WEST VIRGINIA UNIVERSITY AT PARKERSBURG

GRAMM-LEACH-BLILEY ACT

POLICIES AND PROCEDURES

Last Updated: April 1, 2023

Table of Contents

Table of Contents, Continued

Table of Contents, Continued

The following Additional Documentation/Evidence is available upon request and includes Network Diagrams Documentation, Data & System Inventory, and Server Inventory.

In accordance with the Delegation of Power to the President document approved during the June 9, 2021, regular meeting of the West Virginia University at Parkersburg Board of Governors, President Chris Gilmer hereby approved the following policies and procedures to act as interim guidance over compliance with the Gramm-Leach-Bliley Act. At a future date, no later than December 31, 2021, these policies and procedures shall be reviewed by all WVUP stakeholders and approved by the Board of Governors.

SECTION 1 - GRAMM-LEACH-BLILEY ACT

A - Introduction

Gramm-Leach-Bliley Act, (GLBA) effective May 23, 2003, addresses the safeguarding and confidentiality of customer information held in the possession of financial institutions such as banks and investment companies. GLBA contains no exemption for colleges or universities. As a result, educational entities that engage in financial activities, such as processing student loans, are required to comply. GLBA and other emerging legislation could result in standards of care for information security across all areas of data management practices both electronic and physical (employee, student, customer, alumni, donor, etc.). Therefore, West Virginia University at Parkersburg has adopted an Information Security Program for certain highly critical and private financial and related information. This Information Security Program applies to customer financial information the University receives in the course of business as required by GLBA as well as other confidential financial information included within its scope.

The purpose of this program is to:

- Ensure the security and confidentiality of customer information in compliance with applicable GLBA rules as published by the Federal Trade Commission.
- Safeguard against anticipated threats to the security or integrity of protected electronic data.
- Guard against unauthorized access to or use of protected data that could result in harm or inconvenience to any customer.

B - Coordination and Responsibility of Program

The President of WVUP has appointed the Executive Vice President of Finance & Operations to serve as the coordinator of the Information Security Program with the assistance of the Chief Information Officer of West Virginia University at Parkersburg. The coordinator is responsible for the development, implementation, and oversight of West Virginia University at Parkersburg's compliance with the policies and procedures required by the GLBA Safeguards Rule. Although ultimate responsibility for compliance lies with the Coordinator, representatives from each of the operational areas are responsible for implementation and maintenance of the specified requirements of the security program in their specific operation.

C- Information Security Governance Committee

The Information Security Governance Committee exists to ensure that this Information Security Program is kept current and to evaluate potential policy or procedural changes driven by GLBA. Committee membership may change from time-to-time but will minimally include the Chief Information Officer, Executive Vice President of Finance & Administration, and representatives from Financial Aid, Business Office, Records, and Faculty. Other individuals may be added as deemed necessary.

Questions regarding GLBA impacts on business processes and policies and questions regarding technical issues, risk assessments, and information technology security policy should be directed to the Coordinator of the Information Security Program.

D - Risk Assessment and Safeguards

There is an inherent risk in handling and storing any information that must be protected. Identifying areas of risk and maintaining appropriate safeguards can reduce risk. Safeguards are designed to reduce the risk inherent in handling protected information and include safeguards for information systems and the storage of paper.

E - Written Plan

The Safeguards Rule requires West Virginia University at Parkersburg and its affected units to develop a written information security plan that describes its program(s) to protect customer information. The plan must be appropriate to WVUP's size and complexity, the nature and scope of our activities and the sensitivity of the customer information it handles. As part of its plan, WVUP and its affected units must:

- designate one or more employees to coordinate its information security program (the Chief Information Officer)
- identify and assess the risks to customer information in each relevant area of the University's operation, and evaluate the effectiveness of the current safeguards for controlling the identified risks
- design and implement a safeguards program, and regularly monitor and test that program
- select third party vendors that can maintain appropriate safeguards, making sure that contracts with these vendors require them to maintain safeguards, and allow the University to oversee their handling of customer information
- regularly evaluate and adjust the program in light of relevant circumstances, including changes in the University's business or operations, or the results of security testing and monitoring.

F- Employee Training and Education

Employees handle and have access to protected information in order to perform their job duties. This includes permanent and temporary employees as well as student employees, whose job duties require them to access protected information or who work in a location where there is access to protected information. Departments are responsible for maintaining a high level of awareness and sensitivity to safeguarding protected information and should periodically remind employees of its importance. Seemingly minor changes to office layout and practices could significantly compromise protected information if a culture of awareness is not present.

The department representative is responsible for ensuring that staff are trained in the relevant GLBA concepts and requirements. Training materials relative to GLBA and data handling are available on the web. Upon approval by the Coordinator for GLBA, these training templates and other materials may be tailored by each department to reflect their individual training needs. Training may be delivered in a variety of ways that meet the department's objectives. Departments are responsible for maintaining records of staff that have received training and must be able to produce written copies upon request.

G - Oversight of Service Providers and Contracts

GLBA requires the University to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. Contracts should be reviewed to ensure the following language is included:

[Service Provider] agrees to implement and maintain a written comprehensive information security program containing administrative, technical and physical safeguards for the security and protection of customer information and further containing each of the elements set forth in § 314.4 of the Gramm Leach Bliley Standards for Safeguarding Customer Information (16 C.F.R. § 314). [Service Provider] further agrees to safeguard all customer information provided to it under this Agreement in accordance with its information security program and the Standards for Safeguarding Customer Information.

The GLBA contract due diligence is considered in various aspects of contract negotiation, including security control reviews.

H - Evaluation and Revision of the Information Security Program

GLBA mandates that this Information Security Program be subject to periodic review and adjustment. The most frequent of these reviews will occur within Information Technology Security and Policy where constantly changing technology and constantly evolving risks indicate the wisdom of regular reviews. Processes in other relevant offices of the University such as data access procedures and the training programs should undergo regular review.

This Information Security Program is reevaluated regularly in order to ensure ongoing compliance with existing and future laws and regulations.

I - Definitions

- Covered Component
    - any area of West Virginia University at Parkersburg, which is required to be compliant with either GLBA regulations.
- CUI (Controlled Unclassified Information)
    - information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.
- Customer Information
    - any record containing nonpublic personal information as defined in 16 C.F.R. § 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of [the financial institution] or [its] affiliates.
- Financial Product or Service
    - (i) any product or service that a financial holding company could offer by engaging in a financial activity; and
    - (ii) Financial Service includes your evaluation or brokerage of information that you collect in connection with a request or an application from a consumer for a financial product or service.
- Non-Public Personal Information
    - (i) Personally identifiable financial information and
    - (ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available. 16 C.F.R. § 313.3(n) (1).
- Personally Identifiable Financial Information
    - any information:
        - (i) A consumer provides to you to obtain a financial product or service from you;
        - (ii) About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or
        - (iii) You otherwise obtain about a consumer in connection with providing a financial product or service to the consumer.
- Protected Information
    - either personally identifiable financial information or protected health information, which is covered by either the GLBA.
- Examples of Activities the FTC is Likely to Consider as a Financial Product or Service include:

- Student (or other) loans, including receiving application information, and the making or servicing of such loans
- Financial or investment advisory services
- Credit counseling services
- Tax planning or tax preparation
- Collection of delinquent loans and accounts
- Sale of money orders, savings bonds or traveler’s checks
- Check cashing services
- Travel agency services provided in connection with financial services
- Real estate settlement services
- Money wiring services
- Issuing credit cards or long-term payment plans involving interest charges
- Personal property and real estate appraisals
- Career counseling services for those seeking employment in finance, accounting or auditing
- Services provided by a principal, broker or agent with respect to life, health, liability or disability insurance products
- Obtaining information from a consumer report
- Providing or issuing annuities

J – General Policies and Procedures

1.1 Account Compromises Policy and Procedures
1.2 Account Management Policy and Procedures
1.3 Server Security Standard
1.4 System Access Procedure
1.5 Anti-Virus and Anti-Spam Policy
1.6 BYOD Policy
1.7 Data Breach Response Policy and Procedures
1.8 Electronic Mail Policy
1.9 Internet Usage Policy
1.10 Multi-Factor Authentication Policy
1.11 Password Policy
1.12 Privileged Accounts Policy
1.13 Distribution List Policy

Section 1 General Policies & Procedures

1.1 - Account Compromise Policy & Procedures

Purpose

To clearly define the types and severities of account compromises that may occur in WVUP systems as well as the process for safeguarding these accounts and notifying users.

Information Sources

WVUP IT receives notifications from WV Net if email accounts from the @wvup.edu domain appear on lists of compromised accounts distributed by MS-ISAC (Multi-State Information Sharing & Analysis Center).

Types, Severity, and Procedure

- Direct
    - Evidence exists that a WVUP-maintained account has been compromised.
        - Access logs are maintained and notifications are sent to appropriate Information Technology staff when a suspicious activity is detected
    - Severity
        - High
    - Procedure
        - All WVUP-maintained accounts assigned to the user will be immediately disabled.
        - The user will be notified through alternative methods to resolve
            - Alternate emails listed in Banner
            - Phone number listed in Banner
        - The user will need to change their password from the default. Users shall not re-use passwords.
- Indirect
    - Evidence exists that an account associated with a WVUP-maintained account has been compromised.
        - WVUP receives notifications from REN-ISAC of any third-party accounts associated with WVUP email addresses found in compromised accounts lists
        - Severity
            - Low to medium

    - Procedure
        - Inform users of potential compromise through their WVUP-issued email
            - Request that user change passwords immediately
            - Include other pertinent security information
                - Best practices, etc.
        - If the password is not changed within x days, WVUP IT will reset the password and make the attempt to communicate with the student again through the alternative methods listed above.

1.2 - WVUP Account Management Policies

Purpose

This policy establishes how user accounts are created, modified, and deleted.

Scope

This policy applies to all faculty, staff, and students.

Policy

User Accounts

- West Virginia University at Parkersburg IT staff are responsible for creating, modifying, and deleting all accounts.
- All faculty and staff accounts must include an electronically submitted form by Human Resources.
- Student accounts are programmatically generated from Banner. Accounts are created multiple times throughout the day.
- WVUP IT will issue a unique account to each authorized individual that will be deactivated when necessary.
- When creating accounts, the principle of "least privilege access" will be used. Users will be granted access to network resources and data required to perform job duties.
- Unless otherwise authorized by WVUP IT, account sharing is prohibited. Users must use their individual IDs to access network resources and data.
- Each department and division will have an identified employee responsible for requesting access modifications.
- WVUP IT will periodically audit existing user accounts to ensure that access and account privileges are still appropriate based on job function, "need to know", and employment status.

Temporary Accounts

- Accounts for contractors and temporary employees will be created as needed following the principle of least privilege.
- Temporary accounts will be set with an expiration date of one year unless otherwise requested.
- All temporary accounts must be authorized by the appropriate supervisor or entity responsible for the temporary employee.

Shared Accounts

- While shared accounts are generally prohibited, some systems require a single administrative account. In these situations, responsible users must ensure that these passwords are only shared with the appropriate personnel and properly secured.
- If at any time a user with access to a shared account leaves, the password for that account must be changed immediately.

Application and System Standards

- Shared accounts are not permitted unless specifically required by the application or business purpose.
- Authentication should take place external to the application. External authentication services, preferably Active Directory, should be used.
- Passwords cannot and will not be stored in plain text.
- Role-based access controls should be used whenever feasible, to accommodate changes in staff or assigned duties.
- Where technically or administratively feasible, systems should allow for account lock-outs after a set number of failed attempts and log the failed attempts.

1.3 – Server Security Standard

Introduction

The WVUP IT department provides numerous software services and data storage to support fundamental infrastructure needs as well as organizational operations. These services are provided in fundamental infrastructure needs as well as organizational operations. These services are provided in a physical and virtual server environment which require regular assessment, maintenance, and hardening to ensure high quality while maintaining the confidentiality and integrity of the infrastructure and data.

Policy

Access Control

- Access to server infrastructure and stored data is limited on the principle of least privilege based on the requirements necessary to configure, assess maintain, and utilize equipment and data.
- User, administrator, and service accounts should be documented, if unique, and should meet the guidelines set forth by organizational account and password policies.
- Remote maintenance and configuration of server infrastructure should be performed using encrypted traffic technologies such as, but not limited to RDP, SSH, and VPN.
    - Remote management technologies should be configured to timeout after a period of inactivity.
- Servers which provide shared directories via SMB, SFTP, or by any other means, should be configured to permit access to documented parties only in a least privileged capacity based on data classification.
    - Regular assessment of permitted users should be performed by the server administrators and maintained accordingly.
- Server infrastructure should be housed in locations restricted by access control mechanisms (key card, combination lock, etc.).
    - Access should be documented and regularly assessed for changes.

Inventory Management

- Server infrastructure inventory should be maintained in accordance with organizational policy.
- To maintain organization sustainability, each server, virtual and physical, should be documented in a unique file located within a server's directory within a common directory.
    - Documentation should include but is not limited to, the general purpose of the server, data categorization, addressing and naming properties, hosted services and relevant configuration information, access controls, management procedures, and business continuity procedures.
    - Service-to-service and server=to=server interactions should be included in documentation to aid I operational awareness and incident management.
    - Additional resources such as software and configuration documentation, should be included in the server's folder.

Service Management

- A server should be configured to perform only the functions required by the hosted service.

    - Unrequired services, ports, configurations, and accounts should be disabled or removed.
- Where applicable, service accounts should be utilized in a least privileged capacity to provide inter-service interactions.
- Servers hosting publicly available resources should be located within a DMZ network to provide separation from internal resources and to mitigate incident spread.

Vulnerability Management

- Regular assessment of server infrastructure should be performed to maintain the integrity and confidentiality of the equipment, operating systems, software, and data.
    - Regular automated vulnerability scans should be performed to identify and document weaknesses from which mitigation plans can be developed and implemented.
- Software, operating system, and firmware patching should be regularly assessed and performed.

Business Continuity

- To ensure high quality availability, server infrastructure should be backed up in accordance with the organizational backup policy and procedures
    - Testing of backup procedures should be performed with regular frequency to ensure functionality.

Change Management

- Notable configuration changes, downtime, and maintenance should be communicated to IT staff and the campus community where appropriate
- Server documentation should be updated to reflect significant changes to the architecture and configurations
- Significant changes should be planned and approved prior to implementation
- New server deployments should be planned, approved, and documented prior to, and during deployment.

1.4 - System Access Request Procedure

General Overview

Resource access must be requested by the individual's supervisor, not by the individual. These requests must be submitted to the OIT Help Desk Form with detailed information, including what the individual will need access to, what type of access, the duration of the access and a general description of why access to the resource is needed for the individual. For security purposes, a supervisor cannot approve access to a resource they do not own. Authorization will need to be granted by the manager of the resource.

Distribution of Access

Access to resources is based on task responsibilities, as well as assigned department. This is to ensure the individual will have access to all the necessary resources they will need to perform their job. All employees are prohibited from sharing an account to access sensitive resources.

Types of Resources and Available Access Options:

Shared Drive:

The drive will be mapped to the individual's account on their primary campus device. An individual can be issued read-only, write or modify access. Access to a shared drive must be requested from the individual's supervisor. Requests can be submitted to https://helpdesk.wvup.edu/scp/helptopics.php?id=65. Upon approval, individuals will be added to the correct departmental group and the appropriate shared drives will be mapped on the individual's college-issued device.

Email Account:

An approved individual will be delegated to the specified email account, which can be accessed via the web client, inside their own account. Individuals will not sign in directly to a delegated email account. If a user is issued access to an email account, they will have full access. A delegated individual will not be able to make alterations to who is delegated to the specific account.

Banner Forms Access and Reporting:

An approved individual will access Banner using their WVUP Network Credentials. Form access can be query-only (read-only) or modify access. Upon approval by the designated data manager, individuals will be able to access the specified Banner Form / Report.

VPN Access:

VPN setup will be configured under the individual's account on their primary campus device. VPN access will allow a user to access WVUP resources remotely. Access to VPN will not grant the individual access to any resources that they were not already issued.

Course LMS:

System access is restricted to faculty, teaching assistants, staff, students and system administrators.

Internal Systems:

System access is granted based on job task and can be customized based on user. These systems include: Advising System, Alternative PIN System for Registration, Course Withdrawal System, Employee Requisition System, Purchase Requisition System, Security System Web Client and the WVUP Portal. Access must be approved by the designated data manager.

Alterations to Existing System Access Settings:

Request for access elevation:

Resource access elevation must be requested by the individual's supervisor, not by the individual. Access elevation pertains to Banner form access or share drive access where an individual's permissions will be changed from read-only to modify access.

Request for access removal:

Resource access removal must be requested by the individual's supervisor. The supervisor is responsible for notifying the individual of any access changes.

1.5 - Anti-Spam, Anti-Virus Policy

Introduction

The purpose of this document is to establish a policy that ensures the proper use of West Virginia University at Parkersburg's email system by taking preventative measures against the proliferation of spam and computer viruses.

Policy

SPAM

West Virginia University at Parkersburg has the authority and responsibility to manage, control, and delete junk mail to prevent the unnecessary or inappropriate use of bandwidth to ensure that illegal, unwanted and solicited advertisements are not received on the college owned network. This policy establishes appropriate procedures to prevent email from known spammers from entering the WVUP mail system.

Spam, or junk mail, is unsolicited commercial email sent in bulk via the internet. While sending spam costs the sender practically no money, Spam puts both a cost and a burden on recipients by consuming network bandwidth and disk space, as well as wasting the time of the recipient with unwanted messages.

In order to reduce the cost to the college, the email system shall use control measures, which may include but will not necessarily be limited to filters and subscription Anti-Spam systems.

WVUP shall take all reasonable measures to use methods which minimize the blocking of legitimate email, but reserves the right to put into effect measures to avoid the financial and personnel costs of Spam emails.

Anti-virus

The purpose of the anti-virus policy is to prevent the infection of college owned computers and systems by computer viruses and other malicious code. This policy is intended to prevent major and widespread damage to user applications, data, and hardware and to prevent the financial losses resulting from such damage. The WVUP email server (Google Apps) has virus protection software built in that:

- Inspects every incoming and outgoing message.
- Automatically deletes all email attachments that include, but are not limited to the following extensions: exe, pdf, vbs.
- If the infected message cannot be cleaned, then it will be deleted.

In addition, WVUP’s network infrastructure is protected by a SonicWALL network security device that provides firewall protection, as well as IDS/IPS, Content Filtering, and antivirus scanning services.

Responsibilities

WVUP email users shall follow these guidelines to avoid receiving unwanted email:

- Do not register with email directory services aside from official college or association sources.
- Never reply to a SPAM message that you receive. Delete it.
- Use an alternative email address to post to bulletin boards or forums.

WVUP computer users shall follow these guidelines to avoid viruses and other forms of malware:

- All computers connected to WVUP’s network or capable of accessing the network shall have WVUP supported anti-virus software installed, configured, activated, and updated with the latest virus definitions before or immediately upon connecting to the network.

- All IT-managed computers will have anti-virus software installed that is centrally managed and updated.
- If a computer is detected as infected, it will be disconnected from the college network until the issue is remediated to prevent propagation of the virus to other devices on the network.
- If a message is received that appears to be suspicious, please do not open any attachments.

1.6 - Bring Your Own Device (BYOD) Standard

Introduction

The purpose of this standard is to establish accepted practices, responsibilities, and procedures for the use of personally owned devices that West Virginia University at Parkersburg authorizes to connect to college computer and network systems. This standard defines the user requirement, and provides guidance for the securing mobile devices, such as smartphones and tablets.

Standard

The following controls must be applied to mobile devices that connect directly to the West Virginia University at Parkersburg network and/or access WVUP-owned data:

- Passcode or password security must be active on the device.
- Any credentials used to access various college data sources (WVUP Network ID, Banner password, etc.) must be changed immediately upon the event of a lost or stolen device that has been configured to access college services or data.
- Safeguards should be taken to remotely erase data stored on the device in the event of theft or loss if available.
- Devices that are jailbroken, “rooted,” or have been subjected to other methods of changing built-in protections are not permitted to access WVUP resources.
- Users must take appropriate precautions to prevent others from obtaining access to their mobile devices. Users will be responsible for all transactions made with their credentials, and must not share individually assigned passwords or other credentials.

Violations

Violation or non-compliance of this standard will be addressed in accordance with established college 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 one’s employment or duties.

1.7 - Data Breach Response Policy and Procedure

Overview

Data breaches are increasingly common occurrences whether caused through human error or malicious intent. WVUP operations rely on the proper use of Confidential Information and Personally Identifiable Information (PII) on a daily basis.   Managing risk and responding in an organized way to Incidents and Breaches is key to operations and required by West Virginia state law.

Purpose

WVUP must have a robust and systematic process for responding to reported data security Incidents and Breaches. This policy is designed to standardize WVUP-wide response to any reported Breach or Incident, and ensure that they are appropriately logged and managed in accordance with best practice guidelines. Standardized processes and procedures help to ensure WVUP can act responsibly, respond effectively, and protect its information assets to the extent possible.

Scope

This policy applies to all WVUP staff.

Policy

GENERAL INFORMATION

A "Data Security Incident" or "Incident' shall mean an accidental or deliberate event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication or information resources of WVUP.

Common examples of data security Incidents include, but are not limited to, any of the following:

- Successful attempts to gain unauthorized access to a WVUP system or Student or Educator PII regardless of where such information is located

- Unwanted disruption or denial of service

- The unauthorized use of a WVUP system for the processing or storage of Confidential Information or PII

- Changes to WVUP system hardware, firmware, or software characteristics without WVUP's knowledge, instruction, or consent

- Loss or theft of equipment where Confidential Information or PII is stored

- Unforeseen circumstances such as a fire or flood that could lead to the loss or misuse of Confidential Information or PII

- Human error involving the loss or mistaken transmission of Confidential Information or PII

- Hacking, social engineering, phishing or other subversive attacks where information is obtained by deceitful practice

A “Data Security Breach” or “Breach” is any Incident where WVUP cannot put in place controls or act to reasonably prevent the misuse of Confidential Information or PII. A Breach is also an Incident where data has been misused.

Adopting a standardized and consistent approach to Incident management shall ensure that:

- Incidents are reported in a timely manner and can be properly investigated

- Incidents are handled by appropriately authorized and skilled personnel

- Appropriate levels of management are involved in response management

- Incidents are recorded and documented

- Organizational impacts are understood and action is taken to prevent further damage

- Evidence is gathered, recorded, and maintained in a form that will withstand internal and external scrutiny

- External agencies, customers, and data users are informed as required

- Incidents are dealt with in a timely manner and normal operations are restored

- Incidents are reviewed to identify improvements in policies and procedures

Incidents can occur locally, in the cloud, or through third party service providers. Reporting and management of Incidents shall occur similarly. Third party providers shall also be governed by contract terms and liability as defined in their operational agreements.

Any contract breach that results in the misuse or unauthorized access to Student PII by a School Service Contract Provider must be handled according to the Board Policies Regarding SSCP Breaches and as required by C.R.S. 22-16-107(2)(a).

DATA CLASSIFICATIONS

Incidents vary in impact and risk depending on a number of mitigating factors including the content and quantity of the data involved. It is critically important that WVUP management respond quickly and identify the data classification of the Incident. This allows staff to respond accordingly in a timely and thorough manner.

All reported Incidents shall be classified as below in order to assess risk and approaches to mitigate the situation. Data classification shall refer to the following WVUP data categories:

Public Data - Information intended for public and community use or information that can be made public without any negative impact on WVUP or its customers. Student PII shall never be considered public data unless the data is Directory Information as defined by WVUP policy.

Confidential/Internal Data - Information of a more sensitive nature to the business and educational operations of WVUP. This data represents basic intellectual capital, applications, and general knowledge. Access shall be limited to only those people that need to know as part of their role within WVUP. Employee and Faculty PII (with the exception of Social Security Numbers (SSN), financial information, or other critical information) falls within this classification

Highly Confidential Data – Information that, if breached, causes significant damage to WVUP operations, reputation, and/or business continuity. Access to this information should be highly restricted. Student PII falls into this category of data. Employee or Faculty Financial Information, Social Security Numbers, and other critical information also falls into this classification.

Incident Reporting

The following process shall be followed when responding to a suspected incident:

- Confirmed or suspected incidents shall be reported promptly to the Chief Information Officer. A formal report shall be filed that includes full and accurate details of the incident including who is reporting the incident and what classification of data is involved.

- Once an incident is reported, the CIO shall conduct an assessment to establish the severity of the incident, next steps in response, and potential remedies or solutions. Based on this assessment, WVUP shall determine if this incident remains an incident or if it needs to be categorized as a breach.

- All incidents and breaches will be centrally logged and documented to ensure appropriate documentation, oversight and consistency in response, management, and reporting.

Classification

Data breaches or incidents shall be classified as follows:

Critical/Major Breach or Incident – Incidents or Breaches in this category deal with Confidential Information or PII and are on a large scale WVUP-wide. All incidents or Breaches involving Student PII will be classified as Critical or Major. They typically have the following attributes:

- Any incident that has been determined to be a Breach
- Significant Confidential Information or PII loss, potential for lack of business continuity, WVUP exposure, or irreversible consequences are imminent.
- Negative media coverage is likely and exposure is high.
- Legal or contractual remedies may be required
- Requires significant reporting beyond normal operating procedures
- Any breach of contract that involves the misuse or unauthorized access to Student PII by a School Service Contract Provider.

Moderately Critical/Serious Incident – Breaches or incidents in this category typically deal with Confidential Information and are on a medium scale. Incidents in this category typically have the following attributes:

- Risk to WVUP is moderate
- Third party service provider and subcontractors may be involved
- Data loss is possible but localized/compartmentalized, potential for limited business continuity losses, and minimized WVUP exposure.
- Significant user inconvenience is likely
- Service outages are likely while the breach is addressed
- Negative media coverage is possible but exposure is limited

- Disclosure of Faculty or Employee PII is contained and manageable

Low Critically Minor Incident – Incidents in this category typically deal with personal or internal data and are on a small or individualized scale. Incidents in this category have the following attributes

- Risk to WVUP is low
- User inconvenience is likely but not WVUP damaging
- Internal data released but data is not student, employee, or confidential in nature
- Loss of data is totally contained on encrypted hardware
- Incident can be addressed through normal support channels

Incident Response

Management response to any reported incident shall involve the following activities:

Assess, Contain, and Recover Data – All security incidents shall have immediate analysis of the incident and an incident report completed by the CIO or their designee. This analysis shall include a determination of whether this incident should be characterized as a Breach. This analysis shall be documented and shared with the WVUP Executive Team, the affected parties, and any other relevant stakeholders. At a minimum the CIO shall:

Step	Action	Notes
A	Containment & Recovery	Contain the breach, limit further organizational damage, seek to recover/restore data
1	Breach Determination	Determine if the Incident needs to be classified as a Breach
2	Ascertain the severity of the incident or breach and determine the level of data involved.	See Incident Classification
3	Investigate the Breach or Incident and forward a copy of the incident report to the WVUP EVP of Finance & Administration	Ensure investigator has appropriate resources including sufficient time and authority. If PII or confidential data has been breached, also contact the Executive Team. In the event the Breach is severe, general counsel shall be consulted
4	Identify the cause of the incident or breach and whether the situation has been contained. Ensure that any possibility of further data loss is removed or mitigated as far as	Compartmentalize and eliminate exposure. Establish what steps can or need to be taken to contain the threat from further data loss. Contact all relevant departments who may be able to assist in this process.

	possible. If this loss cannot be mitigated, any incident will be considered a breach	This may involve actions such as taking systems offline or restricting access to systems to a very small number of staff until more is known about the incident.
5	Determine depth and breadth of losses and limit exposure/damages	Can data be physically recovered if damaged through use of backups, restoration or other means?
6	Notify authorities as appropriate	For criminal activities where property was stolen or fraudulent activity occurred, contact the appropriate authorities and general counsel. Should the Breach involve student PII that involves a School Service Contract Provider, notify the WVUP Board of Governors
7	Ensure all actions and decisions are logged and recorded as part of incident documentation and reporting	Complete Incident Report and file with EVP of Finance.

Asses Risk and Incident Scope – All incidents or Breaches shall have a risk and scope analysis completed by the CIO or their designee. This analysis shall be documented and shared with the EVP of Finance & Administration, President, the affected parties, and any other relevant stakeholders. At a minimum the CIO shall:

B	Risk Assessment	Identify and assess ongoing risks that may be associated with the incident or breach
1	Determine the type and breadth of the incident or breach	Classify incident or Breach type, data compromised, and extent of the breach
2	Review Data Sensitivity	Determine the confidentiality, scope, and extent of the incident or breach
3	Understand the current status of the compromised data	If data has been stolen, could it be used for purposes that harm the individuals whose identity has been compromised, if identity theft is involved, this possess a different type and level of risk.
4	Document risk limiting processes or technology components that contain and manage the incident	Does encryption of data/device help to limit risk of exposure?

5	Determine what technologies or processes will mitigate the loss and restore services	Are there backups of the compromised data? Can they be restored to a ready state?
6	Identify and document the scope, number of users affected, and depth of incident	How many individuals PII were affected?
7	Define Individuals and Roles whose data was compromised	Identify all students, staff, customers or vendors involved in the incident or breach
8	If exploited, what will the compromised data tell a third party about the individual? Could it be misused?	Confidential information or PII could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a criminal build up a detailed picture associated with identity theft or fraud.
9	Determine actual or potential harm that could come to any individual	Identify risks to individual's physical safety, emotional wellbeing, personal or business reputation, financial implications, or identity concerns
10	Are there wider consequences to consider?	Is there risk to the State or loss of public confidence?
11	Are there others who might provide support or advise on risks/courses of action?	Contact local colleges, agencies, or companies impacted by the breached data and request assistance.

Notification and Incident Communication – Each security incident or breach determined to be "moderately critical or critical" shall have communication plans documented by the CIO, executive team, President or their designee to appropriately manage the incident and communicate progress on its resolution to effected stakeholders

Post Mortem Evaluation and Responses – Each incident or Breach determined to be "moderately critical or critical" shall have a post mortem analysis completed by the CIO and their designees to appropriately document, analyze, and make recommendations on ways to limit risk and exposure in the future.

Each of the four elements shall be conducted as appropriate for all qualifying incidents or Breaches. An activity log recording the timeline of the incident management shall also be completed. Reporting and documentation shall be filed and managed through the office of the CIO.

Audit Control and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy. Appropriate audit controls and management practice examples are as follows:

- Archival completed incident reports demonstrating compliance with reporting, communication and follow-through
- Executed communication for incident management
- Evidence of cross-departmental communication throughout the analysis, response, and post-mortem processes.

Enforcement

Staff members found to be in violation may be subject to disciplinary action, up to and including termination.

1.8 - Electronic Mail Policy

The following represent WVUP's electronic mail policy:

- West Virginia University at Parkersburg reserves the right, consistent with policy and applicable law, to access, review, and release all relevant electronic information that is transmitted over or stored on the college computer and network systems, whether or not the information is private in nature, and therefore cannot complete confidentiality or privacy of electronic mail is not guaranteed. Confidentiality cannot be guaranteed due to the nature of the medium, the need for authorized staff to maintain electronic mail systems, and the college's accountability as a public institution, as well as instances involving the health or safety of people or property; violations of college codes of conduct, regulations, policies, or law; other legal responsibilities or obligations to the college, or the locating of information required for college business.
- Terminating employees' accounts will be closed on the last day of employment. Terminating employees shall be advised that their email accounts may be accessed by departmental directors in order to continue to conduct college business after their departure. Departmental directors and deans must send a written request to the Office of Information Technology requesting this access. The Office of Information Technology will reset the password and restore access. By default, accounts re-activated for this purpose will stay active for thirty days, which gives the user with acquired access enough time to transfer relevant emails and to inform correspondents of an address change.
- Users should exercise extreme caution in using email to communicate confidential or sensitive matters, and should not assume that their electronic mail is private or confidential.

- Users may not access, use or disclose personal or confidential information without appropriate authorization, and must take necessary precautions to protect confidentiality of personal or confidential information in compliance with college policy and applicable law, regardless of whether the information is maintained on paper or whether it is found in electronic mail or other electronic records.
- Electronic mail users and operators must follow sound professional practices in providing for the security of electronic mail records, data, applications programs, and systems programs under their jurisdiction.
- Users are responsible for safeguarding their login credentials (username and password) for using them only as authorized. Each user is responsible for all electronic mail transactions made under the authorization of his or her user ID.

Misuse

- Using the West Virginia University at Parkersburg email system for illegal activities is strictly prohibited. Illegal use may include, but is not limited to:
    - obscenity
    - child pornography
    - threats
    - harassments
    - theft
    - attempting unauthorized access to data or attempting to breach any security measures of a communications system
    - attempting to intercept any electronic communication transmissions without proper authority
    - violation of copyright, trademark or defamation law
- The following electronic mail practices are prohibited:
    - entry, examination, use, transfer and/or tampering with the accounts and files of others, unless authorized pursuant to policy
    - altering electronic mail system software or hardware configurations
    - interfering with the work of others or with college or other computer facilities
- College-provided email services shall not be used for commercial activities, personal financial gain or advancement of a political agenda.
- Email users shall not give the impression that they are representing, giving opinions, or otherwise make statements on behalf of West Virginia University at Parkersburg or any unit of the college unless expressly authorized to do so.
- Email services shall not be used for purposes that could reasonably be expected to cause strain on any computer system, or interference with others' use of the email systems.

Such uses include, but are not limited to, the use of email services to:

- send or forward chain letters
- send SPAM (unsolicited email)
- send letter bombs
- knowingly send or transmit computer viruses

Violations

Suspected or known violations of policy or law should be reported to the appropriate supervisory level for the operational unit in which the violation occurs. Violations will be processed by the appropriate college authorities and/or law enforcement agencies. Violations may result in various actions, including but not limited to revocation of electronic mail privileges; academic dishonesty or Code of Conduct proceedings; faculty, staff, or student disciplinary action up to and including dismissal; referral to law enforcement agencies, or other legal action.

1.9 - Internet Usage Policy

The purpose of this policy is to establish the acceptable usage of West Virginia University at Parkersburg internet resources, which are provided by WVUP to faculty, staff, students, and third parties for the purpose of the advancement of WVUP's mission statement.

This policy applies to all faculty, staff, students, and third parties who utilize any WVUP-provided internet connection.

Policy

Users of WVUP internet resources must adhere to all applicable WVUP policies, standards, contracts and licenses, as well as applicable federal, state, and local laws and regulations.

WVUP internet resources shall only be used by authorized individuals for the purpose for which the access was granted.

Incidental personal usage of internet resources is permitted; however, users of WVUP-provided internet resources are advised that they should have no expectation of privacy or confidentiality in connection with the personal usage of these resources. Personal use is permitted if and only if the user does not:

- Consume more than a trivial amount of network resources that would otherwise be used for academic and administrative purposes.
- interfere with employee and student productivity
- preempt any academic and administrative activity
- promote or result in a hostile work or academic environment

West Virginia University at Parkersburg Office of Information Technology reserves the right to monitor internet activity for operational needs and to ensure compliance with applicable laws and WVUP policies and procedures.

Rights and Responsibilities

All users of WVUP internet resources are expected to use good judgement and common sense. This includes, but is not limited to:

- Using WVUP internet resources in a lawful and appropriate manner
- Respecting the rights and privacy of others
- Using the college's trademarks and logos only as authorized and not representing personal comments as being those of the college.

Unacceptable Internet Usage

The following constitutes unacceptable usage of WVUP internet resources:

- Bypassing or circumventing security and content filters by using a proxy service or other means such as VPN.
- Using college technology or network resources for one's own commercial gain, or for other commercial purposes not expressly approved by the University.
- Using college technology or network resources to operate or support a personal or other non-University-related business.

Violations

Violation or non-compliance of this standard will be addressed in accordance with established college 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 one's employment or studies.

1.10 - Multi-Factor Authentication Requirement Policy

Purpose

West Virginia University at Parkersburg interacts with various forms of sensitive data. In order to better protect this information, users with access to this data are required to use additional security measures.

Definitions

- Personally Identifiable Information (PII) - information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Examples include Social Security Numbers and Driver’s License ID numbers.
- Data store - repository for persistently storing and managing collections of data which include not just repositories like databases, but also simpler store types such as simple files, emails etc.
- Multi-factor Authentication - electronic authentication method in which a device user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something only the user knows), possession (something only the user has), and inherence (something only the user is).
- Information system - a computer system or set of components for collecting, creating, storing, processing, and distributing information, typically including hardware and software, system users, and the data itself.

Policy

- All user accounts (staff, faculty, or student employee) with access to data stores housing Personally Identifiable Information are required to be set up with multi-factor authentication.
- Information Technology determines whether or not this is required, depending on what data stores and information systems the user has access to.
- All mobile devices used as authenticators must have screen locking and passcode/biometric security set up
- In the event of a lost or stolen authenticator device, IT must be notified immediately so that the device can be de-registered.
- Information Technology reserves the right to prohibit authenticator devices that do not meet security requirements.

1.11 - Password Policy

Information security is a vital component of the Office of Information Technology at West Virginia University at Parkersburg. As such, it is very important that all users follow established password policies and best practices.

Overview

These guidelines will reduce the risk of a data breach at West Virginia University at Parkersburg.

Password Complexity

- All users’ passwords must be at least ten characters

Password History

- Passwords may not be re-used. A history of the last ten passwords will be kept and the password management system will prevent the re-use of passwords recently used.

Password Security

- All users are expected to not share account credentials with anyone.
- All users are expected to secure account credentials.

Password Expirations

- For employees using Multi-Factor Authentication, password changes are required once every 365 days.
- Password changes are required for all other users once every 180 days.
- Users will be notified via email a week before their password is set to expire. Included in the email will be a link to the password management system that will allow users to change their password.
- Users will continue to receive reminder emails, either until the password has been changed or the deadline is reached.
- In the event that the password is not changed, and the deadline has been reached, the account will be disabled until the user changes the password.

Exceptions

Exceptions to this policy may be made at the discretion of the Chief Information Officer. A formal email must be sent to the Chief Information Officer with the affected user’s full name and justification for the exception.

1.12 - Privileged Account Standard

Introduction

Privileged accounts are used to access and maintain various computer systems on the West Virginia University at Parkersburg network. A privileged account is an account that has elevated administrative rights. A user with a privileged account has the ability to access confidential information, change data, and destroy data. Privileged accounts can pose a security risk to the college if proper controls and procedures are not in place.

Policy

Access Control Measures

- Access to critical systems, networks, files, data and processes is limited based on the principle of least privilege and need to know according to job responsibilities. Access will be granted to the least amount of data and privileges needed to perform a job.
- Access rights will be confirmed for a user to ensure that he or she only has the access necessary to perform job responsibilities.
- A procedure is established for employees to request privileged account access.
  - This request must be approved by a higher-level administrator.
- A unique login will be created for each person that has been granted privileged access. It is imperative that privileged account access information is never shared.
- Privileged accounts must have strong passwords (at least twelve characters with numbers and symbols) and must be changed every six months.
- Compliance requirements of federal regulations (FERPA, SOX, GLBA, etc.) and industry standards (PCI, DSS, etc.) pertaining to privileged accounts will be followed.
- OIT will investigate and report incidents that violate protective measures or cause unacceptable risk to privileged accounts.
- OIT will track and document the issuance and usage of privileged accounts.

Violations

Violation or non-compliance of this standard may lead to disciplinary action up to and including termination.

1.13 - Distribution List Policy

Introduction

Email distribution lists are designed to provide an easy way to communicate important college information to large groups of users. Distribution lists can be used for the one-way distribution of information, for email-based discussion, etc. Lists are created and “owned” by a WVUP user who manages the list’s behavior.

Policy

- Any faculty or staff member is eligible to be a list owner, but the creation of the list must first be approved by the Director of Marketing and Communications. Student Organizations are also eligible, but one individual must be designated the owner of the group and must first be approved by the Vice President of Student Services.

- The purpose of any list created must pertain to West Virginia University at Parkersburg business.
- Lists are not opened to off-campus subscribers unless special permission is obtained.
- It is the list owner’s responsibility to manage the list’s providers, with the exception of OIT-supported distribution lists.
- Under no circumstances can a list be used to participate in or promote activities that are illegal or violate the West Virginia University at Parkersburg code of conduct or policies.

OIT-Supported Distribution Lists

- Certain institution-wide distribution lists are owned and maintained by the Office of Information Technology. These distribution lists include:
  - All Students
  - All Full-time Faculty
  - All Adjunct Faculty
  - All Staff
- Distribution lists are also maintained by OIT for each academic division and administrative department.
- Errors in distribution group membership or configuration for these groups should be reported to the Office of Information Technology.
- Additions, deletions, and modification notifications are sent to OIT by Human Resources for these groups.
- To mitigate the risk of inappropriate usage of these distribution lists, security measures have been taken to limit sending access to these groups.
  - Permanent access to these groups must be approved by the Director of Marketing and Communications.
  - If a message is needed to be sent to one of these groups, and the sender does not have access to these groups, a request can be made to the Director of Marketing and Communications to be sent as an “E-FYI.” Transmission of the message is dependent on approval.

SECTION 2 - WVUP Information Security Plan

Core Concepts

- All data stored on any information system used by West Virginia University at Parkersburg, both internal as well as external, will be classified by the sensitivity of the data and will be stored, transmitted, and destroyed according to industry standards and best practices
- Access to systems storing sensitive information will be secured.
    - Electronically
        - Accounts with privileged access must use Multi-Factor Authentication.
        - File servers and information systems will be configured using the principle of least privilege (POLP), meaning that users will be granted access strictly based on the needs to perform their job functions.
    - Physically - all paper records containing PII will be secured by lock and key. Offices that work with PII will be secured by lock and key or other access means.
    - Appropriate measures will be taken to secure computer workstations used by employees, including, but not limited to
        - Screen lock after inactivity
        - Password history and length requirements
        - Account lockout policies
        - Encrypted file systems for local storage
- Information systems will be monitored
    - Any suspicious activity will be investigated by the Office of Information Technology and will be remediated as needed.
    - Access will be reviewed periodically to ensure that information systems security meets organizational needs will maintaining POLP
- Information systems will be updated regularly
    - Patches and updates must be installed on a regular basis to ensure that critical security issues are corrected in a timely manner
    - Administrative credentials for these systems will be updated on a regular basis
- Information systems will be tested
    - WVUP OIT will perform periodic penetration testing of all information systems using industry standard tools and third-party vendors, as needed.
    - Change requests for WVUP-maintained systems will be analyzed for impacts on security, infrastructure, and integrated systems before being implemented.
    - All internally developed systems will go through the appropriate level of testing, dependent on the type of data stored and access required, before being deployed in a production environment.

- Vendors will be expected to follow the same guidelines
  - Specific verbiage must exist in vendor agreements that ensures sensitive data is treated with the same level of security as it would at West Virginia University at Parkersburg.
- Employees Will Be Knowledgeable
  - All employees interacting with PII will undergo regular training in regards to data security best practices, as well as general information regarding security awareness.
  - Information Technology staff will stay up to date with technology and security trends to identify and adopt new standards as well as identify new threats to West Virginia University at Parkersburg's information systems.

2.1 - Disaster Recovery and Business Continuity Plan

Introduction

This policy provides a framework for the management, development, implementation, and maintenance of the disaster recovery framework for the data/technology services managed by West Virginia University at Parkersburg Office of Information Technology (OIT).

The primary objectives of the disaster recovery framework are to:

- Establish operational control over the disaster
- Communicate with relevant parties about the disaster
- Activate a specific recovery plan

Purpose

While West Virginia University at Parkersburg (WVUP) has taken measures to prevent disasters, emerging risks continue to threaten university data/technology capabilities. This framework has been created to address a non-routine event that could significantly impair WVUP's data/technology capabilities.

Scope

WVUP data/technology services are used by members of the University community, including faculty, staff, students, and affiliates. A disaster could impair the ability to access WVUP data/technology resources.

Definitions

Disaster - disaster for the purpose of this document is a non-routine event that significantly impairs WVUP's data/technology capabilities

Disaster Recovery (DR) - Disaster Recovery is WVUP OIT’s response to minimize the disruption of operations and expedite the recovery of data/technology.

Business Continuity - Business Continuity addresses the strategy to continue business operations at WVUP without the use of technology/data. DR is part of the Business Continuity Plan.

University Community - Faculty, staff, students, affiliates, authorized visitors, guests, and others whom University technology resources or access to the network have been granted.

WVUP Technology Systems - Including, but not limited to: computers, computer accounts, internet access, printers, networks and network devices, software, email, web sites, video systems, telephones, voicemail systems, and mobile devices that are provided for the use of University community in support of the programs of the University.

OIT - Office of Information Technology

Contacts

Policy Management	Office of Information Technology	304-424-8280
Disaster Coordination	VP of Facilities & Internal Affairs	304-424-8200

Responsibilities

Chief Information Officer or Designee	Has the ability to declare a disaster involving WVUP technology systems. Responsible for ensuring the policy remains current and for managing the application of the policy
WVUP Executive Staff and OIT Managers	Has the ability to declare a disaster involving WVUP technology systems
WVUP Emergency Response Team	The response team assembled by OIT with the talents and skills necessary to facilitate the University’s response to a particular crisis.
Systems Owners of non-OIT managed Systems	Individuals and departments that own non-OIT managed systems are responsible for the backup/recovery of those systems
WVUP Marketing and Communications	WVUP Marketing and Communications is the lead to disseminate communications regarding a disaster.

Assumptions

The disaster response and recovery plan are based on the following assumptions:

The safety of students, faculty, and staff is the primary concern of the University.

- Once a disaster has been declared, appropriate priority and support will be given during the recovery effort.
- A disaster may range significantly in regards to scope and impact. This plan is put into place to address any disaster, from a significant outage to a major loss. Not every section of this plan will apply to every disaster, but it should serve as a framework of possible options given the impairment to University data/technology.
- OIT provides centralized backups for the user profiles of faculty and staff, as well as University systems. System administrators need to ensure systems are backed up if they are not part of the OIT centralized backup process.
- During the recovery period, several departments and offices on campus may need to modify their current operations and plan for the unavailability of data/technology capabilities. The business continuity plan to accommodate such disruptions is not part of the OIT disaster recovery plan. Additionally, OIT's primary focus will be on the recovery effort for University-wide data/technology. Departments and offices should have plans in place to modify their operations during a disaster.
- While recovering data/technology, the University still has obligations to be compliant with data protection requirements during the recovery process.
- There are several systems on campus that are not supported by OIT. OIT will assist to the extent possible, but it is the responsibility of the systems owners to recover their data/technology on non-ITS managed systems.

2.2 - Declaring a Disaster

Executive Staff and/or available senior OIT leadership team members will consult and determine whether a disaster should be declared based on an initial assessment of a prolonged unplanned disruption of normal operations. Additionally, the Executive Vice President of Finance & Administration and the Executive Director of Business Services may need to be contacted when a disaster is declared, so as to put our insurance carriers on notice of the event. The policies may provide immediate assistance or possible future reparations for losses incurred. Once a disaster is declared, OIT senior management will update the appropriate senior management personnel. OIT senior management will establish a schedule of communication to provide updates regarding the recovery.

2.3 - Emergency Response

OIT Recovery Team

OIT senior management will assemble key members of the OIT leadership team and other staff members who will provide the technical and management skills necessary to achieve a smooth technology and business recovery. During the disaster, staff members' duties may be reassigned to the recovery team efforts based on their skillsets. Depending on the timing and duration of the disaster, normal schedules may be adjusted to focus on the recovery effort.

Outward Communications in an Emergency

In the event of an outage of the WVUP websites (including emergency situations), it may be necessary to communicate with a broad range of constituencies (faculty, staff, students, alumni, parents, community members, and the media). WVUP Marketing and Communications will take the lead on communications.

The following methods, depending on availability, will be used to provide ongoing updates regarding the recovery:

- Email messages to the faculty, staff, and student links
- WVUP OIT Website (http://it.wvup.edu)

Disaster Recovery Priorities

The overarching goal of the disaster recovery framework is to minimize the disruption of operations and recover data/technology. While a disaster may vary in size and scope, OIT will focus on the core areas:

- Authentication and network delivery services
- Cloud systems
- Data networks and telecommunication
- Website and services
- On-premises enterprise applications

Once the core areas are functional, OIT will address priorities established by the OIT Emergency Response Team and/or Executive Staff in the recovery effort.

Note: Response to and recovery from a disaster at West Virginia University at Parkersburg will be coordinated by the University’s Emergency Management Team within the office of the Vice President of Facilities and Internal Affairs. Their response and actions are governed by the West Virginia University at Parkersburg Emergency Operations Plan. This policy serves as a supplement to the University’s plan.

Recovery Evaluation

It’s important to remember that some of the best lessons are learned during difficult times. While our efforts attempt to identify and mitigate emerging risks, the potential for an unforeseen event remains. Therefore, after the completion of significant recovery of operations at the University, lessons learned meetings will take place within OIT and Executive Staff to determine what part of the plan was successful and which parts need to be improved going forward.

SECTION 3 – GLBA GENERAL CONTROLS

3.1 - ACCESS CONTROL

Access, Security and Control of Data and Information Policy

Introduction

This policy establishes a standard for the protection of the college computer information systems, data, and software. This policy establishes rights and responsibilities for the protection of staff and faculty who use these systems.

Policy

Data contained in the college systems are the property of West Virginia University at Parkersburg and represent official college records. Users who accept access to this data also accept responsibility for adhering to certain principles in the use and protection of that data.

- Information systems within the college shall be used only for and contain only data necessary for fulfillment of the college's mission.
- College data shall only be used for the legitimate business of the college.
- Due care shall be exercised to protect college data and information systems from unauthorized use, disclosure, alteration or destruction.
- College data, regardless of who collects or maintains it, shall be shared among those faculty or staff whose responsibilities require knowledge and access of such data.
- Applicable state and federal laws, as well as college policies and procedures concerning storage, retention, use, release, transportation, and destruction of data and/or all information systems contents and components shall be observed.
- Appropriate college procedures shall be followed in reporting any breach of security or compromise of safeguards.
- College information systems shall be implemented in such a way that:
    - Accuracy and completeness of all system contents are maintained during storage and processing.
    - Data, text and software stored and processed can be traced forward and backward for audit capability.
    - Information systems capabilities can be re-established within an acceptable amount of time upon loss or damage by accident, malfunction, breach of security or act of God.
    - Actual or attempted security breaches can be detected promptly.

- Any employee engaging in unauthorized use, disclosure, alteration, or destruction of information systems or data in violation of this policy shall be subject to the appropriate disciplinary action, including possible dismissal.
- Users may not utilize information systems to access data that they have not been given explicit access to. This data can include, but is not limited to:
  - transcripts, grade reports, enrollment reports
  - financial aid information
  - personnel, leave, salary reports
  - reports for government or funding agencies
  - fund-raising activities
  - mailing lists and labels
  - private or public release of data to outside parties such as students, parents and news media.

Responsibilities

The proper safeguarding of college information systems and the data contained wherein shall be the responsibility of all faculty and staff that have access and knowledge of the system or data. Specific responsibilities are as follows:

- Data Management - for each source of data, a designated manager is responsible for permitting any requested access to ensure appropriate permissions are granted.
- Management - all levels of management are responsible for ensuring that system users within their area of accountability are aware of their responsibilities as defined within the policy. Specifically, managers are required to validate the access requirements of their staff according to job functions, prior to submitting requests for the provisions of access, and for ensuring a secure office environment with regard to college information systems.
- Users - users are responsible for the protection, privacy, and control of all data, regardless of the storage medium. Users must ensure that data, including media, are maintained and disposed of in a secure manner. Users are responsible for understanding the meaning and purpose of the data to which they have access, and may use this data only to support the normal functions of the user’s duties. Users are responsible for all transactions occurring under their account credentials. Account credentials shall not be shared with anyone else under any circumstances unless the Chief Information Officer specifically approves an exception.
- Chief Information Officer - Responsible for ensuring that appropriate security controls are being provided, including protection of all areas from risk of exposure.
- Office of Information Technology staff - responsible for providing administrative, technical and educational support in the area of information security for all users of administrative systems. This support includes, but is not limited to:

- ○ creation and deletion of user accounts, after appropriate approval has been obtained.
- ○ providing access to administrative systems, transaction, or production after appropriate approval.
- ○ Recommendations to the Chief Information Officer on appropriate training to ensure consistent practice among departmental support personnel.

Violations

The Chief Information Officer is the policy administrator for information technology resources and will ensure that this process is followed. Additionally, deans, directors, and department heads are responsible for compliance with college policy within their respective administrative areas.

3.2 - Employee Onboarding

Account Creation

A. WVUP Network ID:
An individual's WVUP Network ID will be the third-party ID found in Banner. New employee information is entered into the system by Human Resources and/or Division Secretaries.

B. Email Alias:
Faculty and staff will be issued an email alias of "FirstName.LastName@wvup.edu". In the case of an individual who has a common name, ex. John Smith, a middle initial will be added to form that alias of "FirstName.LastName@wvup.edu".

C. Account Backup to Synology:
Employee accounts will be added to our backup system. This system will store historical data from WVUP Email, Google Drive, Google Calendar and Google Contacts.

Account Membership

A. Banner Access:
Access to Banner forms must be requested from the individual's supervisor. Requests can be submitted to https://helpdesk.wvup.edu/.

B. Departmental Shared Drives:
Access to shared drive must be requested from the individual's supervisor. Requests can be submitted to https://helpdesk.wvup.edu/. Upon approval,

individuals will be added to the correct departmental group and the appropriate shared drives will be mapped on the individual's college-issued device.

C. Distribution Groups in Active Directory:
All employees will belong to at least one distribution group. Individuals will need to be placed in their corresponding email distribution group based on the department they are working in. Updates must be made in Active Directory and not directly in Google Admin.

D. Folder Redirection:
All employees need to be assigned as a member of the folder redirection OU. This process will provide a backup of the employee's desktop files and My Documents folder. If the person has internet favorites in Internet Explorer, these will also be backed up.

E. VPN Access:
Employees with college-issued mobile devices may need to have access to campus resources offsite. VPN access requires approval from a supervisor and notation on what resources they will need access to. VPN access can be granted on a temporary or continuous basis, depending on the nature of the request.

Issued Technology

A. General Overview:
All employees will have access to campus computers. Depending on the individual's role, they may be issued campus technology. This technology includes, but is not limited to, a primary computer (either desktop or laptop), a monitor, keyboard and mouse. An individual is responsible for the equipment assigned to them. In the event campus technology is damaged, beyond normal wear and tear, the employee's department will be responsible for the replacement of the technology.

B. Computer Setup:
For new employees, the room the individual will be residing in will be evaluated to determine what, if any, additional resources would be needed.

1. Full Setup: The room has been recently refurbished and there is no equipment or cabling present. The machine for the room will be imaged with the latest operating system and installed with the specified software for the department. Full setups are typically for new positions.

2. Partial Setup: The room was recently occupied and the primary computer will need to be imaged, with the latest operating system and the specified software for the department, for the new employee.

C. Telephone Setup:
An employee’s role will determine if they are issued a unique extension. The voicemail system will need to be updated with the new individuals first and last name. This will impact the name displayed on the caller ID and the name address on the voicemail system itself.

For individuals to access Audix, the PIN on the account will need to be temporarily reset. This PIN must be at least five characters long.

D. Telephone Extension Types:

All full-time faculty and staff lines will have the ability to call long distance. Individuals who have a 4XX, 65X, 66X and 67X extension will be able to call out, but they cannot be reached directly by outside callers. An example is that an outside caller can reach the IT Help Desk at 304-424-8215, but if someone called an individual at 304-424-8402, this would not reach the WVUP employee.

If an individual would need to be reached directly by an outside caller, their supervisor would need to contact IT to work on getting them issued a different extension.

3.3 - Employee Offboarding (Termination)

No account termination shall take place without approval from Human Resources. A supervisor may request the removal of resource access only.

I. Account Transition:

A. Emeritus Status:
This status must be approved through their supervisor and the president’s office. If an account is issued emeritus status, their email address will remain active, but they will no longer have access to shared resources that were associated with their previous position

B. Regular Account:
For standard accounts that have not been issued emeritus status, the account password will be reset and the account will be disabled.

C. Email Forwarding:
Employee email accounts, upon request of their supervisor, can be forwarded to another email account within the department.

II. Account Membership

A. Banner Access:
Access, if issued, will be removed based on the end of employment date from Human Resources. Emeritus accounts will not have access to Shared Drives.

B. Departmental Shared Drives:
Access, if issued, will be removed based on the end of employment date from Human Resources. Emeritus accounts will not have access to Shared Drives.

C. Distribution Groups in Active Directory:
Access, if issued, will be removed based on the end of employment date from Human Resources. Emeritus accounts will be included in campus-wide email notifications, but they will not have administrative access to the lists.

D. VPN Access:
Access, if issued, will be removed based on the end of employment date from Human Resources. Emeritus accounts will not have access to VPN.

III. Issued Technology:

A. General Overview:
All assigned technology, including keyboards, mice and portable devices, but be returned by the last date of employment.

B. Equipment Sign Off:
Prior to their last day, the individual will need to schedule a meeting with someone for IT to take final inventory of the returned equipment and to document, if any, damages or missing equipment. Only a member for the IT department can sign off on this process.

IV. Third-Party Software Licensing:

. General Overview:
Any software that has been renewed or managed by the employee needs to be documented and list what credentials, if any, were used to register the software.

Equipment Sign Off:
For new employees, the room the individual will be residing in will be evaluated to determine what, if any, additional resources would be needed.

3.4 – AWARENESS TRAINING

Employee Training Standard

I. **Overview:**

West Virginia University at Parkersburg ensures that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

II. **Security Awareness Training:**

- West Virginia University at Parkersburg periodically conducts workshops that are open to faculty and staff focusing on a variety of topics related to security and data protection.
- Documentation provided during these sessions are made available to everyone at the end of the session and Zoom session recordings are posted to the college's online video management system.
- In the event an individual requires access to a system, the individual must complete paperwork which outlines why the access is needed, duration of access, type of access.

III. **Personnel Security (HR SECTION)**

- West Virginia University at Parkersburg screens individuals prior to authorizing access to organizational systems containing CUI.
- West Virginia University at Parkersburg ensures that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

3.5 - Personnel Security and Security Awareness Training

Policy

Security Awareness Training

- West Virginia University at Parkersburg ensures that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
- West Virginia University at Parkersburg ensures that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
- West Virginia University at Parkersburg provides security awareness training on recognizing and reporting potential indicators of insider threat.

Personnel Security

- West Virginia University at Parkersburg screens individuals prior to authorizing access to organizational systems containing CUI.
- West Virginia University at Parkersburg ensures that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

Relevant NIST SP800-171 Sections

3.2.1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
3.2.2	Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.
3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.
3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

3.6 - Audit & Accountability Policy

Policy

- West Virginia University at Parkersburg creates and retains system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.
- West Virginia University at Parkersburg ensures that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.
- West Virginia University at Parkersburg reviews and updates audited events.
- West Virginia University at Parkersburg alerts in the event of an audit process failure.
- West Virginia University at Parkersburg correlates audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.
- West Virginia University at Parkersburg provides audit reduction and report generation to support on-demand analysis and reporting.
- West Virginia University at Parkersburg provides a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.
- West Virginia University at Parkersburg protects audit information and audit tools from unauthorized access, modification, and deletion.
- West Virginia University at Parkersburg limits management of audit functionality to a subset of privileged users.
- West Virginia University at Parkersburg identifies system users, processes acting on behalf of users, and devices.

Relevant NIST SP800-171 Sections

3.3.1	Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.
3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.
3.3.3	Review and update audited events.
3.3.4	Alert in the event of an audit process failure.

3.3.5	Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.
3.3.6	Provide audit reduction and report generation to support on-demand analysis and reporting.
3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.
3.3.8	Protect audit information and audit tools from unauthorized access, modification, and deletion.
3.3.9	Limit management of audit functionality to a subset of privileged users.
3.5.1	Identify system users, processes acting on behalf of users, and devices.

3.7 - Change/Configuration Management

Policy

- West Virginia University at Parkersburg has established and will maintain baseline configuration and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
  - Baseline Configuration and Inventory Procedure
- West Virginia University at Parkersburg has established and will enforce security configuration settings for information technology products employed in organizational systems.
  - Server Security Standard
  - Endpoint Device Security Standard
  - Network Device Security Standard
- West Virginia University at Parkersburg tracks, reviews, approves or disapproves, and audits changes to organizational systems.
  - Change Request Procedure
- West Virginia University at Parkersburg analyzes the security impact of changes prior to implementation.
  - Change Request Procedure
- West Virginia University at Parkersburg defines, documents, approves, and enforces physical and logical access restrictions associated with changes to organizational systems.
  - Change Request Procedure

- West Virginia University at Parkersburg restricts, disables, or prevents the use of nonessential programs, functions, ports, protocols, and services.
  - Endpoint Device Security Standard
- West Virginia University at Parkersburg applies deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
  - Endpoint Device Security Standard
- West Virginia University at Parkersburg applies deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
  - Endpoint Device Security Standard
- West Virginia University at Parkersburg controls and monitors user-installed software.
  - Endpoint Device Security Standard

Relevant NIST SP800-171 Sections

3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.
3.4.3	Track, review, approve or disapprove, and audit changes to organizational systems.
3.4.4	Analyze the security impact of changes prior to implementation.
3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.
3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.
3.4.8	Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
3.4.9	Control and monitor user-installed software.

3.8 - Identification & Authentication

Introduction

The purpose of this standard is to provide guidance to those who are responsible for granting access to West Virginia University at Parkersburg (WVUP) technology resources and data. The technology and data resources referred to within this documentation include those owned by or entrusted to the college for the purpose of supporting academic, administrative, and service related activities.

Policy

- The Office of Information Technology has implemented a formal procedure for granting, tracking, and revoking access to data. Authorization is typically implemented through the assignment of a user account. Authorization is based on the principle of least privilege, which means that a user will be given the minimum level of access needed to support his or her job responsibilities. The documented authorization controls include the following information:
    - Reason for accessing resource
    - Date of authorization
    - Effective dates or duration of authorization
    - Record of individual authorizing the access
    - Record of the individual receiving the access privileges
    - Type and scope of access privileges
    - Procedures for tracking accounts and privileges based on responsibilities and employment status, including position changes or separation from the college.
- It is the responsibility of the employee's direct supervisor to request both access and revocation of access rights.
- Data Resource requests will be tracked by the Office of Information Technology and access will be audited periodically to ensure that levels of access are still accurate and necessary.

3.9 Incident Response Policy

Scope

This policy covers all computer systems, network devices, and any additional systems and outputs containing or transmitting West Virginia University at Parkersburg (WVUP) Protected data or WVUP Sensitive data.

Purpose

The purpose of this policy is to provide a process to report suspected thefts involving data, data breaches or exposures (including unauthorized access, use, or disclosure) to appropriate individuals; and to outline the response to a confirmed theft, data breach or exposure based on the type of data involved.

Policy

- West Virginia University at Parkersburg establishes an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.
- West Virginia University at Parkersburg tracks, documents, and reports incidents to appropriate officials and/or authorities both internal and external to the organization.
- West Virginia University at Parkersburg tests the organizational incident response capability.

Reporting of suspected thefts, data breaches or exposures

Any individual who suspects that a theft, breach or exposure of WVUP Protected data or WVUP Sensitive data has occurred must immediately provide a description of what occurred via email to infosec@wvup.edu, or by calling 304-424-8215. This email address and phone number are monitored by WVUP's Information Security team. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the Information Security team will follow the appropriate procedure depending on the class of data involved.

If the incident is a suspected theft, WVUP's Security office shall also be contacted at 304-424-8235. They will determine whether a local law enforcement agency should be contacted based on the location and details of the incident. If a local law enforcement agency is contacted, the name of the agency and the report number should be provided to WVUP via the methods of contact outlined above.

Confirmed theft, data breach or exposure of WVUP Protected data or WVUP Sensitive data

As soon as a theft, data breach or exposure containing WVUP Protected data or WVUP Sensitive data is identified, the process of removing all access to that resource will begin as soon as possible. If the information is available on a site outside of WVUP, that site will be contacted to have the information removed as soon as possible.

The CIO will chair a response team to handle the breach or exposure. The team will include members from:

- Office of Information Technology
- Marketing and Communications
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed
- Additional departments based on the data type involved, as listed in the appendix
- Additional individuals as deemed necessary by the CIO

If a theft of physical property occurred, the WVUP Security Office will be notified by OIT. This team will provide information to Marketing and Communications regarding how the breach or exposure occurred, the types of data involved, the WVUP classifications of those data types, any protective measures around the involved data (such as encryption), and the number of internal/external individuals and/or organizations impacted. Marketing and Communications will handle all communications about the breach or exposure. OIT will work with the appropriate parties to remediate the root cause of the breach or exposure.

Confirmed theft, breach or exposure of WVUP Public data

The CIO will be notified of the theft, breach or exposure, and will inform Marketing and Communications as soon as possible. OIT will analyze the breach or exposure to determine the root cause. OIT will work with the appropriate parties to remediate the root cause of the breach or exposure. OIT will also examine any involved systems to ensure that they did not also house any WVUP Protected data or WVUP Sensitive data. If the systems are found to also contain WVUP Protected data or WVUP Sensitive data, the CIO will be notified and the “Confirmed data breach or exposure of WVUP Protected data or WVUP Sensitive data" section of this policy will be invoked. If a theft of physical property occurred, the WVUP Security Office will be notified by OIT. The WVUP Security Office will determine if it is also appropriate to necessary other law enforcement agencies based on where the theft occurred.

Questions about this Policy

If you have questions about this policy, please contact the Information Security team at infosec@wvup.edu.

Policy Adherence

Failure to follow this policy can result in disciplinary action as provided in the Staff Handbook, Student Worker Employment Guide, and Faculty Handbook. Disciplinary action for not following this policy may include termination, as provided in the applicable handbook or employment guide.

Appendix

For any data breaches, exposures, or thefts involving information listed below, a representative from the listed areas will be included on the response team:

Data Type	Areas or individuals to be additionally included on response team
Financial information, including but not limited to credit card, numbers, bank account numbers, investment, information, grant information, and budget information	Executive Director/CPO
Information about individual employees, including but not limited to social security numbers	Human Resources
Student financial information	Financial Aid

Student information protected by FERPA	Student Affairs, Registrar, Provost, Marketing Communication Services
Student information not listed above	Student Affairs, Marketing Communication Services
PII concerning faculty	Faculty Administration, Provost
PII concerning donors or unreleased information about gifts received	Advancement
Payroll information	Controller and/or Payroll

Checklist

This checklist covers items that the response team should consider while responding to a security incident.

- Materials that may need to be developed to handle the incident including:
  - Web pages
  - Notification letter
  - Press release
  - Q&A for media
  - Q&A for call center and other responders
- Alert university leadership teams (President, Cabinet, Information Technology Executive Steering Committee, Deans) so they understand what is being done to address the incident and are apprised of status. The order and frequency of updates to these groups will be determined by the CIO depending on the incident.

- All available information about the incident, including both information that has been confirmed and information that is suspected, will be provided to the response team. As new information is discovered, it will be provided to the response team as quickly as possible.
- Daily conference calls to checkpoint progress and obstacles are tremendously helpful in keeping things moving and sharing information.
- Size and severity (likelihood of fraud) of the incident may warrant different actions, i.e. whether credit monitoring is affordable and/or appropriate.
- Track the amount of time that has passed between incident, discovery of incident, and notification of affected individuals. While none of these steps are necessarily long, each one of them adds to the number of days to notification.
- If contracts need to be negotiated to provide services to the affected individuals, those negotiations should begin immediately. Check to see if previously negotiated contracts can be applied to the situation (especially for credit monitoring).
- Depending on the number of individuals impacted, it can take some time to assemble mailing address information for large groups. Begin pulling this data immediately.
- Identify the best location for mail merge and volume printing, envelope stuffing and metering of the mail.
- Ensure that adequate letterhead and envelopes are available or ordered. Letter should come from the Vice President in charge of the area in which the incident occurred. Determine the type of envelopes (windowed vs. address labels) as this will affect printing and speed of envelope stuffing.
- The cost of printing, letterhead, envelopes and credit monitoring will be covered by the area in which the incident occurred.
- A percentage of the initial mailings will be returned as undeliverable so the number of deliveries to attempt and methods to pull additional delivery information should be identified.

Relevant NIST SP800-171 Sections

3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.
3.6.2	Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.
3.6.3	Test the organizational incident response capability.

3.10 - Maintenance & Vulnerability Management

Policy

- West Virginia University at Parkersburg performs regular maintenance on organizational systems.
  - System Maintenance Procedure and Standard
- West Virginia University at Parkersburg provides controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
  - System Maintenance Procedure and Standard
- West Virginia University at Parkersburg ensures equipment removed for off-site maintenance is sanitized of any CUI.
  - Data Sanitation Procedure
- West Virginia University at Parkersburg will check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.
- West Virginia University at Parkersburg requires multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
  - Account Security Standard
  - MFA Policy
- West Virginia University at Parkersburg supervises the maintenance activities of maintenance personnel without required access authorization.
  - System Maintenance Procedure and Standard
- West Virginia University at Parkersburg scans for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
  - System Vulnerability Testing Procedure
- West Virginia University at Parkersburg remediates vulnerabilities in accordance with assessments of risk.
  - System Vulnerability Testing Procedure
- West Virginia University at Parkersburg monitors, controls, and protects communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.
  - Information Security Standard
- West Virginia University at Parkersburg employs architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
  - Information Security Standard
- West Virginia University at Parkersburg separates user functionality from system management functionality.

    - Information Security Standard
- West Virginia University at Parkersburg prevents unauthorized and unintended information transfer via shared system resources.
    - Information Security Standard
- West Virginia University at Parkersburg implements subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
    - Information Security Standard
- West Virginia University at Parkersburg denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).
    - Information Security Standard
- West Virginia University at Parkersburg prevents remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).
    - Information Security Standard
- West Virginia University at Parkersburg implements cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
    - Information Security Standard
- West Virginia University at Parkersburg terminates network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
    - Information Security Standard
- West Virginia University at Parkersburg establishes and manages cryptographic keys for cryptography employed in organizational systems.
    - Information Security Standard
- West Virginia University at Parkersburg employs FIPS-validated cryptography when used to protect the confidentiality of CUI.
    - Information Security Standard
- West Virginia University at Parkersburg prohibits remote activation of collaborative computing devices and provides indication of devices in use to users present at the device. From SP 800-53: “Collaborative computing devices include, for example, networked white boards, cameras, and microphones.”
    - Information Security Standard
- West Virginia University at Parkersburg controls and monitors the use of mobile code. From SP 800-53: “Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript.”
    - Information Security Standard
- West Virginia University at Parkersburg controls and monitors the use of Voice over Internet Protocol (VoIP) technologies.
    - Telecommunications Standard

- West Virginia University at Parkersburg protects the authenticity of communications sessions.
    - Information Security Standard
    - Telecommunications Standard
- West Virginia University at Parkersburg protects the confidentiality of CUI at rest.
    - Information Security Standard
- West Virginia University at Parkersburg identifies, reports, and corrects system flaws in a timely manner.
    - Information Security Standard
- West Virginia University at Parkersburg provides protection from malicious code at appropriate locations within organizational systems.
    - Information Security Standard
- West Virginia University at Parkersburg monitors system security alerts and advisories and acts in response.
    - Information Security Standard
- West Virginia University at Parkersburg updates malicious code protection mechanisms when new releases are available.
    - Anti-Virus and Anti-Malware Standard
- West Virginia University at Parkersburg performs periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.
    - Anti-Virus and Anti-Malware Standard
- West Virginia University at Parkersburg monitors organizational systems including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
    - Anti-Virus and Anti-Malware Standard
- West Virginia University at Parkersburg identifies unauthorized use of organizational systems.
    - Account Compromise Procedure
    - Account Security Standard

Related Policies, Procedures, and Standards

- Account Security Standard
- Anti-Virus and Anti-Malware Standard
- Data Sanitation Procedure
- Information Security Standard
- System Maintenance Procedure and Standard
- System Vulnerability Testing Procedure
- Telecommunications Standard

Relevant NIST SP800-171 Sections

3.7.1	Perform maintenance on organizational systems.
3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.
3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.
3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.
3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
3.11.3	Remediate vulnerabilities in accordance with assessments of risk.
3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
3.13.3	Separate user functionality from system management functionality.
3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.
3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).
3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.
3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.
3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. From SP 800-53: “Collaborative computing devices include, for example, networked white boards, cameras, and microphones.”
3.13.13	Control and monitor the use of mobile code. From SP 800-53: “Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript.”
3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.
3.13.15	Protect the authenticity of communications sessions.
3.13.16	Protect the confidentiality of CUI at rest.
3.14.1	Identify, report, and correct system flaws in a timely manner.
3.14.2	Provide protection from malicious code at appropriate locations within organizational systems.
3.14.3	Monitor system security alerts and advisories and act in response.
3.14.4	Update malicious code protection mechanisms when new releases are available.
3.14.5	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.
3.14.6	Monitor organizational systems including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
3.14.7	Identify unauthorized use of organizational systems.

3.11 - Account Security Standard

Introduction

This policy establishes a standard for the protection of the college computer information systems, data, and software. This policy establishes rights and responsibilities for the protection of staff and faculty who use these systems.

Policy

Data contained in the college systems are the property of West Virginia University at Parkersburg and represent official college records. Users who accept access to this data also accept responsibility for adhering to certain principles in the use and protection of that data.

- Information systems within the college shall be used only for and contain only data necessary for fulfillment of the college's mission.
- College data shall only be used for the legitimate business of the college.
- Due care shall be exercised to protect college data and information systems from unauthorized use, disclosure, alteration or destruction.
- College data, regardless of who collects or maintains it, shall be shared among those faculty or staff whose responsibilities require knowledge and access of such data.
- Applicable state and federal laws, as well as college policies and procedures concerning storage, retention, use, release, transportation, and destruction of data and/or all information systems contents and components shall be observed.
- Appropriate college procedures shall be followed in reporting any breach of security or compromise of safeguards.
- College information systems shall be implemented in such a way that:
  - Accuracy and completeness of all system contents are maintained during storage and processing.
  - Data, text and software stored and processed can be traced forward and backward for audit capability.
  - Information systems capabilities can be re-established within an acceptable amount of time upon loss or damage by accident, malfunction, breach of security or act of God.
  - Actual or attempted security breaches can be detected promptly.
- Any employee engaging in unauthorized use, disclosure, alteration, or destruction of information systems or data in violation of this policy shall be subject to the appropriate disciplinary action, including possible dismissal.
- Users may not utilize information systems to access data that they have not been given explicit access to. This data can include, but is not limited to:
  - transcripts, grade reports, enrollment reports

  - financial aid information
  - personnel, leave, salary reports
  - reports for government or funding agencies
  - fund-raising activities
  - mailing lists and labels
  - private or public release of data to outside parties such as students, parents and news media.

Responsibilities

The proper safeguarding of college information systems and the data contained wherein shall be the responsibility of all faculty and staff that have access and knowledge of the system or data. Specific responsibilities are as follows:

- Data Management - for each source of data, a designated manager is responsible for permitting any requested access to ensure appropriate permissions are granted.
- Management - all levels of management are responsible for ensuring that system users within their area of accountability are aware of their responsibilities as defined within the policy. Specifically, managers are required to validate the access requirements of their staff according to job functions, prior to submitting requests for the provisions of access, and for ensuring a secure office environment with regard to college information systems.
- Users - users are responsible for the protection, privacy, and control of all data, regardless of the storage medium. Users must ensure that data, including media, are maintained and disposed of in a secure manner. Users are responsible for understanding the meaning and purpose of the data to which they have access, and may use this data only to support the normal functions of the user's duties. Users are responsible for all transactions occurring under their account credentials. Account credentials shall not be shared with anyone else under any circumstances unless the Chief Information Officer specifically approves an exception.
- Chief Information Officer - Responsible for ensuring that appropriate security controls are being provided, including protection of all areas from risk of exposure.
- Office of Information Technology staff - responsible for providing administrative, technical and educational support in the area of information security for all users of administrative systems. This support includes, but is not limited to:
  - creation and deletion of user accounts, after appropriate approval has been obtained.
  - providing access to administrative systems, transaction, or production after appropriate approval.
  - Recommendations to the Chief Information Officer on appropriate training to ensure consistent practice among departmental support personnel.

Violations

The Chief Information Officer is the policy administrator for information technology resources and will ensure that this process is followed. Additionally, deans, directors, and department heads are responsible for compliance with college policy within their respective administrative areas.

3.12 - Anti-Spam, Anti-Virus Policy

Introduction

The purpose of this document is to establish a policy that ensures the proper use of West Virginia University at Parkersburg's email system by taking preventative measures against the proliferation of spam and computer viruses.

Policy

SPAM

West Virginia University at Parkersburg has the authority and responsibility to manage, control, and delete junk mail to prevent the unnecessary or inappropriate use of bandwidth to ensure that illegal, unwanted and solicited advertisements are not received on the college owned network. This policy establishes appropriate procedures to prevent email from known spammers from entering the WVUP mail system.

Spam, or junk mail, is unsolicited commercial email sent in bulk via the internet. While sending spam costs the sender practically no money, Spam puts both a cost and a burden on recipients by consuming network bandwidth and disk space, as well as wasting the time of the recipient with unwanted messages.

In order to reduce the cost to the college, the email system shall use control measures, which may include but will not necessarily be limited to filters and subscription Anti-Spam systems.

WVUP shall take all reasonable measures to use methods which minimize the blocking of legitimate email, but reserves the right to put into effect measures to avoid the financial and personnel costs of Spam emails.

Anti-virus

The purpose of the anti-virus policy is to prevent the infection of college owned computers and systems by computer viruses and other malicious code. This policy is intended to prevent major and widespread damage to user applications, data, and hardware and to prevent the financial losses resulting from such damage. The WVUP email server (Google Apps) has virus protection software built in that:

- Inspects every incoming and outgoing message.

- Automatically deletes all email attachments that include, but are not limited to the following extensions: exe, pdf, vbs.
- If the infected message cannot be cleaned, then it will be deleted.

In addition, WVUP's network infrastructure is protected by a SonicWall network security device that provides firewall protection, as well as IDS/IPS, Content Filtering, and antivirus scanning services.

Responsibilities

WVUP email users shall follow these guidelines to avoid receiving unwanted email:

- Do not register with email directory services aside from official college or association sources.
- Never reply to a SPAM message that you receive. Delete it.
- Use an alternative email address to post to bulletin boards or forums.

WVUP computer users shall follow these guidelines to avoid viruses and other forms of malware:

- All computers connected to WVUP's network or capable of accessing the network shall have WVUP supported anti-virus software installed, configured, activated, and updated with the latest virus definitions before or immediately upon connecting to the network.
- All IT-managed computers will have anti-virus software installed that is centrally managed and updated.
- If a computer is detected as infected, it will be disconnected from the college network until the issue is remediated to prevent propagation of the virus to other devices on the network.
- If a message is received that appears to be suspicious, please do not open any attachments.

3.13 - Data Sanitation Procedure

I. Overview:

West Virginia University at Parkersburg sanitizes or destroys system media containing CUI before disposal or release for reuse.

II. System Sanitation:

A. Equipment Replacement:

In the event the individual replaces their primary device, the media is removed from the device and placed in a fire safe. The media is coded and will remain in the fire safe until it is disposed of.

B. Equipment Redistribution
Equipment reissued to another individual is wiped and reimaged with a new operating system installed.

III. Media Disposal:
Media containing CUI is disposed of via the destruction of the entire unit. The serial number of each media item is logged and the media is shredded on site via a local disposal company

Information Security & Risk Assessment

Policy

- West Virginia University at Parkersburg periodically assesses the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.
- West Virginia University at Parkersburg periodically assesses the security controls in organizational systems to determine if the controls are effective in their application.
- West Virginia University at Parkersburg develops and implements plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
- West Virginia University at Parkersburg monitors security controls on an ongoing basis to ensure the continued effectiveness of the controls.
- West Virginia University at Parkersburg develops, documents, and periodically updates system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

Relevant NIST SP800-171 Sections

3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.
3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.
3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

3.14 Media Security Policy

Policy

- West Virginia University at Parkersburg protects (i.e., physically controls and securely stores) system media containing CUI, both paper and digital.
- West Virginia University at Parkersburg limits access to CUI on system media to authorized users.
  - Information Security Standard
- West Virginia University at Parkersburg sanitizes or destroys system media containing CUI before disposal or release for reuse.
  - Data Sanitation Procedure
- West Virginia University at Parkersburg marks media with necessary CUI markings and distribution limitations.
  - Information Security Standard
- West Virginia University at Parkersburg controls access to media containing CUI and maintains accountability for media during transport outside of controlled areas.
  - Information Security Standard
- West Virginia University at Parkersburg implements cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
  - Information Security Standard
- West Virginia University at Parkersburg controls the use of removable media on system components.
  - Endpoint Device Security Standard
- West Virginia University at Parkersburg prohibits the use of portable storage devices when such devices have no identifiable owner.

  - Endpoint Device Security Standard
- West Virginia University at Parkersburg protects the confidentiality of backup CUI at storage locations.
  - System Maintenance Procedure and Standard

Related Policies, Procedures, and Standards

- Data Sanitation Procedure
- Endpoint Device Security Standard
- Information Security Standard
- System Maintenance Procedure and Standard

Relevant NIST SP800-171 Sections

3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.
3.8.2	Limit access to CUI on system media to authorized users.
3.8.3	Sanitize or destroy system media containing CUI before disposal or release for reuse.
3.8.4	Mark media with necessary CUI markings and distribution limitations.
3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
3.8.7	Control the use of removable media on system components.
3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.
3.8.9	Protect the confidentiality of backup CUI at storage locations.

3.15 - Personnel Security and Security Awareness Training

Policy

Security Awareness Training

- West Virginia University at Parkersburg ensures that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

- West Virginia University at Parkersburg ensures that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
- West Virginia University at Parkersburg provides security awareness training on recognizing and reporting potential indicators of insider threat.

Personnel Security

- West Virginia University at Parkersburg screens individuals prior to authorizing access to organizational systems containing CUI.
- West Virginia University at Parkersburg ensures that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

Related Policies, Procedures, and Standards

- Employee Training Standard
- Personnel Onboarding Procedures

Relevant NIST SP800-171 Sections

3.2.1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
3.2.2	Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.
3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.
3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

WVUP Employee Onboarding

Welcome to West Virginia University at Parkersburg. As an employee of the college, you will have access to multiple campus systems. Your role will determine which specialized system access you will have, but all employees are issued a WVUP email account.

Important Information:

- Never share your WVUP ID with ANYONE. (Treat your WVUP ID like your Social Security Number.)
- Never share your WVUP Network ID and Password.
- Never share your OLSIS PIN or Security Question.

WVUP Systems

General Systems:

WVUP Find My ID: *https://findmyid.wvup.edu/*

Find My ID portal allows an individual to look up login usernames for all the systems a person would need to access at WVUP. Employees can also look up their WVUP ID, using this portal.

WVUP Email: *https://webmail.wvup.edu/*

A WVUP Email account is an institutionally generated email account. It will be the primary email for sending valuable information concerning events and important updates from the college. Each employee is responsible for checking their WVUP Email account.

WVUP Network ID and Password are used for WVUP Email, Blackboard, resources Library resources and access to campus computers.

Password Self-Service: https://pw.wvup.edu/

This system allows employees to reset their WVUP Network ID Password 24/7. Systems which use WVUP Network credentials are: Campus Computers, Blackboard, Off-Site Library Resources and WVUP Email.

3.16 - Physical Protection

Policy

- West Virginia University at Parkersburg limits physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.
- West Virginia University at Parkersburg protects and monitors the physical facility and support infrastructure for organizational systems.
- West Virginia University at Parkersburg escorts visitors and monitors visitor activity.

- West Virginia University at Parkersburg maintains audit logs of physical access.
- West Virginia University at Parkersburg controls and manages physical access devices.
- West Virginia University at Parkersburg enforces safeguarding measures for CUI at alternate work sites.

Relevant NIST SP800-171 Sections

3.10.1	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.
3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.
3.10.3	Escort visitors and monitor visitor activity.
3.10.4	Maintain audit logs of physical access.
3.10.5	Control and manage physical access devices.
3.10.6	Enforce safeguarding measures for CUI at alternate work sites.

3.17 Risk & Security Assessment

Policy

- West Virginia University at Parkersburg periodically assesses the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.
- West Virginia University at Parkersburg periodically assesses the security controls in organizational systems to determine if the controls are effective in their application.
- West Virginia University at Parkersburg develops and implements plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
- West Virginia University at Parkersburg monitors security controls on an ongoing basis to ensure the continued effectiveness of the controls.
- West Virginia University at Parkersburg develops, documents, and periodically updates system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

3.18 Systems and Communication Protection

Campus Telecommunications Standard

Introduction

The purpose of this standard is to define the requirements to ensure availability, stability, and efficient operations management of West Virginia University at Parkersburg telecommunications voice systems. This standard is designed to minimize the potential exposure of West Virginia University at Parkersburg and its community to damages, attacks, and unauthorized access.

This standard applies to:

- All students, employees and guests who order or use WVUP telecommunications infrastructure.
- Any entities that operate external systems which directly interconnect with WVUP telecommunications voice systems.
- WVUP telecommunications infrastructure (including components purchased with grant funding) and privately-owned equipment that directly connects to the telecommunications infrastructure.

Telecommunications equipment includes all WVUP-owned or leased equipment, services and cabling that is used for providing fax or voice telecommunications service. This equipment includes, but is not limited to, telephones, voice mail servers and software, routers, and fiber optic and copper cabling.

Policy

- The West Virginia University at Parkersburg Office of Information Technology is responsible for designing, managing, and securing the WVUP telecommunications system infrastructure.
- Only specific classes of devices may be connected to the WVUP telecommunications infrastructure. Approved devices are:
  - Commercial-quality analog and digital telephone devices approved by OIT.
  - Voice Over IP (VOIP) devices approved by OIT.
- The Office of Information Technology shall have authority over all physical and logical VOIP interfaces and connections with any legacy voice systems.
- Unapproved modifications or extensions to the WVUP telecommunications system, including but not limited to extending data networks that carry VOIP transmissions, is prohibited.
- Call detail records of calls placed or received on the campus telecommunications system are kept for a short period of time. This information is available upon request for official law enforcement entities or as advised by WVUP legal counsel. OIT shall deny or

prevent requests for device or line additions or changes if it determines that the change would adversely affect WVUP business or educational operations, system stability, or overall availability or security.

- OIT maintains contracts and accounts with external service providers for the purposes of providing Public Switched Telephone Network access, intercampus and intra campus communications, and access to additional services. All requests for goods and services through these contracts shall be made through OIT.

Violations

Violation of this standard will be addressed in accordance with established college 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 one’s employment or studies.

3.19 Systems and Information Integrity

Introduction

The discipline of information systems security relies on the practice of ensuring and maintaining the confidentiality, integrity, and availability of information systems and the data transmitted, processed, and/or stored on those systems. Integrity is defined as guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity. It is the assertion that data can only be accessed or modified by authorized entities.

PURPOSE

System and information integrity provide assurance that the information being accessed has not been tampered with or damaged by an error in the information system. Examples of system and information integrity requirements include:

- Flaw remediation;
- Malicious code protection;
- Information system monitoring;
- Security alerts;
- Information input validation;
- Error-handling; and
- Memory protection.

SCOPE

This policy applies to all institutional business units, workforce members, and institutional information systems that collect, store, process, share, or transmit institutional data.

Policy

Information owners are accountable for developing appropriate procedures for the implementation of this policy.

IMPORTANT! Information owners are to develop procedures to implement this policy in a reasonable amount of time, not to exceed 12 months after this policy goes into effect.

BEFORE INSTALLATION

Before installation of information systems, institutional business units must:

- Identify, report, and correct information system flaws; and
- Test software updates on nonproduction systems for potential side effects on University information assets.

SOFTWARE AND FIRMWARE UPDATES

After installation, institutional business units must install security-relevant software and firmware updates within an appropriate amount of time, in accordance with University policies and business unit procedures.

Flaw Remediation

Automated processes are to be used continuously to identify the state of information systems regarding flaw remediation.

MALICIOUS CODE PROTECTION MECHANISMS

Malicious code protection mechanisms must be employed at information system entry and exit points as well as system endpoints to detect and eradicate malicious code. The malicious code protection mechanisms are to be automatically updated whenever new releases are available, in accordance with University policies and business unit procedures.

Configuration

Malicious code protection mechanisms are to be configured to perform periodic scans of the information systems and take automated actions against any malicious code that is found. Information systems are to be scanned on a regular basis for malicious code and in real-time on system endpoints and information system exit points, as files are downloaded, opened, or executed.

Malicious Code Detection

On detection of malicious code, the malicious code protection mechanisms must block and/or quarantine malicious code and send alerts to the WVUP OIT

MONITORING

In accordance with the University's established logging and monitoring objectives, WVUP policies, and applicable laws, regulations, and standards, institutional business owners must ensure that information systems are monitored to detect:

- Attacks;
- Indicators of potential attacks; and
- Unauthorized use.

Regular Monitoring

Information systems as well as information system boundaries (i.e., perimeters) are to be monitored continuously to provide near real-time analysis of alerts and/or notifications generated by institutional information systems.

Heightened Risk Monitoring

The level of information system monitoring is to be heightened when there is an indication of increased risk to University operations and assets, individuals, and/or other organizations.

Alerts

Malicious Code

When indications of compromise are received from malicious code protection mechanisms, automated alerts are generated and sent to the WVUP OIT.

External Security Alerts, Advisories, and Directives

Business units are to receive information system security alerts, advisories, and directives on an ongoing basis from:

- United States Computer Emergency Readiness Team (US-CERT);
- WVUP Chief Information Officer (CIO);

- Other organizations, as warranted.

Internal Security Alerts, Advisories, and Directives

Business units must ensure that internal security alerts, advisories, and directives are generated as deemed necessary and disseminated to institutional area technology officers (ATOs), information system owners, and other appropriate business unit personnel according to their roles.

Implementation

Security alerts, advisories, and directives must be implemented within established time frames defined in University polices and business unit procedures.

List of Authorized Information Systems

Business units must maintain a list of authorized business information systems and software and protect the list from the loss of integrity.

Integrity Checks

Integrity checks of the authorized business systems and software are to be performed during system startup, restart, and shutdown.

Unauthorized Change Detection

The detection of unauthorized changes to authorized business systems and software must be integrated into University business unit incident response processes.

Spam Protection

Centrally managed spam protection mechanisms must be employed at information system entry and exit points to detect and act on unsolicited messages.

Automatic Updates

Information systems are to be automatically updated when new releases become available, in accordance with University policies and business unit change management processes.

Input Validity Checks

Where operationally feasible, institutional information systems are to check the validity of system inputs to help ensure accurate and correct inputs and prevent cyberattacks, such as crosssite scripting and a variety of injection attacks. System inputs may include, but are not limited to, character set, length, numerical range, and acceptable values.

Error Messages

University information system developers must ensure error messages generated from the information system provide the information necessary for corrective actions without revealing information that could be exploited by adversaries.

Enforcement

The Office of the Chief Information Officer (CIO) is responsible and has the authority for enforcing compliance with this policy.

Exceptions

Exceptions to this policy are managed and maintained by the Office of the CIO, under the guidance of the University Chief Information Security Officer (CSIO).

The Office of the CIO must document and maintain all policy exceptions in writing for the life of the exception. Approvals for policy exceptions are effective for a specified period of time and must be reviewed by the Office of the CIO on a periodic basis.

Maintenance

The Office of the CIO is to review this policy every three years or on an as-needed basis due to changes to technology environments, business operations, standards, or regulatory requirements.

3.20 Campus Telecommunications Standard

Introduction

The purpose of this standard is to define the requirements to ensure availability, stability, and efficient operations management of West Virginia University at Parkersburg telecommunications voice systems. This standard is designed to minimize the potential exposure of West Virginia University at Parkersburg and its community to damages, attacks, and unauthorized access.

This standard applies to:

- All students, employees and guests who order or use WVUP telecommunications infrastructure.
- Any entities that operate external systems which directly interconnect with WVUP telecommunications voice systems.

- WVUP telecommunications infrastructure (including components purchased with grant funding) and privately-owned equipment that directly connects to the telecommunications infrastructure.

Telecommunications equipment includes all WVUP-owned or leased equipment, services and cabling that is used for providing fax or voice telecommunications service. This equipment includes, but is not limited to, telephones, voice mail servers and software, routers, and fiber optic and copper cabling.

Effective Date

Policy

- The West Virginia University at Parkersburg Office of Information Technology is responsible for designing, managing, and securing the WVUP telecommunications system infrastructure.
- Only specific classes of devices may be connected to the WVUP telecommunications infrastructure. Approved devices are:
    - Commercial-quality analog and digital telephone devices approved by OIT.
    - Voice Over IP (VOIP) devices approved by OIT.
- The Office of Information Technology shall have authority over all physical and logical VOIP interfaces and connections with any legacy voice systems.
- Unapproved modifications or extensions to the WVUP telecommunications system, including but not limited to extending data networks that carry VOIP transmissions, is prohibited.
- Call detail records of calls placed or received on the campus telecommunications system are kept for a short period of time. This information is available upon request for official law enforcement entities or as advised by WVUP legal counsel. OIT shall deny or prevent requests for device or line additions or changes if it determines that the change would adversely affect WVUP business or educational operations, system stability, or overall availability or security.
- OIT maintains contracts and accounts with external service providers for the purposes of providing Public Switched Telephone Network access, intercampus and intra campus communications, and access to additional services. All requests for goods and services through these contracts shall be made through OIT.

Violations

Violation of this standard will be addressed in accordance with established college 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 one’s employment or studies.