Youngstown
STATE UNIVERSITY

Information Technology Security Manual[i]

V2.2 – October, 2015[ii]

Table of Contents

Purpose:

The intent of the YSU Information Technology Security Manual (ITSM) is to strengthen and secure the computing, networking, and telecommunications environment, helping to protect all members of the YSU community from internal and external information security threats. University Guidebook policy 3356-4-09 (Acceptable Use Policy - AUP) provides the authority and basis for the Information Technology Security Manual (ITSM).

This manual expands upon the AUP and sets standards for the security and protection of the YSU Information Technology resources and (IT) infrastructure; including network and computing resources, systems, and privacy related data processed or stored on YSU systems. The ITSM supports these objectives by providing guidance and direction that will minimize the effect of the threats and vulnerabilities on information systems, and by providing the guidance needed by end users to support the Information Security program.

Scope:

The ITSM applies to all systems and users with access to YSU resources. It applies to faculty, staff, students, visitors, vendors, and any other person using any portion of the YSU IT infrastructure. The YSU IT infrastructure includes, but is not limited to: Internet connectivity, computer systems and networks, telephone systems, voicemail systems, cellular phones, pagers, fax machines, electronic mail systems, messaging systems, mobile devices, entertainment systems, wireless devices, and connected networks.

User Responsibilities:

Users have a special role in keeping sensitive information safe. This manual will help you understand your role. In summary:

1. By using any YSU systems or network component you agree to comply with the Acceptable Use Policy and the IT Security Manual.
2. You are responsible for any activity performed using your username and password. Keep it secret, keep it safe.
3. You are responsible for any activity performed on your work computer. Lock or logout your computer when not using it.
4. There is no expectation of personal privacy when using university resources.
5. Sensitive information should be guarded against theft. Restrict access to sensitive information to a limited number of key individuals and use data encryption to protect the information.
6. Increase your IT security awareness. Attend awareness sessions to brush-up on how little steps can go a long way in protecting our data and resources.
7. Areas with special requirements can request a waiver or exemption from the related IT Security Manual.

End users play a key role in the information security program of any organization. This section of the IT Security Manual outlines the responsibilities of the end user within the

YSU environment, and provides guidelines and recommendations on how to address common security concerns. These responsibilities apply to any individual that operates a system or device on the YSU network. Users are responsible for all activity associated with their YSU user accounts or personal systems while connected to YSU IT infrastructure.

User Accounts:

The University's systems make use of several different type of account roles in providing access to system resources. Rogue local accounts and passwords are prohibited from use on campus systems. The following are valid account roles and common privileges:

- End-user account – provides normal local computer and network resources
- Shared role account – provides specific privileges to local computer/services for IT System Administrators. Common examples are the local admin account and database admin account/password.
- Individualized IT Admin account – provides administrator privileges to resources (local computer, servers, domain, network, etc.) assigned to an individual IT System Administrator
- Individualized End-user Admin account – provides administrator privileges to a single local computer, and is assigned to an individual end user (typically non-IT staff).

Passwords:

In General: Passwords and secure password management are an essential aspect of any information security program. Where possible, YSU will implement technical controls to assert the quality of passwords, but these measures are not foolproof, and are not available everywhere. All YSU passwords and user IDs must be encrypted when transmitted. The following requirements outline how passwords are to be managed with respect to YSU. For the purpose of this section, a "Privileged admin account" is defined as any account with administrative responsibilities for any university system or application not including those needed for general employee supervision (i.e. access to production systems). Desktop computers would not be classified as a university system.

Password rotation is an important part of an effective password management strategy. Rotation of passwords on regular intervals ensures that compromised passwords are not usable for an indefinite period of time. However, password rotation does create additional work for the end user, and if done too frequently, encourages insecure practices such as writing down passwords in easily discovered areas.

Special passwords used for inter-system communication (e.g. service accounts and databases) do not require a standard rotation interval. However, they should be changed upon every major system upgrade or modification.

Password Composition:

Standard end-user account passwords must be set according to the following rules where

applicable on capable systems:

1. Passwords must be a minimum length of eight (8) characters.
2. Passwords must contain at least two of the following character types: lowercase letters, uppercase letters, numbers or special characters.
3. Passwords must not contain any portion of your network username, full name, address or other personally identifiable information.
4. Standard end-user account passwords will expire every 180 days
5. New passwords must differ from the previous password by at least three (3) characters.
6. Passwords may not be re-used for seven iteration of changes (i.e. PasswordXYZ expires August 2012, seven new passwords must be used before University systems allow PasswordXYZ to be re-used as the password).
7. End user account passwords must not be shared between individuals.
8. End users must not allow others to use their accounts for purposes of obtaining additional access to YSU systems and/or information. In the instance where it is discovered an end-user has granted access to a university system to a non-authorized user, both parties will be referred to the Offices of Human Resources, Student Affairs, Information Technology Services, General Counsel, and/or YSU-PD, as appropriate, for all applicable consequences and disciplinary measures.

Privileged admin account passwords must be set according to the following rules where applicable on capable systems:

1. Passwords must be a minimum length of seven (8) characters.
2. Passwords must contain at least three of the following character types: lowercase letters, uppercase letters, digits numbers or special characters.
3. Passwords must not contain any portion of your network username, full name, address or other personally identifiable information.
4. Privileged admin account passwords should expire quarterly
5. New passwords must differ from the previous password by at least three (3) characters.
6. Passwords may not be re-used for seven iteration of changes (i.e. PasswordXYZ expires August 2012, seven new passwords must be used before University systems allow PasswordXYZ to be re-used as the password). Passwords used for role accounts on systems, such as 'Administrator', are limited to those with a need to know, such as an IT Systems Administrator, and are only used when no other option is available:
    a. IT System Administrators will make use of individualized system admin accounts wherever possible to avoid the sharing of a common administrator account.
    b. IT System Administrators will maintain a separate user account for routine operations and will use the Administrator account only when the higher privileges are required.

YSU reserves the right to periodically audit passwords on any system to ensure that these standards are maintained.

Password Storage: YSU makes every effort to reduce the number of passwords that an end

user is required to use. However, there will be cases where multiple usernames and/or passwords must be used, sometimes infrequently. To avoid the support costs associated with resetting these passwords each time they are forgotten, the ITSM permits the storage of end user credentials under the following conditions:

1. At no time will an application or device store passwords for authentication. All university systems, created and/or acquired, will utilize the university directory system for authentication and storage of passwords. For applications or systems which act in a manner representing the university and cannot utilize the university directory account system, a minimum of two (2) administrative UIDs and passwords must be utilized. Consisting of one for the director of the department utilizing the service, and one for the administrator of the system/application. For the instance of social media accounts deemed "official", the same requirements would be followed with the addition of a third UID for the Director of Marketing and Communications or his/her designee. Administrators of these systems will be tracked by the Department of Human Resources and be subject to the "Separation of Employment" process for access revocation.
2. Passwords documented or written on paper must be protected from casual observation, and should be stored in a locked container or otherwise secured whenever possible.
3. Passwords stored electronically should be protected with an encryption key or passphrase that meets or exceeds the YSU password policies.

Passwords stored in configuration files for purposes of machine authentication should be limited to specific purposes and must be protected with file system access controls

Minimum Device Security Standards

The University has minimum security standards for University owned devices to accessing University technology resources. These standards include:

1. Anti-Virus[iii] - An approved, actively running, and regularly updated anti-virus application is required on all connected devices. This includes wired and wireless connections.

   This applies to University owned devices, personally owned devices, and visitor or corporate devices on campus as well as remote systems that are connected through a VPN or another remote access method.

   If no recommended anti-virus is available for a device, no anti-virus will be installed.

2. Operating System Updates - Operating Systems and applications must be set to auto update software when applicable. Systems unable to auto update should be manually updated on a regular basis (every 30 days is required).

3. Screen Locking - All end-user computers and mobile devices must lock after a specified time period of inactivity; this includes passcode locks on mobile devices.

The recommended specified time period for University devices is 15-minutes, or 5-minutes for mobile devices.

4. Passwords - All end-user computers and mobile devices must require the use of a password or passcode to authenticate access to the system. When applicable, passwords should make use of the campus directory for authentication.

5. Encryption - Encryption is required for any system requiring access to or storage of the University's sensitive information.

Network Access:

YSU reserves the right to physically or electronically disconnect any system that is attached to the YSU network for any reason without notification. Systems observed to be running malicious software or lacking effective anti- virus controls may be isolated from the rest of the network until the malicious software is removed.

Use of Computing and Network Resources:

In General: YSU provides computing and network resources to students, faculty and staff to accomplish our primary mission as an educational institution. In order to maintain an environment that supports the educational and expressive needs of our organization, YSU supports a fairly broad array of uses for the network. However, to ensure the availability of network resources for all, certain policies surrounding the use of the network have been implemented.

Implied Consent: - These policies apply to all users of YSU computing and network resources; by using these resources the user agrees to abide by the policies presented by the AUP and ITSM.

Privacy of Others: - YSU does not provide any guarantee of privacy for any activity performed on the YSU network, and reserves the exclusive right to monitor any system or network activity on YSU equipment at any time. There is no expectation of privacy when using university computing and network resources. Users may not attempt to observe, copy, or otherwise obtain access to private information or network activities of another student, faculty or staff member.

Intellectual property rights and copyright enforcement: - End users must respect intellectual property and copyright policies when utilizing YSU network and computing resources. The illegal appropriation of copyrighted or protected works is strictly prohibited. YSU network and computing resources must not be used to commit or support copyright infringement or use of improperly licensed or unlicensed software.

Systems Integrity: - YSU network and computing resources must be used in a manner that

respects the integrity of the YSU environment and any external network resources.

- Activities conducted from the YSU network for the express purpose of denying service to legitimate users of any resource is strictly prohibited.
- Any attempt to compromise the security of a system from the YSU network is strictly prohibited.
- Individuals responsible for systems, projects or activities which legitimately rely upon heavy utilization of resources, on or off the YSU network, should notify the owner of those resources whenever possible.

Unsolicited Communications: - YSU network and computing resources must not be used for the purpose of unsolicited communications on any medium, including but not limited to: email, instant messaging, fax, and voice communications. Furthermore, reasonable effort should be exercised to ensure that any internal communication resources are not misused for these purposes.

YSU reserves the right to interrupt or limit connectivity to any resource suspected of violating this standard without prior notification.

In addition to being in violation of the AUP and ITSM, legislation has been enacted to regulate the terms by which unsolicited email may be legally sent to individuals.

There are two laws that govern unsolicited commercial email in the State of Ohio. The CAN SPAM Act of 2003, a Federal law, has four main provisions:

a) Email recipients must have an opt-out method. Unsolicited messages must include an option for the recipient to opt-out of future mailings from the sender. The opt-out method must be Internet accessible, and must take effect within 10 business days. The method may provide users with the option to only opt-out of certain mailings, but it must include an option to opt- out of all future mailings.

b) The message must notify the recipient that it is an advertisement, and a valid physical address suitable for mailing must be included.

c) Emails must not contain false or misleading header information Header information, such as the 'From:' and 'To:' fields, must accurately reflect the identity of the sender and the recipient.

d) Deceptive message subjects are prohibited. The message subject must not be deceptive with respect to the content of the message.

In addition to the CAN SPAM Act of 2003, there are several provisions in the Ohio Revised Code, enacted in 2002, that in most cases mirror the provisions of the CAN SPAM Act. In 2005, a revision to the Ohio Revised Code was implemented to make it a felony offense to forge or otherwise falsify the point of origin or routing information in an unsolicited commercial email.

Harassment: - The use or involvement of YSU computing or network resources to harass or threaten any individual or organization, regardless of their affiliation with YSU, is strictly prohibited.

Hacking Programs or Activity: - The unauthorized use of 'hacking' programs or activity,

such as port scanning or password guessing, is strictly prohibited. Legitimate use of these programs for educational purposes must be communicated to the Tech Desk at least two days in advance. The use of these tools also requires coordination with the IT staff so that a contained environment can be created. Limiting the scope of these tools will minimize the risk of impacting YSU infrastructure resources.

Illegal Activities: - YSU strictly prohibits any use of computing or network resources for the conduct of illegal activities. YSU reserves the right to report any identified illegal activity to the proper authorities, and reserves the right to comply with law enforcement or court orders for information related to the activity.

Authentication Requirement: - Access to the YSU network requires authentication with a valid YSU username and password. Users must not attempt to bypass or otherwise disable network authentication.

Security Awareness: - All end users of YSU IT resources have the responsibility to participate in security awareness initiatives provided by YSU. While many aspects of YSU security can be controlled and enforced with technology, YSU still depends heavily on the end user to help maintain a secure environment. Studies show that the majority of successful intrusions are either initiated by an internal user or aided by information gained from an internal user. Besides being aware of the methods used by attackers to "social engineer" the end user, being aware of the ITS Security Manual and knowing how to interact with the security group when necessary is essential.

YSU will provide an ongoing security awareness program to keep end users aware of the latest security threats and changes to security policies. Minimally, all new and existing users will be provided with a brief training on the the AUP and ITSM to acknowledge indicating their understanding and acceptance of the AUP and ITSM. YSU will provide security alerts, ITSM updates, and security news/tips in an ongoing basis.

Telephone, Fax, Instant Messaging, and Email Guidelines

Telephone Security - Receiving a Telephone Call:

- Individuals seeking to gain privileged or sensitive information will often call and masquerade as an employee or help desk staff. All employees should exercise caution when providing any information over the phone.
- If there is any doubt of the caller's identity or need to know, arrange to call them back on a known number or refer them to your supervisor.
- Verify the caller's need to know and authorization, and verify that the return telephone number is that of the identified person.
- Remember that you should never disclose a password or privileged account information to anyone over the telephone.
- Do not be intimidated by demands for information, by the title of the caller, or by threats if you do not give the person the information requested.
- Notify your supervisor or the Tech Desk of any suspicious activity. Making a Telephone Call:

- Ensure you are talking to the right person
- Keep in mind that others may overhear your conversation.
- Ask who is present if the recipient is using a speakerphone.
- If using cordless, mobile, or cellular telephones take caution while discussing sensitive and confidential subjects as you are, in reality, using radio communications.

Fax Security: -
Faxing sensitive documents must be done carefully to avoid unauthorized disclosure of information:

- Fax messages with sensitive content should have any unnecessary portions rendered unreadable if possible.
- Only authorized persons should be involved with the transmission and reception of sensitive information.
- Do not send a sensitive fax without first verifying that the number is correct and that the recipient is available to secure the document as it is received.
- All copies of sensitive fax messages should immediately be removed from the fax machine and given appropriate protection to prevent unauthorized disclosure.

Instant Messaging and Email Security: -
Social engineering is a primary form of attack for Email and IM communications; where legitimate users are tricked into releasing sensitive or useful information to the attacker.

In addition to this context, there are a number of other means by which social engineering attacks are conducted. Consider the following tips:

- Be suspicious when anyone unknown to you seeks information of a technical or sensitive nature, such as a username, password or network address.
- Never click on a hyperlink embedded within an e-mail or Instant Message (IM), as the URL may appear to go to a trusted host but actually link to a malicious site. If you must follow the link, always copy and paste the text into your browser address bar.
- If you receive a notification that there is a problem with your account at a bank, auction site, payment site or other important location, confirm the notice with the site via phone. Never provide sensitive account information, such as username and password, to the sites linked from these messages.
- Do not exchange files with others using IM software, as these transfer requests can bypass firewalls and contain malicious software. IM attacks have also imitated a known IM user and resulted in the installation of "Trojan" software which opened up all files on the victim's system.
- Never divulge sensitive personal information in an IM conversation or e-mail.
- Never open an attachment unless you are expecting it and you trust the source. Remember that faking the "From:" address in an e-mail message is very simple and is performed in a majority of these types of messages.
- Be especially aware of malicious software and phishing attacks:

    - In the malicious software attack, malicious code is sent to the end user and they are tricked into executing it.
    - In the phishing (pronounced "fishing") attack, emails are sent posing as

legitimate services, requesting the user log in to perform some function. By clicking on links in the phishing email, users are directed to sites that look legitimate, but collect sensitive information from the user.

Privacy & Sensitive Information:

In General: - It is YSU policy not to ask for the following over the phone for any information technology related issue:

- Passwords or PINs for any account (email, voicemail, network)
- Social Security Number
- Credit Card or Bank Account Numbers

If, due to some highly unusual circumstance, YSU Tech Desk personnel do require the above information, be sure to authenticate the Tech Desk personnel requesting the information. The most straightforward method of doing this is by getting the caller's name, then call the Tech Desk directly and request to speak with the same person or the Tech Desk supervisor.

Disclosure of Personal Information: - YSU must comply with all applicable state and federal regulations related to the maintenance and disclosure of personal information. Any residual authority to share personal information without the explicit approval of the individual will be carefully managed, and information will only be disclosed on an as-needed basis.

System Monitoring and Logging: - These capabilities are maintained solely to monitor and enforce the ITSM, to meet regulatory requirements, and audit requirements, thereby promoting the safety of all end user data. YSU periodically monitors computer and network use to ensure compliance with the ITSM and provide safeguards for YSU network users. YSU has automated and manual processes to ensure ITSM compliance; including audit logs of Internet access, intrusion detection systems, network access controls, security firewall logs, network traffic capture, system access logs, e-mail archives, and others.

Data Retention: - YSU will retain personal information related to students, faculty and staff for as long as necessary to support administrative, operational or regulatory requirements. See the University's Record Retention schedule for more information (www.ysu.edu/recordsmgt).

Sensitive Information Handling and Encryption: - Sensitive information comes in many forms, from passwords and configuration files to Social Security Numbers, date of birth of students and employees, and medical information. Consult the University Guidebook Policy 3356-4-13 on Sensitive Information for more information. Everyone that has access to sensitive information has a responsibility to secure it. Improper handling of sensitive information exposes it to compromise.

Secure Email: - YSU provides the campus community with the ability to send encrypted email content to off-campus users.

Secure Document Exchange: - YSU provides the campus community with the ability to exchange documents via an SSL transfer protocol. For instructions, contact the Data Security Supervisor.

Guarding information on user systems: - The following standards for handling sensitive information on user systems must be followed at all times

- Users must lock their screen when leaving system unattended.
- Users must follow all policies related to end user responsibility for personal systems.
- Sensitive information pertaining to YSU must not be copied to systems or networks outside the scope of the ITSM without prior approval.
- Sensitive information must not be transmitted over the Internet without encryption.
- Removable media, including laptop computers, that contains sensitive information should be stored in a locked cabinet or safe when not being used.
- Sensitive information should only be stored on YSU managed systems.
- Sensitive information stored on end-user computers or removable media must be encrypted.

Protecting paper-based information: - Paper is often overlooked as a source of sensitive information. The following policies are designed to help ensure that improper handling does not lead to unauthorized information disclosure.

- Sensitive information on paper should be stored in a secured location.
- When printing sensitive information, immediately remove it from the printer to avoid having it taken by parties unauthorized to see the information.
- When faxing sensitive information, notify recipient of the incoming fax prior to sending and confirm receipt after the transmission completes. Faxes that do not complete due to busy or other temporary issue should be cancelled to ensure that the transmission occurs under controlled circumstances.
- Sensitive papers must be shredded when no longer needed, but in conformity with the University's record retention schedule.

File transmission security: - Files transmitted over the YSU network are not guaranteed protection from disclosure. If files contain sensitive information, the file transfer protocol must require authentication of the client, and should employ the use of encryption to protect information while it is in transit.

Regulatory Compliance:

State of Ohio: - The State of Ohio's Office of Information Technology sets statewide IT Policy requirements. The state IT policies are applicable to every organized body, office, or agency established by the laws of the state. Its scope includes state computer and telecommunications systems and the employees, contractors, temporary personnel and other agents of the state who use and/or administer such systems.

State of Ohio Compliance - The overriding purpose of state IT policies is to protect system

assets, comply with legal requirements, promote public trust, ensure continuity of services, and recognize risks and threats.

FERPA: - The Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the privacy of student education records. The law gives students specific rights concerning their education records, including the right to access records kept by the school, the right to demand that education records are disclosed only with the student's consent, and the right to amend education records. Students have a right to expect that information in their education records will be kept confidential unless they give permission to the school to disclose such information. The University Office of the Registrar is responsible for FERPA compliance.

- Protected Information - Information is divided into two categories for the purposes of FERPA; directory information and non-directory information.

- Directory Information - Directory information includes items such as the student's name, address, telephone number and dates of attendance. For a complete list of directory information please consult University Policy 8004.01, the Student Right to Know newspaper, and/or the University Undergraduate Bulletin. YSU may disclose directory information to the public unless the student formally requests that it remain confidential. Students may go to the Registrar's Office and complete a Student Privacy Hold Form to have directory information withheld from the public.

- Non-Directory Information - Non-directory information is any education record that is not considered directory information. Examples of this information include Social Security numbers, race and ethnicity, gender and grade reports or transcripts. In general, non-directory information will not be disclosed without express written consent of the student. However, FERPA does provide an allowance for disclosure to certain organizations or under certain circumstances, such as the following:

    - School officials with legitimate educational interest
    - Other schools to which a student is transferring
    - Appropriate parties in connection with financial aid to a student
    - Organizations conducting certain studies for or on behalf of the school
    - To comply with a judicial order or lawfully issued subpoena

FERPA Compliance - YSU fully supports FERPA and complies with its standards for privacy. Regarding directory information, YSU informs all students of the nature of directory information that will be disclosed to the general public, and provides an option to 'opt out' of this directory publication. For non-directory information, such as grades and financial information, YSU has implemented safeguards to protect the information and ensure that it is only released to individuals that are authorized to access the information. For more information on FERPA compliance and Student Rights, please consult University Policy 8004.01, the Student Right to Know newspaper and/or the University Undergraduate Bulletin.

GLBA: - The Gramm-Leach-Bliley Act (GLBA) established that financial institutions have

an affirmative and continuing obligation to respect the privacy of their customers and a duty to safeguard the security and confidentiality of their customers' nonpublic personal information. The Federal Trade Commission (FTC) determined that higher education institutions are financial institutions subject to the GLBA. The Office of Financial Aid is responsible for GLBA compliance.

All nonpublic personal information is protected under the GLBA. This information includes social security numbers, account balances, and any other personally identifiable financial information that is not publicly available.

GLBA Compliance - There are two areas of compliance regarding GLBA. The privacy rules are similar to the privacy requirements of FERPA. YSU maintains compliance with both privacy standards. The other area of GLBA compliance is our Information Security program. YSU maintains a comprehensive security program as defined in GLBA to identify risks and protect private information from unauthorized disclosure.

HIPAA: - The Health Insurance Portability and Accountability Act (HIPAA) protects the privacy and security of health information. Protected Health Information (PHI) must not be disclosed without written authorization and must be safeguarded to prevent unauthorized disclosure.

HIPAA regulations apply wherever PHI is used or stored. The areas of YSU that handle medical information for staff, faculty, students, or patients are subject to HIPAA regulations. The locations identified on campus possibly with access to this information are: the Dental Hygienist program, student health clinic, and Human Resources medical benefits.

HIPAA Compliance - YSU uses standard administrative, physical and technical safeguards to protect electronic PHI from unauthorized access, alteration, deletion and transmission. Access to PHI is limited to individuals that require access to perform their assigned functions.

PCI-DSS: - The Payment Card Industry Data Security Standard (PCI-DSS) protects the privacy and security of credit card holder information. The Offices of Student Accounts and Financial Services are responsible for PCI compliance.

PCI regulations apply wherever credit card transactions occur: in person, by telephone, or electronic (online). The areas of YSU that handle card holder information must enforce compliance through business unit practices. The locations identified on campus conducting electronic credit card transactions: Athletic Ticket Office, Bookstore, Food Services, Student Accounts (Bursar Office).

PCI Compliance - YSU requires electronic transactions conducted on-site to be segmented away from other campus systems. Web-based transactions must be encrypted.

Red Flags: - The Red Flags Rule under sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003. The regulation is intended to reduce the risk of identity theft by requiring stronger fraud prevention to protect consumers' personal data. The Offices of Student Accounts, Financial Aid, and General Accounting are responsible for Red Flags compliance.

Visitor Network Access Process & Procedures:

As users of YSU technology resources, all visitors are subject to ITSM policies.

Visitors Requiring Wireless Internet Access: - AT&T - AT&T provides wireless Internet access for use by visitors, students, faculty, and staff. The AT&T network is a separate network from YSU. End-users are bound by AT&T rules and policies while using the service. Information on obtaining credentials for visitors is available.

Visitors Requiring YSU Network Access (wireless or wired):

- Acknowledgement of the Acceptable Use Policy - Visitors using the YSU network implicitly agree to the Acceptable Use Policy (Guidebook Policy 4009.01) by their use of the network.

- Obtaining Credentials - Department sponsorship must be obtained for a visitor requiring access to the YSU network. The YSU sponsor should initiate the request for a network access account for each visiting user. Network access accounts can be created within three business days. The YSU sponsor is responsible for notifying the YSU IT staff through Computer Services when the access is no longer required and may be disabled. Visitor accounts will be provisioned to expire in seven days unless otherwise requested on the Non-patron Account Request form.

- Access restrictions - Visiting users will not be granted access to any network segment containing sensitive/protected data without appropriate justification.

Mobile Computing/Mobile Data Storage:

- Sensitive Information stored on end-user computing and mobile storage devices must be encrypted[iv].

Mobile computing involves information storage or remote access to the YSU technology resources on mobile devices or off-site locations, such as a home or hotel. Without the benefit of physical security, the mobile computing platform is exposed to significant threats, including physical theft, insecure or hostile network access, and misuse by persons not affiliated with YSU. The primary mobile computing solutions in practice at YSU include: VPN over the Internet and secure campus wireless. The minimum security standards for University-issued devices and Non-University devices are specified above.

IT staff provisioning University issued mobile devices (laptops, tablets, smartphones, etc.) will ensure the devices are configured with the minimum University security standards when applicable (anti-virus, screen locking/passwords, updated OS, and when needed encryption for sensitive information) when deploying to a client. Non-University devices should have the same minimum security standard implemented to access YSU technology resources. IT

staff will configure non-University devices with the minimum security standard when they are asked to service such devices for access to YSU technology resources. The Tech Desk self-help documents will state the minimum security standards as part of the process for configuring YSU technology resource access.

Mobile Data Drive Encryption: - Personal laptop and mobile devices (smartphones, tablets, etc.), including other mobile storage devices such as USB drives, must use an active form of encryption to prevent loss of sensitive information. University laptops that store YSU sensitive information must employ approved forms of drive encryption software and theft recovery software. Please contact the Tech Desk for current solutions..

Wireless Networking: -

Wireless LAN (Wi-Fi) networking is the predominant means by which network access is extended to laptops and other mobile computing devices. YSU has implemented wireless networking technologies to provide students, faculty, staff with access to the YSU network. This improves the flexibility of our campus facilities and supports more pervasive integration of information technology into the educational environment. YSU has implemented several policies regarding wireless use.

1. Wireless Access Control: - Because wireless networking technologies are generally immune to physical security measures, it is important to ensure that access to the wireless network is well managed and secure. YSU has implemented technologies to provide access control and encryption to maintain a level of security in this portion of our network.

2. Authentication Requirement: - Access to the YSU wireless network requires authentication with a valid YSU username and password. Users must not attempt to bypass or otherwise disable network authentication.

3. Wireless Security Protocols: - The use of inferior or ineffective wireless security protocols or solutions presents a risk to the organization. YSU has standardized on the Wireless Protected Access (WPA)-2 Enterprise protocol for securing wireless networking technologies. All access to the YSU network over wireless LAN technologies must be protected with WPA-2 Enterprise.

Prohibition on personal wireless access points: - As stated in the Acceptable Use Policy, wireless access to the YSU campus network must be provided by YSU infrastructure devices. Personal wireless access points must not be attached to the YSU network. Unauthorized access points detected on the network may be confiscated and will be physically or electronically isolated from the rest of the YSU network.

Theft Recovery Software: - University laptop computers are required to actively run the university's laptop theft recovery software. The software enables YSU to recover lost and stolen laptops and mitigate the loss of sensitive information. The procurement process for new university laptops includes a process for ordering the theft recovery software. In addition, the software can be obtained by contacting the Tech Desk.

VPN: - YSU provides Virtual Private Network (VPN) remote access to students, faculty and staff that desire access to protected campus resources from remote locations. Access to the VPN requires a client utility, which may be obtained from the YSU Tech Desk, and a valid YSU username and password.

While operating the VPN, the workstation in use is be considered an extension of the YSU network, and all YSU security and acceptable use policies apply.

Further:

- VPN access must not be shared with users that are not affiliated with YSU.
- VPN clients must not bridge, proxy or otherwise expose the YSU network to other systems at any time. If multiple systems require VPN access, a VPN client must be installed on each system.
- Users must not attempt to use unauthorized or otherwise unsupported VPN clients with the YSU network as they may impair the operation of the VPN gear or compromise the VPN client access policies in place.

Non-University Computers and Devices:

Personally owned equipment is authorized for use on the wireless YSU network under the following conditions. Non-University devices should have the same minimum security standard implemented to access YSU technology resources (See Section 8 – Mobile Computing). IT staff will configure non-University devices with the minimum security standard when they are asked to service such devices for access to YSU technology resources. The Tech Desk self-help documents will state the minimum security standards as part of the process for configuring YSU technology resource access.

Minimum Security Standard for Non-University devices: - All personally owned equipment must be configured according to the YSU security standard for the platform in question. These security standards can be obtained from the Tech Desk: http://techdesk.ysu.edu. If a standard is not available, the platform should be configured according to generally accepted best practices for security.

Anti-virus: - All systems attached to the YSU network must be protected by YSU approved anti-virus software, and must be regularly updated to ensure effectiveness. YSU provides anti-virus software free of charge to students, faculty, and staff. This software can be obtained through the Tech Desk: http://techdesk.ysu.edu/downloads.htm.

Security Updates: - Personally owned systems must comply with YSU policies for maintaining security updates. This includes the use of automated update mechanisms whenever possible, and regular manually applied updates in circumstances where the platform does not support automated updates.

Screen Locking: - All personal systems should be configured to automatically lock the screen when the system is not in use, this includes passcode locking on mobile devices. All end users must ensure that the screen is locked while the system is unattended to avoid

misuse and disclosure of sensitive information. Contact the Tech Desk if assistance is needed with this system feature.

Password Controls: - All YSU password policies apply to personal systems attached to YSU network resources, as well as those owned and operated by YSU. If the personal system supports configuration of password controls, the YSU password policy should be implemented in that control, and the control enabled. In circumstances where the operating system does not have the capability of directly enforcing these policies, the end user is responsible for manually ensuring compliance with YSU password policies.

Encryption: - All personal computing and mobile storage computing devices must follow policies for sensitive information handling. See section 5.5 for more information.

Technical Support:

The Tech Desk provides first level Information Technology support via phone or in person on the 4th floor of the Maag Library.

The YSU Tech Desk can be reached at 330-941-1595, or via Email: techdesk@ysu.edu.

The Tech Desk on-line help web page provides hours of operation, and access to many helpful resources, including instructions for getting connected to the YSU networks.

Links to security updates and Anti-Virus downloads.

Public Facing Web Sites:

Background

In order to meet the growing need for individuals, departments, and organizations to develop and maintain their own public facing **web servers** and yet maintain the security required for the YSU network and the main YSU web server, ITS has deployed a system called cPanel.

A key aspect of cPanel is built-in protection from cross-site malware infections.

In the past, the main YSU server was host to web sites maintained by individuals, departments and organizations. Due to repeated security breaches of the main YSU web server, starting in the summer of 2015 all personal and group web sites are being moved to the cPanel-based group services system. Groups and individuals will be advised prior to their site being moved. URL and access credentials should remain the same.

Going Forward:
Web sites for individuals will be required to use **"People" or "people.ysu.edu"**.

Web sites for departments, groups, organizations, or individuals needing DNS services will be required to use **"Groupweb".** An exception can be made for a departmental web site on the main web server if the site is in Drupal and the maintainers do not have FTP/SFTP access to the serever.

To request services for yourself or your organization, please use the Tech Desk self-service request form, or contact the Tech Desk.

Cloud Hosted Systems:

Systems hosted in the cloud are not exempt from security and reliability concerns. The American Institute of Certified Public Accountants (AICPA) has established audit standards for cloud systems called Service Organization Controls Reports. YSU requires:

- A SOC3 report for all hosted systems

- A SOC2 report
    - For all hosted systems that contain Sensitive Information as defined in University Guidebook Policy 3356-4-13
    - For all hosted systems that contain confidential research or proprietary research
    - When a SOC2 is required, the SOC3 is not needed.

Information Security Controls:

YSU has implemented technical information security controls to support our policies and protect the information and assets of YSU and its students, faculty and staff.

Anti-Virus Filtering: - YSU has implemented an email filtering product that provides virus and malicious code protection for the students, faculty and staff of YSU. This gateway scans all messages that pass through the primary YSU email infrastructure. In cases where malicious software is discovered, the recipient is notified, and the malicious code is blocked. This may result in attachments being removed or quarantined by the gateway for further inspection.

To ensure this gateway achieves the desired effect, YSU has implemented the following policies:

- All email messages sent to and from the YSU network must pass through the Anti-virus filter.
- Attempts to bypass the gateway are prohibited, and YSU reserves the right to block any SMTP traffic that circumvents this control.
- While YSU strives to maximize availability, email is not to be considered a reliable delivery method. YSU assumes no responsibility for delay or loss of information due to this scanning activity.

Anti-Spam Filter: - Unsolicited commercial email, commonly described as “spam”, presents

a significant challenge for many organizations. While many of these messages are simple annoyances, some are used to perpetrate scams or spread malicious software.

To protect the YSU user community from spam-related nuisances and threats, all inbound email to standard YSU email accounts will be processed by anti-spam filtering technology. This technology will reduce the amount of spam that is received by end users, and will reduce the impact on the YSU email infrastructure from processing and storing unwanted spam messages.

To assist with the effort to reduce spam, YSU encourages students, faculty and staff to follow these recommendations:

- Avoid publishing your YSU email address, in its entirety, to Internet accessible web sites. Avoid mailing lists with archives that do not block or obscure email addresses.
- When supplying your YSU email address to Internet services for registration or any other purpose, always examine the form closely and opt-out of any unwanted email communication.
- It is against YSU Policy to send or otherwise support the sending of spam from the YSU network. Messages sent from YSU that are determined to be spam may be deleted without warning.
- YSU email accounts sending spam may be suspended without notice.
- YSU assumes no liability for information lost or delayed through this process.

Malware Filtering – Today, one of the most frequent means of getting past security measures is to insert a program (malware) into a web page. When a user view the web page the program is launched and infects the users system.

YSU defends against this form of attack by actively filtering all off campus web pages viewed on campus.

Authentication Controls: - Authentication is one of the pillars of an effective information security program, and plays an essential role in the security of YSU systems and infrastructure. Poorly implemented authentication strategies can undermine the security of an organization by allowing users to violate password policies, expose credentials, or maintain access to systems long after the rationale for it has passed.

To avoid this, YSU has implemented the following policies for authentication controls:

- All access to sensitive information must be protected by some form of authentication.
- Any new systems or applications implemented within YSU should use the YSU Directory of Accounts for authentication.
- Any new authentication service implemented within YSU should support all existing user account standards and password policies.
- Any new authentication service should support integration with existing services to promote effective identity management practices.

Enterprise anti-virus management: - Anti-virus solutions have been implemented by YSU to prevent infection by viruses and other malicious software. The anti-virus solution provides a reporting facility to provide metrics for the source of malicious code and percentage of deployment for signature and scanning engine updates. In addition:

- Anti-virus controls are a critical asset in the information security program, and must not be disabled or otherwise limited on any YSU managed system.
- Personally owned systems must utilize YSU approved anti-virus solutions to protect the integrity of the system and limit the impact of a virus outbreak.

Firewalls: - A firewall is a network device that provides filtering and security services for network traffic. The primary objective of the firewall is to limit access to the YSU network from external locations, including the Internet. The secondary objective is to ensure that the YSU internal network is effectively partitioned to ensure that administrative control is maintained at all times, and that high value systems may be protected from attacks and malicious traffic that originate from the YSU network.

To maintain the effectiveness of the firewalls implemented at YSU, the following policies have been implemented:

- Firewall rules are enabled to enforce policies regarding network use. Actively evading firewall policies through the use of tunneling or proxying is prohibited.
- YSU reserves the right to block or redirect any traffic that passes through the YSU network, and assumes no liability for losses due to network traffic filtered by a firewall or other device.
- Host-based firewalls are an effective means of preventing system compromise from network-based attacks. Users are encouraged to install YSU approved firewall software on personally owned systems to improve security.
- Host-based firewall software installed on YSU owned or operated equipment must not be disabled or modified without prior authorization.

Internet Traffic Shaping: - In order to protect essential network services and maintain acceptable performance levels for administrative and academic purposes, YSU has deployed a bandwidth management solution. This solution is currently configured to limit certain non-essential applications, such as peer to peer file sharing. Owners of high priority systems should contact the Tech Desk to request special bandwidth classification.

Intrusion Detection: - YSU has implemented Intrusion Detection System (IDS) services throughout the network. These systems are designed to detect activity that may indicate an attack and notify YSU personnel or actively respond in some manner. The IDS capability is primarily geared towards protecting the environment from external threats, but is deployed internally to ensure that anomalous traffic and attacks originating from the YSU network are detected as well. To maintain the effectiveness of our Intrusion Detection software, the following policies have been implemented:

- IDS operates by actively monitoring and analyzing network traffic. This monitoring does not discriminate between private and public information, and could cause private information to be logged or otherwise documented if it is considered suspicious.

- Using encryption or obfuscation techniques for the sole purpose of evading IDS monitoring is prohibited.
- IDS detection of malicious activity may cause specific systems or network traffic to be blocked or disconnected from the YSU campus network. YSU assumes no liability for any impact from this activity.

Login Banners: - All systems that support interactive access must include the following login banner:

> *"Unauthorized use of Youngstown State University computer and networking resources is prohibited. Any use of this system acknowledges your awareness of, and agreement with, the Youngstown State University Acceptable Use Policy. Any violators of this policy will be subject to disciplinary action, which may include prosecution."*

Network Access Control: - YSU provides network services to a wide array of personally owned systems that are not under the administrative control of YSU Information Technology Services. Because these systems may contain viruses or be running Trojan horse applications, they present a threat to the network. To minimize this threat, YSU has implemented Network Access Control (NAC) on remote access networks, such as the residence hall network, VPN, and the wireless network. This technology provides a measure of control over what systems are admitted to the network, and provide essential access to systems that need to be attended to before they are provided full access.

In support of this implementation, YSU has implemented the following policies:

- Any attempt to bypass or support the bypass of Network Access Control (NAC) is prohibited.
- Systems that have had network access disabled through Network Access Control should be attended to as soon as possible to avoid file damage and/or information loss.

Network Segmentation Controls: - The YSU network has been designed to provide a scalable and robust environment to support the administrative needs of the organization without undue restrictions on the student body. This capability is maintained through network segmentation that has been engineered into the YSU network. This segmentation provides for areas of containment that allow diverse security policies to be applied with minimum side effects.

To maintain this effectiveness, the segmentation is enforced with technical controls and supported by the following policies:

- Any attempt to circumvent YSU network segmentation controls is prohibited.
- Implementation of any network bridging between segments, including the use of wired, wireless or tunneled connections, is prohibited.

Security Monitoring Tools: - YSU has implemented monitoring tools to maintain awareness of any events or problems that occur within the environment. In addition to monitoring systems for performance and availability, YSU monitors systems for security-related events.

Critical events may cause a notification to be sent, while informational events may be archived to support any future investigations.

Wireless Security: - The YSU wireless network infrastructure provides a valuable resource to students, faculty, staff and guests alike. To protect this network, YSU has implemented several wireless network security controls. Principal among these controls is the use of Wireless Protected Access (WPA) to authenticate and encrypt legitimate wireless network traffic. WPA is supported by many wireless clients and provides an adequate level of security for this application.

To ensure that the YSU network is not abused by attackers through wireless network connectivity, the following policies have been implemented:

- Wireless access point devices, or hosts acting in the role of a wireless access point must not be attached to the YSU network without authorization.
- Wireless access points or other wireless devices that mimic or clone YSU network profile information, such as SSID or WPA requirement, are strictly prohibited.
- Workstations that are attached via wired communications should disable any wireless radios while they are connected.
- Users of the YSU wireless network should be careful to ensure that they are connecting to the proper YSU wireless network every time.

Vulnerability Scanners: - YSU will periodically conduct network vulnerability tests to ensure protection of key systems from known vulnerabilities. These tests will combine the use of multiple network assessment techniques, including port scans and vulnerability scans. These scans will attempt to connect with systems attached to the YSU network and determine what services are available. If services are discovered, the vulnerability scan will attempt to determine if the service has any known vulnerabilities. Only authorized IT personnel are allowed to perform vulnerability scans.

YSU Directory of Accounts: - Maintaining a centralized directory is essential in environments where there is a high degree of user account turnover. Without a centralized directory service, account passwords would quickly become desynchronized, password quality would not be managed, and accounts will tend to remain active for much longer than required. To avoid these issues, YSU maintains a centralized directory of all user account information. This directory is to be considered the authoritative source for current YSU account credentials and status. To support this role, any new applications that are brought into the YSU environment must leverage the account information in the YSU Directory of Accounts, either directly as a client, or through an automated synchronization process.

Technical Security Standards: - Consistency is one of the essential characteristics of an effective information security program. Security standards are implemented to support consistency by providing a standard set of procedures and configuration elements that should be consistently applied to the subject platform across the environment.

Security standards are generally focused on eliminating the most common security issues for a given platform, and are not designed to be extensive ‘hardening’ guides. For more information on security standards for YSU systems, contact the Tech Desk.

Technical Management Controls:

Periodic Security Assessments: - YSU will conduct security assessments periodically in order to validate YSU risk mitigation efforts and discover vulnerabilities introduced over time due to software and hardware changes, network equipment modifications, and new methods of security exploitation.

Internal server discovery and remediation: - The security of the internal network requires that all servers be properly secured against malicious use. All servers on the YSU network are required to conform to YSU security standards, and must be identified to the IT staff so they can be included in the vulnerability management process. YSU will use automated tools to scan the network frequently for unidentified servers and will disable network connectivity for these servers until security validation is accomplished. It is the responsibility of each system owner to notify IT of the intent to deploy a new server, which will allow IT to properly validate system security before new risk is introduced to the network. Systems requiring inbound access from the Internet require approval and the associated application for Public Access Server on file. Applications for Public Access Servers may be requested through the Tech Desk.

Physical and Environmental Security: - While physical security in the University setting is fairly open to accommodate the student population, sensitive data, network servers, and network devices must be located in a secure environment in order to protect privacy and ensure the integrity of the IT infrastructure. YSU maintains a datacenter with the appropriate security and environmental controls, and it is YSU Policy that all critical processing devices, servers, core network equipment, and network security devices will be physically located in the Data Center. In addition to physical access controls, the data center also has backup power and a controlled climate to help maintain high availability for YSU end users.

Servers not residing in the datacenter must have an approved exception or waiver to the ITSM, and must adhere to YSU physical security standards:

- Physical access to information processing and storage areas and their supporting infrastructure (communications, power, and environmental) must be controlled to prevent, detect, and minimize the effects of unauthorized or unintended access to these areas
- Physical access controls must be in place for the following:

    - Data Centers, including the Computer Center
    - Areas containing servers and associated media
    - Networking cabinets and wiring closets
    - Power and emergency backup equipment
    - Operations and control areas

Security Violations: Reporting, and Disciplinary Measures

The YSU Information Technology Security Manual will be supported by standards, procedures, and awareness programs, as necessary. Compliance with Information Security Policies, Standards and Procedures is mandatory.

AUP or ITSM violations will be subject to disciplinary action commensurate with seriousness of the offense:

- End user systems and departmental servers will have their network access terminated immediately for serious violations of either the AUP or ITSM. This will ensure that the offending system is properly isolated, allowing the security issue to be corrected before other systems are affected.
- Appropriate disciplinary measures for AUP or ITSM violations will be determined by the Offices of Human Resources, Student Affairs, Information Technology Services, General Counsel, and YSU-PD, as deemed necessary.

Reporting a Security Incident: - The Tech Desk should be notified immediately of all security incidents. The Tech Desk can be reached by calling 330-941-1595 or via email by submitting the issue and all details to techdesk@ysu.edu. Incidents of an urgent nature must be submitted directly to the Tech Desk via voice communication.

- Recognizing a Security Incident: - Security incidents can be very obvious, such as a widespread virus outbreak or network denial of service attack, or very subtle, such as end user workstations suddenly running very slow with highly active disk drives. Since any security event has the potential to negatively impact the University, it is imperative that all YSU network users understand how to recognize and report potential security incidents. While some incidents are not time critical, others represent a serious exposure that increases with time, and therefore needs to be remedied quickly.

- What classifies as a reportable incident: - For the purposes of the ITSM, a security incident is any perceived or actual event relating to Information Technology that has the potential to:

    - Cause an exposure to personal privacy information
    - Create an unfavorable public impression of YSU if released to the media
    - Cause YSU to be in violation of any law or government regulation
    - Disrupt computer operations or network availability
    - Cause significant manpower expenditure to resolve

    Some examples of security incidents that would be subject to this plan include:

    - Successful Internet-based attack of any sort, including web page defacements, denial of service attacks, unauthorized data harvesting, and others.
    - Evidence that internal information systems have been breached by unauthorized personnel with potential exposure of sensitive data.
    - Evidence that systematic efforts are underway to gain unauthorized

access to any information system.
- Malicious code (virus, worm, Trojan) activity with the potential to quickly spread to multiple systems.

- What information is needed: - When submitting a security incident, complete information is needed in order for the IT staff to respond quickly if necessary. At a minimum, the information should contain the following:

    - Name and office of the person with knowledge of the incident
    - Primary and alternate phone number if additional information is needed
    - Description of the incident, including potential damage if known
    - Type of system or network the incident occurred on
    - Any steps already taken to reduce the impact of the incident (system turned off, etc.)

- Tech Desk Incident Response Procedure: -The objective of this procedure is to outline the escalation process for security incidents that effect a University owned PC(s). Anytime a security incident has been identified or is suspected, the YSU Network Security team should be notified based on the contact list below.

- Definition of a security incident:
    - End-user/System Administrator reports an unauthorized activity that results in the disruption of a University- owned system(s), such as the following:
    - Unauthorized access/change to YSU information or data
    - Active malicious software that effects multiple PCs i.e. a worm that is spreading malicious code to other YSU systems
    - Existence of a Key logger on one or more YSU PCs
    - Denial of Service attack
    - Possible compromise of sensitive information (including credit card numbers or social security numbers)
    - Website defacement
    - Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent
    - The unauthorized use of a system for the processing or storage of data
    - IP Spoofing
    - Commercial use of YSU IT resources.
    - Social engineering activity - Unknown people asking for information which could gain them access to YSU's data (i.e. a password or other details).
    - Unauthorized disclosure of sensitive or confidential information electronically, in paper form or verbally
    - Connecting unauthorized third party equipment to the organization's network
    - Giving sensitive or confidential information to someone who should not have access to it - verbally, in writing, or electronically

The Security Incident Response Procedure

When a security incident is suspected, staff should immediately follow the Security Incident Response Procedure.

Security Program - Key Roles and Responsibilities

Chief Technology Officer:

- Overall responsibility for the Information Security program
- Approval and Oversight of Information Technology Security Manual
- Provides guidance, direction, and authority for the YSU Information Security Program
- Coordinates ITSM and compliance issues with department heads and the Board of Trustees as necessary

Information Security Officer:

- Directs the YSU security program to ensure YSU information is properly protected
- Directs internal and external security assessments
- Develops and distributes:
  - security standards
  - The Security Incident Response Procedure
- Directs the implementation of new security architectures and controls
- Directs the YSU security awareness program
- Enforces ITSM compliance through automated and manual controls
- Reviews requests for ITSM exceptions and controls
- Manages the YSU vulnerability management program
- Manages the maintenance and implementation of YSU security systems
- Manages the YSU Incident Response capability, providing emergency response for critical security issues
- Coordinates with YSU departments and System Administrators to ensure security standards are maintained for departmental systems
- Manages risk mitigation activities associated with security assessments and the vulnerability management program
- Carries out all eDiscovery data collection and filtering

IT Security Manual Maintenance:

The Information Officer along with the ITS management Team, and the General Counsel's Office will review the IT Security Manual on a periodic basis and will disseminate updates. Updates will include changes to existing items or inclusion of new items as needed to address changing technology, and security process improvements.

ITSM Exceptions and Waivers: - YSU intends for security policies to be followed by all users. Although YSU has drafted the security policies with all users and their needs in mind,

it is recognized that the security policies will not fit every conceivable situation. However, YSU intends to monitor and enforce ITSM compliance to the extent possible with current processes and technology. Regardless of the reason, end users do not have the right to violate the IT Security Manual unless an exception or waiver has been requested and approved by the Information Security team and Chief Technology Officer.

- Exceptions: - An "exception" refers to a one-time event where the IT Security Manual cannot be followed due to some technical or logistical reason. An example of an exception would be an urgently needed wireless access point to support a conference. In this case, the process of requesting the exception would allow the Information Security team to setup the access point securely, and provide secondary protections for the internal network if necessary.

- ITSM Waivers: - A "waiver" refers to a long-term deviation from the IT Security Manual, usually for technical reasons. Examples of this would be a server that cannot accept mandated security settings due to application incompatibility, or systems that cannot accept current security patches for some technical reason. In both cases, the waiver request provides the opportunity to implement alternative security controls, and possibly additional intrusion monitoring. In most cases, a waiver indicates a less than ideal security situation, and the waiver request allows that situation to be properly managed. Waiver requests are intended for long-term issues where the ITSM cannot be complied with due to technical or operational reasons. All waivers will be evaluated to determine if alternative security measures may be enacted to reduce YSU risk.

- Approval Process: - Exceptions and waivers will be considered on an individual case basis. Where appropriate, a risk assessment will be performed to evaluate the threats, countermeasures, and extenuating circumstances associated with the exception and the impact of the exception on resources and business processes. Requests for exceptions will be made in writing to Information Security team for evaluation and appropriate action.

- Documentation requirements: - Exception and waiver requests can be submitted online using the Security Waiver and Exception form. Requests for security waivers and exceptions must be accompanied by compelling rationale and enough detail to allow the YSU Information Security Officer to make a determination. For a security exception, the time period for the exception must be stated.

- Periodic validation requirements: - Exceptions will have a predetermined time frame for expiration. Compliance will be validated once the exception expires. Waivers represent long-term deviations from the ITSM, and will be validated as agreed when the waiver is granted. A revalidation timeframe will be determined based on the severity of the risk and the nature of the deviation.

Physical Access Control Procedures:

Data Center (room #401) Physical Access Procedure

Visitors if not possessing a key to the computer room must:

A. Show a photo ID such as a Driver's license
B. Sign the visitor's log
C. Enter date
D. Enter name
E. Enter time in
F. Reason for visiting
G. Enter time out when leaving

Fourth Floor Meshel - Physical Access Procedure

Prior to meeting with staff and administration in Meshel Hall, Room 437, vendors and visitors are asked to sign in and complete the Sign-In Vendor and Visitor Log. The vendor/visitor will provide name, date, destination office, and time of day on the log sheet.

Fourth Floor Meshel Staff - Key Inventory & Numeric Keypad Procedure

To request a key:

1. Receive a key request from an employee.
2. Retrieve a key record card from the Blank Forms/Originals drawer in the file folder labeled "Key Record Card".
3. Complete a key record card. For access to the Dorms, Coffelt Hall, and College of Business Administration use card titled YSU – Key/Pin Record. For all other campus buildings, use Form No. 75101 (see samples attached).
4. Forward the key card to the employee's supervisor for signature.
5. After the employee's supervisor has signed the card, update the Access database key inventory on the front office shared folder with all pertinent information (see attached sample).
6. Forward the key record card to John Hyden in Facilities for his signature.
7. Once the key is made, Facilities will notify the employee. The employee must pick up and sign for the key in Facilities.
8. Update the key inventory file on the Front Office Shared Folder with the assigned key number. Print one copy and file with office support Staff. Send copy to E-Drive to save.

To return a key(s):

1. Receive the key (s) from the employee.
2. Update the memo to Key Control on Form 11:Key Return with the necessary information. See attached sample.
3. Print one copy.
4. Make a copy of the memo and the key(s) and file the copy with office support Staff.
5. Mail the original memo and the key(s) to Key Control.

To request a key change or core change:

1. Receive the change request from the employee (i.e., office location move).
2. Update the appropriate memo to Key Control on Form 11:Key Core Change or Forms 11:Edit Key Card. See attached sample.
3. Print one copy.
4. Make a copy of the memo and file with office support Staff. Mail the original memo to Key Control.

To request numeric keypad access:

1. Receive the approval from the appropriate supervisor for a request for numeric keypad access.
2. Employee requesting access to the secured areas includes Rooms 401/401A/401C. The employee will provide a four digit access code.
3. Prepare the appropriate memo to Key Control-University Facilities, Attention: Locksmith asking to add the employee keypad access and to activate the four digit key code/pin number.
4. Once the keypad access is granted and the locksmith activates the access code, the pin number/access code is saved on Excel spreadsheet and kept in secured location in locked file cabinet.
5. Any access that is removed (i.e. employee separation) must be sent via memo to Key Control- University Facilities, Attention: Locksmith requesting the deletion of the keypad access code/pin number.

Computer & Media Disposal Procedure

Computer, electronics, and electronic media disposal is the responsibility of Electronics Maintenance Services (EMS).

Data Cleansing/Wiping/Scrubbing Procedure

When EMS receives equipment that is to be surplused, redeployed or scrapped that contains magnetic or electronic memory, staff are required to perform a 3 pass DOD wipe of functional devices.

On nonfunctional equipment, staff will remove the hard drives and wipe them with special equipment.

Functional SCSI drives removed from servers are wiped with special equipment.

Defective drives are destroyed by drilling.

All units are then tagged and marked as data removed.

Data Storage Media Procedure used by EMS staff

Old diskettes, CDs, DVDs, and flash drives received by EMS are boxed and shredded.

---

[i] The Information Technology Security Manual was formerly known as the "Information Security Practice".

[ii] Information Technology Security Manual – Update History
V2.2 – October, 2015 – Updated Policy Renumbering, Updated ISO title as appropriate
V2.1 – August, 2015 – Added public facing website restrictions, Added hosted system SOC2 or 3 requirement
V2.- April 15, 2015 – Upgraded Mobile data encryption requirements section, Upgraded for ADA requirements
V1.9 – Sept 2014 – Updated password requirements section, and created physical security section, complete re-write.
V1.8 - February 2014 - Updated password requirement and rotation requirements
V1.7 - May 2013 – Updated section on sharing passwords with emphasis on roles of accounts/passwords
V1.6 - Updated March 2013 –
Updated section 7 on wireless access, section 4 to highlight the minimum security standards for University owned devices, and, modified language related to non-University device security standards in section 9, updated mobile device process
V1.5 - Updated July 2012 –
Modified sensitive information section to include reference to DOB, updated document formatting, wording, and logo V1.4 – Updated June 2012
V1.3 – Updated April 2012
V1.2 - Updated January 2011
Implemented - January 8, 2008

[iii] Anti-virus and malicious code controls are essential to prevent the damage and misuse of both YSU and personal computing property. YSU has implemented anti-virus controls for all servers and email systems to prevent the ingress of viruses and Trojan horse applications. However, end user equipment that is not centrally managed by YSU presents an opportunity for viruses to infect and spread across the network. This could cause direct damage to infected systems. If the malicious code includes aggressive scanning behavior, network connectivity could be disrupted for some or all of the YSU campus.

The policies for anti-virus protection have been implemented to protect the environment from these risks. It is the responsibility of the end user to ensure that they adhere to these policies.

Many of the most damaging virus and worm outbreaks have exploited one or more vulnerabilities in widely used software products. Due to the rate at which these outbreaks are able to spread, many software vendors have greatly improved the response time and delivery methods available for software updates. To protect the integrity and availability of YSU network and computing resources, the following policies have been implemented:

All end user systems attached to the YSU campus network must be regularly updated to ensure they are running the most secure software available from the vendor. For commodity operating systems such as Microsoft Windows, Apple OSX and various UNIX variants, these updates may be largely, if not completely, automated. If the system does not support automated updated, it is required that software is

updated every 30-days.

Systems observed to be violating this standard by operating insecure or obsolete services may be isolated from the network until the situation has been addressed.

[iv] Encryption: - When implemented properly, modern encryption protocols, algorithms and toolkits provide a very powerful capability to protect sensitive information. However, when implemented poorly, encryption may provide no additional protection, and may actually increase the overall risk due to poor key management. For more information on supported encryption tools at YSU, please contact the Tech Desk.
Because of the potential for loss of information, YSU policies regarding encryption are primarily on an 'as needed' basis:

- Encryption must be used when required by any applicable standard for which YSU is held accountable. Cases where encryption is recommended, but not required, must be reviewed by Network Security prior to implementation.
- Passwords and other sensitive information must not be transported over the network in the clear. For example, web applications must use HTTPS for authentication instead of standard HTTP, and UNIX systems must use SSH instead of Telnet for system administration.
- Encryption keys must be stored securely, with access controls that prevent disclosure of the key(s) to unauthorized individuals.
- Encryption strength selected for a given application should be the highest possible strength that maintains acceptable performance and load criteria for a given application while adhering to industry best practices.