INFORMATION TECHONOLGY POLICY
CATS - INFORMATION TECHNOLOGY

VERSION HISTORY

Version	Date	Author Name	Reason for Revision
1.1	4/10/2013	Mike Natale	Initial Publication
1.1	4-9-2014	Ken Nelson	Annual Review
1.1	05-25-2015	Michael Natale	Annual Review
1.2	05-25-2015	Michael Natale	Modified Director of CaTS to CIO of CaTS
1.2	08-01-2016	Michael Natale	Annual Review
1.2	10-01-2017	Michael Natale	Annual Review
1.2	02-01-2019	Michael Natale	Minor updates to protocol use (RDP, Telnet, FTP)
1.3	1-23-2020	John Remley	Minor updates to Inappropriate Use definition, and other various edits.
1.3	9-21-2021	John Remley	Annual Review and minor edits
1.3	11-23-2021	Matt Hemker	Added SRE assets to monthly vulnerability scanning
1.3	4-21-2022	Mike Natale	Annual Review
1.3	2-23-2024	Mike Natale	Annual Review

	Wright State University Information Security	

Controls	
Policy Title:	Information Technology Policy
Category:	Information Technology
Audience:	WSU Faculty, Staff, and Students
Reason for Revision:	*N/A*
Created / Modified Date:	4-10-13
Next Review Date:	9-21-2022
Location:	http://www.wright.edu/security/policy/

Responsible Parties	
Author	Michael Natale
Technical Reviewer/Mgr	Michael Natale

TABLE OF CONTENTS

Policy Purpose

The purpose of this policy is to implement the minimum guidelines for the establishment, administration and maintenance of security for the WSU CaTS network resources as related to campus Intranet and Internet connection.

This policy is not written to restrict the use of the network, but to ensure that adequate protection is in place to protect WSU data from attacks, unauthorized file access and service disruption.

Responsibility

The CISO of CaTS will:

- Review WSU Network Security policies, procedures, and guidelines for the protection of WSU information system resources
- Approve WSU Network Security policy
- Reassess WSU Network Security policy, and associated procedures and guidelines periodically to ensure validity
- Maintain and enforce an appropriate level of compliance

The WSU Security Function will:

- Develop, coordinate, implement, interpret, and maintain Internet Security policies, procedures, and guidelines for the protection of WSU information system resources.
- Determine adequacy of security measures used.
- Conduct periodic risk assessments, security evaluations, and internal control reviews of WSU systems.
- Update WSU Network security policy accordingly

WSU CaTS and the University community will:

- Support CaTS efforts and comply with security policies
- Enforce security policies within perspective departments

The WSU CaTS Network and Systems Staff will:

- Assist in the development and maintenance of security policies, procedures, and guidelines
- Adhere to security policies, procedures, and guidelines
- Report any misuse or incident to management and the Security Function

Actions

All users of data and systems are responsible for complying with this network and systems security policy, as well as procedures and practices developed in support of this policy.

Anyone suspecting misuse or attempted misuse of WSU systems resources is responsible for reporting such activity to their management and/or to the Security Function.

Violations of standards, procedures, or practices outlined in this policy will be brought to the attention of CIO of CaTS and the Security Function for action.

Point of Contact

Report all incidents and refer all questions to WSU Information Security Function via the Helpdesk or WSU ServiceNow.

Definitions

For the purposes of this policy, the following definitions will apply:

WSU - Wright State University
CaTS - Computing and Telecommunications Services
CaTS Staff - a group of full-time professional staff and part-time student employees who work in the areas of network and systems support.
Security Function – any person(s) designated with the responsibility for administering the security strategy
System Resources - any information or software applications or tools in electronic format, including, but not limited to electronic mail, local databases, externally accessed databases and any digitized information that may be made available on the LAN/WAN.
Inappropriate Use - improper use of computing resources, use of computing resources for non-university purposes, including commercial use, any violation of local, state and/or federal law, or any other prohibited use as set forth in this policy.
Users – refers to any person consuming resources on the WSU network. This includes all permanent and temporary university personnel, faculty and students, including WSU managed contractors, consultants and vendor partners, who are authorized by WSU to access the WSU network.
General Public – refers to any client who is authorized to use WSU resources without an account (for example, the public stations in the library).
Internet Access – includes viewing Web sites, sending and receiving e-mail, transmitting and receiving files, and running Internet applications from global Internet.
WSU Network – consists of electronic devices communicating with one another and sharing hardware, software, data, and information resources. Includes all of the communication and computer hardware, operating systems, data, application software and any stored electronic media utilized to facilitate access to or provide information from the WSU Intranet and global Internet.

Associated WSU Policies

Responsible Use of University Computing Resources – WrightWay Policy number*: 11210* – refer to this document for guidelines for responsible use of Wright State University computing resources.

Policy for Responsible Use of Information Technology (Student) - refer to this document for guidelines for responsible use of WSU network.

World Wide Web Policy - refer to this document for guidelines applicable to Web services.

Computing and Telecommunications Account Policy Statement - refer to this document for guidelines and responsibilities for user accounts.

Computer Account Application - refer to this document for required client information

Wright State University computing and network resources are intended for university-related communications and information exchange with public, educational, and other research or information resources.

The Wright State University CaTS organization is responsible for securing the campus backbone and central systems resources against unauthorized access and/or abuse, while making them accessible for authorized and legitimate users. This responsibility includes informing users of expected standards of conduct and the punitive measures for non-adherence. Any attempt to violate the premise of this policy will result in disciplinary action.

The users of the network are responsible for respecting and adhering to local, state, federal, international laws and University standards of conduct and policies. Any attempt to break those laws through the use of the WSU network or systems resources may result in litigation against the offender by the proper authorities. If such an event should occur, WSU and CaTS will fully comply with the authorities to provide any information necessary for the litigation process.

Access to University resources and the Internet from a home computer through the University must adhere to the same policies that apply to use from within the University facilities.

General Guidelines

The Security Function, CIO, and Associate CIOs of CaTS will review the Network Security Policy on a regular basis (yearly minimum). Where requirements for network connections and services have changed, the security policy will be updated and approved. If a change is to be made, the Security Function will ensure that the change is implemented and the policy modified.

The details of WSU's security architecture will not be visible from outside the firewall, nor will information be provided to users or vendors unless specific justification and approval are met.

System administration staff will inspect systems resources periodically to verify system best practices are implemented.

Data, which is protected by the Family Education Rights and Privacy Act of 1974 and the Ohio Revised Code Section 102, will not be transmitted over the Internet in clear text. Access to this data is only permitted by those approved and must be authenticated prior to retrieval.

Host-based security is a required method of protecting system resources. However, WSU will use a layered approach of overlapping controls, monitoring and authentication to ensure overall security of WSU network and systems resources.

No WSU system or network subnet which houses privacy or protected information can have connection to the Internet without the use of firewall(s) or some other means to protect the information deemed appropriate by WSU Security Function.

Mandatory scans for vulnerability and susceptibility to risk of existing firewall(s) are required at annual intervals. The initial assessment should be completed within three (3) months of the issuance of this policy and initial installation of protection systems.

The Security Function will conduct daily reviews of audit trails of firewall(s), router(s) and monitoring platforms for breaches of security.

Systems resources will be scanned regularly to ensure compliance with WSU security guidelines.

Vulnerable protocols such as, but not limited to, FTP, Telnet, RDP will not be accessible from the Internet. These protocols should be replaced with their secure counter parts, sFTP, SSH, Secure RDP to access systems. Secure RDP will only be assessable from off campus via VPN.

Time Synchronization: All systems in scope for PCI-DSS are required to be time synchronized to an on Campus time source. Campus Time Servers are sync'd to the Oarnet time servers, which are in turn synchronized to the Naval Observatory Time Servers. Only CaTS Networking function and Security function will have access to time synchronization data. Time synchronization activity is logged to the central Security Information and Event Management System (SIEM).

Virus Handling

Anti-virus software will be installed on file servers to limit the spread of viruses within the network. Scanning of all files and executable will occur daily on the file servers. Workstations will have memory resident anti-virus software installed and configured to scan data as it enters the computer. Programs will not be executed, and files opened by applications prone to macro viruses without prior scanning.

Clients share the responsibility for scanning incoming electronic mail for viruses.

Employee security training should include information about virus infection risks.

Virus scanning tools will be configured to automatically update.

Users should inform the Security Function, systems administrator or Help Desk of any virus that is detected, configuration change or different behaviour of a computer or applications via in-person, phone or by e-mail.

When informed that a virus has been detected the system administrators should inform all users who may have access to the same programs or data that a virus might have also infected their system. The users will be informed of the steps necessary to determine if their system is infected and the steps to take to remove the virus. Users will report the results of scanning and removal activity to the system administrators.

Any system suspected to be infected by a virus will be reported to the Security Function. The system may be disconnected to the network until Security Function or systems administration staff can verify that the virus has been neutralized or removed. If virus-scanning software fails to remove the virus, all software on the computer will be deleted including boot records if necessary. The software will then be reinstalled with uninfected sources and re-scanned for viruses.

Logging and Intrusion Detection

Operating system and application software logging processes should be enabled on all host and server systems located on server segments.

All system and network devices in scope for PCI-DSS are to log to a central log system. The minimum logging will include audit trails, invalid access attempts, identification/authentication, modification of audit logs, creation/deletion of system level objects, anti-virus logs, and time setting changes.

The central logging system will restrict access to logs to only authorized personnel. The security function will have access to all logs.

File Integrity monitoring will be utilized for all PCI-DSS assets.

Logging processes must be enabled on all WSU Network routers and main switches.

All network traffic may be logged.

Firewall logs are retained for ninety days. PCI-DSS network devices, firewalls, servers, and payment stations will have logs retained for a minimum of 1 year.

System integrity checks of firewall(s), monitoring/reporting system(s) and other network perimeter access control systems must be performed no less than on a weekly basis.

Audit logs from firewall(s), monitoring/reporting system(s) and perimeter access control systems must be reviewed daily.

Audit logs for servers and hosts on server segments should be reviewed on a daily basis.

All trouble reports received by system administration personnel should be reviewed for symptoms that might indicate intrusive activity.

All servers located on server segments, Domain Name Servers, authentication servers and mail servers must utilize additional host-based monitoring tools to supplement (if necessary) the activity logging process provided by the operating system.

Host-based intrusion tools, such as Tripwire, will be checked on a routine basis.

Unless critical systems have been compromised, WSU will first make an attempt to track intruders before correcting systems. The Security Function has the authority to make decisions concerning closing security holes or attempting to learn more about the intruder. Those making these decisions must be well trained in legal issues surrounding incident handling and must abide by the procedures outlined in the WSU Incident Response process.

Rogue Wireless Detection: A process to detect and identify rogue wireless access points will be run on a daily basis. Any rogues detected on the PCI-DSS network are to be removed immediately. Logs/reports of rogue activity are to be kept for 1 year.

Vulnerability Scans: Internal vulnerability scans of all servers and network devices will be conducted on a quarterly basis. Internal vulnerability scans of all PCI-DSS and SRE assets will be conducted on a monthly basis. External vulnerability scans and penetration test will be conducted annually.

Network Policy

Decryption or sniffing of systems, networks or user passwords is prohibited except for intrusion detection or security logging purposes or in the process of protecting system resources by the Security Function or their delegates.

The Security Function and systems administrators will be required to monitor CERT and appropriate systems and application vendors for security related information, relevant threats, vulnerabilities, or incidents and relevant service patches, upgrades or updates.

Any attempts to secure a higher level of privilege on network or system resources than authorized are prohibited.

The wilful introduction of computer “viruses” or disruptive/destructive programs into the WSU network or into external networks is prohibited.

The CIO or an Associate CIOs of CaTS must approve all connections from/to the WSU network to external networks for network services. All connections to approved external networks will pass through approved firewalls or other perimeter control security systems.

An unsecured system is a one that is not supported by the CaTS staff. The primary user of the system, or someone designated by departments’ management, is responsible for the integrity of the system, and will ensure the system meets the minimum WSU security requirements. The responsible person or group ensures that the security of the system is maintained by installing needed security patches and security checking programs. Unsecured systems are treated as unsecured by the WSU network and are viewed, as much as possible, like any other system on the Internet.

Router Policy

Router alarm, alert functions and logging must be enabled.

Router passwords will be encrypted.

Appropriate router documentation will be maintained on off-line secure storage at all times. Such information will include but not be limited to the network diagram, including all IP addresses of all network devices, the IP addresses of relevant hosts of the Internet Service Provider (ISP) such as external news server, router, DNS server, etc. and all other configuration parameters and access lists. Documentation will be updated any time there is a configuration change.

The Security Function and router administrator(s) must evaluate each new release of the router operating system software to determine if an upgrade is required. All security patches recommended by the router vendor must be implemented in a timely manner.

The Security Function and router administrator(s) will monitor the router vendor's mailing list or maintain some other form of contact with the vendor to be aware of all required upgrades. After any upgrade, router assurance testing will be completed to verify proper operation and configuration prior to going operational.

Access to routers should be via a secure username and password based on a centralized database. Each user must have a unique identifier utilizing two-factor authentication for remote access.

Rule set review for routers in scope for PCI-DSS will be conducted semi-annually.

Internet

Users posting to newsgroups, Internet mailing lists, etc. should include a university disclaimer as part of each message.

WSU will not register, filter, monitor or otherwise control Internet web sites except in extraordinary cases where it is obvious that the integrity of the WSU network or systems resources might be compromised or if it is obvious that the web site violates federal, state or local laws.

WSU will monitor Internet connections for activity that is detrimental to WSU network operations.

The Security Function, CIO and Associate CIOs of CaTS must approve connections to servers with potentially large and constant traffic generating applications. Connection will be reviewed as to operational impact and effect to network capacity.

Protection has been placed between WSU trusted networks and the Internet to protect systems resources and data. Users will not circumvent the firewall by using modems or network tunnelling software to connect to the Internet unless specifically reviewed by Security Function. Approval will be based on impact to security architecture and justification of need.

Specific protocols and services have been blocked or redirected. If department or user has a specific need for a particular protocol or service – user must raise the issue with the Security Function. Approval will be based on impact to security architecture and justification of need.

All other forms of Internet access (such as via dial-out modems) from sites connected to the WSU network is discouraged.

Firewall

If multiple University firewalls utilized in parallel for availability or performance reasons, the configuration of each firewall will be identical and under the control of the Security Function.

Any change to any University PCI-DSS firewall must follow the appropriate Change Management procedures.

Firewall accounts will be limited to only those absolutely necessary.

The password policy for firewall system(s) will be different than those stated in the Password Management Policy due to the need for strong authentication for this critical security component. The root password(s) will be a minimum of eight (8) characters, alphanumeric, not be a phrase or common word, no repeat passwords for ten (10) changes and should be changed at minimum every 180 days or immediately if the password is compromised.

The PCI-DSS firewall policy rules will be reviewed every 6 months.

The firewall(s) will view any attempt to gain access to the WSU network or systems resources behind the firewall as non-trusted.

All services on the firewall(s) that are not needed will be disabled, including other network access, user shells and applications.

Firewall(s) must utilize additional host-based monitoring tools to supplement the activity logging process provided by the operating system.

If a firewall(s) fails – connection to Internet should be immediately terminated until incident response plan is implemented.

Firewall(s) should fail to a configuration that denies all services, and require a firewall administrator to re-enable services after a failure.

Appropriate firewall documentation will be maintained on off-line secure storage at all times. Such information will include but not be limited to the network diagram, including all IP addresses of all network devices, the IP addresses of relevant hosts of the Internet Service Provider (ISP) such as external news server, router, DNS server, etc. and all other configuration parameters such as packet filter rules, etc. Documentation will be updated any time the firewall configuration is changed.

University firewalls will be located in a controlled environment, with access limited to the authorized personnel designated by CIO of CaTS.

Firewall(s) must be physically located in facility that is equipped with heat, air-conditioner, and smoke alarms to assure the proper working order of the room. Uninterruptible power service must be provided to the firewall.

If an incident has been detected, a firewall may need to be brought down and reconfigured. If it is necessary to bring down the firewall, Internet service must be disabled or a secondary firewall made operational - internal systems will not be connected to the Internet without a firewall. After being reconfigured, the firewall must be brought back into an operational and reliable state. The process should be conducted in accordance with WSU Incident Response process.

PCI-DSS firewall policy will be set to deny all for inbound and outbound traffic with the exception of those protocols and services needed to conduct business – such as: HTTP/HTTPS, Card Reader Ports. Protocols that are not encrypted such as telnet, snmp, ftp, etc. are not allowed.

General Administration

The Security Function and/or firewall administrators must evaluate each new release of the firewall software to determine if an upgrade is required. All security patches recommended by the firewall vendor should be implemented in a timely manner.

Any firewall specific upgrades will be obtained from the specific firewall product vendor only. The use of virus checked CDROM or secure file transfer to a vendor's site is an appropriate method.

The Security Function will monitor the firewall vendor's mailing list or maintain some other form of contact with the vendor to be aware of all required upgrades. Before an upgrade of any of the firewall component, the firewall administrator must verify with the vendor that an upgrade is required. After any upgrade the firewall assurance testing will be completed to verify proper operation and configuration prior to going operational.

Remote Administration

Remote access over untrusted networks to the firewall for administration purposes must use secure access methods with two-factor authentication.

Remote access for firewall administration is allowed from trusted segments on the WSU network. Encrypted communication between management station and firewall, strong authentication and unique account names are required. Passwords must meet policies specified previously.

Backup

The firewall(s) (system software, configuration data, database files, etc.) must be backed up according the Disaster Recovery Policy. Backup files should be stored securely on a read-only media so that data in storage is not over-written inadvertently and locked in secure facility to ensure media is only accessible to the appropriate personnel.

System failure and data / configuration recovery must be tested annually.

Firewall(s) hardware must be kept on maintenance contract with hardware vendor. Maintenance program must be twenty four-hour response time and replacement of failed components. WSU must keep spare components on-site as appropriate.

Demilitarized Zone

A subnet will be configured as a perimeter network (DMZ) to separate the internal network from the external.

A screening technology will be utilized between the DMZ and Internet connection. Internal network routers will be configured to screen and filter network access.

The DMZ will house the appropriate WSU external servers.

Configuration

System(s) at minimum must be configured according to firewall vendor specifications.

Inbound E-mail gateway commands (EXPN and VFRY) must be disabled and removed.

Tunnels through firewall(s) to the Internet to allow friendly systems or users special entrance access will not be allowed unless specifically reviewed by Security Function. Approval will be based on impact to security architecture and justification of need.

Source routing will be disabled on all firewalls and routers.

The firewall will not accept traffic on its external interfaces that appear to be coming from internal network addresses.

The firewall will provide detailed audit logs of all sessions so that these logs can be reviewed for any anomalies.

Media will be used to store log reports such that access to this media is restricted to only authorized personnel.

Firewalls will be tested off-line and the proper configuration verified.

Unless approved by the Security Function, all in-bound services will be intercepted and processed by the firewall.

The firewall will be configured to deny all services not expressly authorized by CaTS and will be regularly audited and monitored to detect intrusions or misuse.

The firewall will be configured to notify the firewall administrators of any time that needs immediate attention such as a lack of available disk space.

To prevent unauthorized modifications of the firewall configuration, some form of integrity assurance process will be used. Typically, checksums, cyclic redundancy checks, or cryptographic hashes are made from the runtime image and saved on protected media. Each time the firewall configuration has been modified by an authorized individual (usually the firewall administrator), it is necessary that the system integrity online database be updated and saved onto a file system on the network or removable media. If the system integrity check shows that the firewall configuration files have been modified, it will be known that the system has been compromised.

The firewall system integrity database will be updated each time the firewall configuration is modified. System integrity will be checked on a regular basis on the firewall in order for the administrator to generate a listing of all files that may have been modified, replaced, or deleted.

The firewall will be configured to log / archive all reports on daily, weekly, and monthly bases so that the network activity can be analysed when needed.

In case of a firewall break-in, the firewall administrator(s) are responsible for reconfiguring the firewall to address any vulnerabilities that were exploited. The firewall will be restored to the state it was before the break-in so that the network is not left wide open and will address exploited vulnerability.

To optimize the performance of the firewall, all vendor recommendations for processor and memory capacities will be followed.

E-mail

Forgery (or attempted forgery) of electronic mail messages is prohibited.

Attempts to read, delete, copy, or modify the electronic mail of other users are prohibited.

Attempts at sending harassing, obscene and/or other threatening email to another user are prohibited.

Attempts at sending unsolicited junk mail, “for-profit” messages or chain letters is prohibited.

Use of electronic mail services for purposes constituting clear conflict of WSU interests or in violation of Policy for Responsible Use of Information Technology is expressly prohibited.

The use of email in any way to facilitate the conduct of a private commercial purpose is prohibited.

The contents of email messages will not be considered private and are subject to the Sunshine Laws.

Users may not use WSU CaTS’ mail servers for any purpose prohibited by this policy.

Network Back-Up

CaTS staff will prevent loss of data in the event of hardware or software failure or through human error by making periodic backup copies of data to magnetic tape or other media. It must be recognized, however, that in rare cases it may not be possible to restore the latest version of every data file from these backups, and some data loss may occur. Because these cases are outside of the CaTS staff's control, the staff cannot be held liable for any loss of data arising directly or indirectly from the failure of hardware, software, or from human error.

Network and system data will be backed up according to a backup schedule. Backup files should be stored securely on a read-only media so that data in storage is not over-written inadvertently and locked in a secure facility to ensure media is only accessible to the appropriate personnel.

Backup recovery process will be tested according to a set schedule.

Network systems equipment will have fault tolerance and alternate routing plans.

Critical network and systems resources will be kept on maintenance contract with the hardware vendor. Maintenance programs must be for next business day replacement of failed components and/or spares on site. Network equipment for remote sites not covered under maintenance agreements should have spares kept on-site.