used for the creation or distribution of any offensive or disruptive messages.

9.5 Users must never execute programs or open e-mail attachments that: (1) have not been requested; or (2) come from an unknown source. If in doubt users should contact the Senior IT Systems Administrator for assistance.

9.6 All users must guard against targeted phishing schemes that request sensitive information through deceptive emails that may appear to be sent from an internal email address. To assist in the prevention of such attempts, external emails will contain a banner at the top stating they are from an external source. Users should contact the Senior IT Systems Administrator if they have questions or concerns.

9.7 Users must follow proper protocol and guidelines when sending mass mailings or group messages.

10. Acceptable Use/Unacceptable Use

Acceptable use encompasses behavior that is ethical, compliant, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and to freedom from intimidation and harassment.

10.1 User Responsibilities

10.1.1 Users will only access files, data, and protected records if they are authorized to have the information, if they own the information, or if the information is publicly available.

10.1.2 All users should conduct themselves as representatives of the Commission and Council and are responsible for becoming familiar with and abiding by all Commission and Council policies and procedures.

10.1.3 Users must only use legal versions of copyrighted software and ensure compliance with vendor license requirements.

10.2 Unacceptable uses include, but are not limited to the following:

10.2.1 Any use which is unlawful, violates local, state, or federal laws, unreasonably interferes with job performance or system operations, or that could be reasonably considered as disruptive to another’s work.

10.2.2 Furnishing false or misleading information or identification in order to access another user's account

10.2.3 Dispersing data to individuals without authorization or through unauthorized methods.

10.2.4 Any use of IT resources for unethical purposes, including sexually explicit material, violence, gambling, racism, harassment, or any illegal activity. sexually explicit material.

10.2.5 Use of unlicensed software or the distribution of Commission and Council software that would violate license agreements.

10.2.6 Any use for promotion of political or religious positions or causes, commercial purposes, product advertisements, or “for-profit” personal activity.

10.2.7 Any use in relation to copyright infringement, placing wagers or bets, promoting the misuse of weapons or the use of devices associated with terrorist activities.

10.2.8 Any use in relation to participating in chain letters, solicitations, abusive correspondences, or forwarding or responding to SPAM.

10.2.9 Any use related to pyramid selling schemes, multi-marketing schemes, or fundraising for any purpose unless agency sanctioned.

11. Exceptions

Exceptions to any part of this policy are rare and must be approved by the Executive Vice Chancellor of Administration for the Commission and Council or his/her designee, and formally documented. Policy exceptions will be reviewed on a periodic basis for appropriateness.

12. Enforcement

Enforcement of this policy is the responsibility of the Executive Vice Chancellor of Administration for the Commission and Council or his/her designee.

Any user found to have violated this policy may be subject to disciplinary or corrective actions based upon the policies, rules, and procedures of Commission and Council. These actions may include sanctions including, but not limited to, revocation of privileges up to and including termination of employment. Certain violations, misuse, or disclosures of confidential information may include civil and/or criminal penalties.

13. Change Log History

June 2019: Updated to align with data privacy and protection efforts; Added Change Log History;