Mississippi State University Information Security Program

The Mississippi State University Information Security Policy mandates a framework of four components that collectively enhance the information security posture of the institution. One of the components, the Information Security Program, identifies technologies, procedures and best practices to ensure ongoing institutional focus on the protection of information. Key elements of the program are:

- Data Classification and Individual Responsibilities
- Risk Assessment and Safeguards
- Training and Awareness
- Monitoring
- Audit and Compliance
- Minimum Security Standards
- Best Practices

The program documents the best practices and procedures which will help safeguard the information assets of the institution. As prescribed by the Information Security Policy, the Information Technology Council coordinates the implementation and execution of the Information Security Program on an ongoing basis.

Mississippi State University Information Security Program
Data Classification and Individual Responsibilities

1. **Purpose.** The purpose of this section is to establish a classification scheme for official data and information maintained by Mississippi State University and to establish responsibilities for its protection from unauthorized release or modification. To that end, this section assigns responsibilities for the control and appropriate stewardship of such data.

2. **Scope.** The data classification program pertains to stewardship of all data assets at MSU, whether digitized/electronic, in paper form, or spoken. It is directed toward the classification and subsequent protection of information used in the conduct of official business and the representation of data is irrelevant to the requirement to classify and protect it.

3. **Authority.** Federal laws such as the Family Educational Rights and Privacy Act (FERPA), the Privacy Protection Act, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Intellectual Property Act, the Gramm-Leach-Bliley Act and the Freedom of Information Act require oversight and protection of specific types of data. This program outlines the university recommended procedure to classify and protect data in accordance with applicable Federal and State requirements.

4. **Roles:** The following roles of university personnel are defined below:

   a. **Data User (custodian):** A university employee who has access to official university data as part of his or her assigned duties. Examples of a data user would include a faculty member, a database administrator, an administrative assistant, secretary, student worker, clerk, or office worker, among others.

   b. **Data Manager:** A university official having operational level responsibility for information management related to the capture, maintenance, dissemination, storage and use of data by an organizational entity. Examples of data managers would include the Dean of a College, a Department head, the Chief Human Resources Officer, the Director of Financial Aid, the Registrar, and the Director of Sponsored Programs, among others.

   c. **Senior Official:** University administrators at the Vice President level or equivalent, who have planning and policy level responsibility for data within their areas and management responsibilities for segments of the institutional data.

5. **Data Classification Categories.** Mississippi State University classifies its official university data into three categories – Category I, Category II, and Category III as described in this section.

5.1 **Classifying Data.** The primary consideration in classifying data is damage that would accrue to MSU should the data be inadvertently released to unauthorized parties through any means. Loss of Category I data would do significant harm to the University. Significant harm is a subjective decision criteria to be made by the Senior Official having data oversight, but must include any data whose protection is mandated by Federal or State law or data that would cause irreparable harm to the University or its reputation (e.g., compromise of donor financial holdings or data that would result in a negative image for the University). Loss of Category II data would result in less substantial harm and its protection is not mandated by law. Category II data may require the same or similar protections as Category I data, but its loss or compromise is not deemed unmanageable (e.g., individual student test scores). Category III data is public and requires no protection.

5.2 **General Examples.** Data classification authorities will use the criteria outlined in paragraph 5.1 to decide which classification their data assets fall under. Classification depends on several factors combined with management judgment. To assist in deciding on the appropriate classification, general examples are given below. These are not intended to be comprehensive or definitive. The actual end classification determination is a management decision based on data sensitivity and harm done if the data is inappropriately released or compromised.

a. **Category I data:** Category I data refers to data protected specifically by law or by Mississippi State University policy. Examples of category I data include data covered by HIPAA; FERPA; donor, employee, or sensitive research data; Social Security identification numbers, payment card data; financial institution data, and data that is not otherwise protected by a known civil statute or regulation, but which must be protected due to proprietary, ethical, privacy, or criticality considerations. Specific examples of Category I data include (but are not limited to) the following:

- Social Security numbers
- Credit card numbers
- Patient medical health or record information
- Personal vehicle license/registration information
- Financial records (e.g., financial donor contributions, student/employee financial accounts, bank accounts, aid/grants, fines, or records of financial transactions)
- Personnel records of employees

- Student-specific grade records (including test scores, assignments, and class grades)
- Student transcripts
- Student entry and transfer records
- Access device numbers/passwords (e.g., building access code, Banner passwords, computer passwords, encryption keys)
- Biometric data with personal identifying information
- Human subject information with personal identifying information
- Sensitive research data, including data subject to export control regulations
- Insurance benefit information
- Driver’s license number or state identification number

b. **Category II data:** Category II data includes data releasable in accordance with proper authority (Freedom of Information Act, law enforcement investigation) and may include items such as the contents of a specific e-mail containing sensitive information, student date of birth, employee salary. Category II data is that which must be protected due to proprietary, ethical, or privacy considerations. This classification applies to data that is not otherwise protected by a known civil statute or regulation, but if inappropriately released to unauthorized parties could do harm to the university and its reputation. Such release might result in negative publicity. Specific examples of Category II data include (but are not limited to) the following:

- The calendar for a university official or employee
- The emails of a university official or employee containing sensitive information
- Lists of electronic mail addresses
- Promotion and tenure files
- External review letters
- Detailed accreditation results
- Date of birth, place of birth of students or employees
- Internal audit data
- Student evaluations of a specific faculty member
- Findings of internal investigations
- Human subjects research data with no personal identifying information
- Donor giving records
- Minutes of meetings involving personnel decisions
- Records of meetings discussing disciplinary actions

c. **Category III data:** Category III data is general access data. This is data that is not restricted or judged to be Category I or II. This data is subject to disclosure to all MSU employees as well as the general public. Specific examples of Category III data include (but is not limited to) the following:

- Departmental Web site
- Library data and holdings
- Public phone directory
- Course catalog and curriculum information
- General benefits information
- Enrollment figures
- Publicized research findings
- State budget
- All public information

6. **Responsibilities for Classification of Data.** The overall responsibility for Data Classification rests with the Provost and Executive Vice President. This authority is delegated to the MSU Chief Information Officer. All senior officials at Mississippi State University will require data managers and data users within their scope of responsibility to classify data at Category I, II, or III. The MSU senior official responsible for specific types of data is as shown in Table 1 below.

TABLE 1

Senior Official Data Classification Responsibilities

Data Type	MSU Senior Official
Payroll Data/Financial Data	Vice President for Budget and Planning
Library Data, Student Data, Electronic Records, Course Data, Admissions Data, Scholarships, Financial Aid, Faculty Data, Communications Data, Human Resources Data	Provost and Executive Vice President
Alumni Data, Foundation Data	Vice President for Development and Alumni
Student Medical, Counseling, Housing, Discipline, and University police data	Vice President for Student Affairs

Sponsored Programs, Human Subject Research, Security Clearances, and Security policies	Vice President for Research and Economic Development
Experiment Station, Agricultural, and Veterinary Medicine data	Vice President for Agriculture, Forestry, and Veterinary Medicine
Facilities Data	Vice President for Campus Services
Bulldog Club donor information, athletic financial information	Athletic Director
Other	Provost and Executive Vice President

7. **Data protection measures.** Data classified in Category I or II as defined above or as classified by the appropriate MSU Senior Official will be protected by data users/custodians as follows. It is important in implementing data protection measures to keep in mind that loss of Category I data is more severe than loss of Category II data and may require a higher level of vigilance. Additionally, the below is not intended to be an all encompassing list – it should serve as a starting point and as an example of good protection practices.

    - All U.S. Government classified material must be stored in accordance with procedures approved and implemented by the Vice President for Research and Economic Development.
    - Paper copies of Category I or II data should be secured in locked containers when not in use. Offices containing such data should also be locked when not occupied. A locked office should not be considered sufficient for protection if multiple access keys exist for the office and the office is routinely left open during normal business hours.
    - Verbal disclosure of Category I or Category II data to unauthorized parties is a violation of the MSU data classification program. Employees of MSU must be reminded to discuss such information in protected environments to preserve its confidentiality. This is particularly important when discussing medical information, personnel decisions, student performance, or disability issues.
    - All Category I and Category II paper waste must be shredded or burned. Under no circumstances should such data be discarded in trash cans.
    - Category I or II data must not be displayed in a public area.

- Data managers should strongly encourage a “clean desk” policy in areas where Category I and II data is routinely accessed by users.
- Category I data must be protected by physical access controls and passwords. It is highly recommended that Category I data not be placed on mobile computing devices. However, mobile devices such as laptops and flash drives containing Category I data must employ encryption since these devices are more likely to be lost or stolen.
- Category II data should be protected by physical access controls and passwords wherever possible. It is highly recommended that mobile computing devices containing Category II data employ encryption to the maximum extent possible to protect information in the event of theft.
- Encryption should be employed when electronically transmitting Category I or Category II data.
- The disposal of electronic media containing Category I data is a particular concern. Such media must be electronically wiped clean or destroyed.   Electronic media containing only Category II or III information can be locally cleaned before release by data managers or their appointed authority.
- University magnetic media containing unencrypted Category I or II data must not be released to maintenance contractors or leasing agents without first being sanitized.
- Data managers should periodically make data protection measures a matter of interest with their subordinates and oversee the implementation of the data classification program.

8. **Compliance**. The MSU Internal Auditor is responsible for assessing compliance with this program during the course of regularly scheduled audits of university organizations. Requests for Category I or II data from outside sources should be directed to the office of the Chief Information Officer for release authority when an existing process has not been established.

Mississippi State University Information Security Program
Risk Assessment and Safeguards

1. **Purpose:** The purpose of this section is to provide a process of identification of information assets in both physical and electronic forms that must be protected and methods to implement safeguards deemed appropriate.

2. **Scope:** The risk assessment program must pertain to all information assets of the institution. The program includes risk management where an ongoing process of risk identification and the subsequent development of plans to safeguard information can be done on a university-wide basis.

3. **Program:** The program must apply a strategic approach to making the university culture evolve into a "risk aware" culture. The complete information security program includes diverse elements such as awareness and training that are in themselves important risk components. The risk assessment process is primarily a management issue that must be addressed by all university personnel whose role includes the management of information wherever it is stored. The State of Mississippi Enterprise Security Policy (ESP) requires an IT security risk assessment from third-party security consultants at least once every three years. MSU's program will meet or exceed the requirements outlined in the ESP Comprehensive Assessment Guidelines.

    - Apply the MSU Data Classification standards to classify institutional information, regardless of media, such as databases, networks, servers and information systems to identify critical systems, assets and risks.

        - Ongoing risk assessment program will include an online risk assessment instrument distributed regularly to correlate the classification and security of information spread throughout the institution.
        - Units must keep an inventory of all server systems and register them with Information Technology Services.
        - A yearly external IT risk assessment for critical units will be focused on providing a comprehensive assessment of all campus within a 3-year period.
        - Penetration testing must be an integral part of external/internal assessments. Proactive social engineering risk analysis will be included.
        - Existing Social Security number usage forms required as per OP 01.23 will be evaluated to confirm system classifications on an ongoing basis.
        - The integrity of MSU's IT environment can be compromised by malicious software running on computer systems

connected to the University’s network. Foreign software that is neither commercially available nor open source is high risk and prohibited on university-owned equipment.
Requests for exceptions can be initiated by completing the Foreign Software Exception Form available in Appendix D. A list of approved exceptions is available at the Information Security website infosecurity.msstate.edu.

- Implement Baseline Security Strategies

  - Promulgate to the campus community minimum security standards for computer systems, see Appendix A.
  - Identify current protection strategies such as campus firewall deployments, anti-virus solutions, intrusion detection and staff operational practices that can provide baseline security.
  - Firewall and other protection strategies will be correlated with the campus system inventory and data classifications.

- Identify Infrastructure Vulnerabilities

  - Identify the systems and physical exposure issues in administrative offices and campus computer systems.
  - Proactive vulnerability scans will be performed on all systems that have requested firewall exceptions and additional systems based on information classifications.
  - A robust internal vulnerability assessment program of monthly scans for all Category I servers will be managed by Information Technology Services. Systems change over time and new vulnerabilities are always being discovered requiring an ongoing internal program of vulnerability assessment confirmed by yearly external review.
  - Periodic monthly results summaries will be delivered to relevant campus units.

- Perform Risk Analysis and Mitigation/Safeguards

  - Strategic planning based on the results of the risk assessment allows the targeted implementation of safeguards to systems that contain critical institutional information and where legal requirements are paramount.
  - Two factor authentication is required for web access to all systems storing, processing, or transmitting Category 1 data, and strongly recommended for all other systems.
  - Apply a cost-benefit analysis to the strategic questions of security safeguards and business processes.

- The diverse nature of computing on campus provides for a variety of environments where the application of industry best practice can mitigate risk.

4. **Summary:** Technology alone cannot ensure a secure environment. Personal responsibility, application of good security practice and a University culture that is aware of the risks associated with information breaches can mitigate many security problems. Ongoing risk assessment is a critical component of a complete security program that should change and evolve as the computing and information assets of the institution grow.

Mississippi State University Information Security Program
Training and Awareness

1. **Purpose:** The purpose of this section is to define the training and awareness program as an element of the Mississippi State University Information Security Program.

2. **Scope:** This program applies to the handling of sensitive information by employees and students of Mississippi State University.

3. **Program:** A key component of the university's Information Security Program is training and awareness on the part of the people entrusted with collecting and handling sensitive information. The university has an additional obligation to educate its students and employees about the importance of protecting their own personal information. Therefore the Training and Awareness section of the Information Security Program has two goals, the first to educate all employees on proper protection of sensitive information and the second to teach students, faculty and staff to protect their own personal information.

3.1. **Training:** The first major element of the training and awareness program is online training aimed at employees, graduate assistants, and student workers. The training is organized in a modular format to facilitate progression through the material, and each module ends with a quiz that measures understanding of the material just covered. Once an individual completes all required modules, that person is certified to have successfully completed the required MSU information security training. This certification is good for a period of two years.

All employees in the following EEO categories are required to complete information security training:

- EEO 10 – Executive/Administrative and Managerial
- EEO 20 – Faculty
- EEO 30 – Professional (non-faculty)
- EEO 40 – Technical and Paraprofessional
- EEO 50 – Clerical and Secretarial

All graduate assistants are also required to complete the training. Employees in other EEO categories and student workers may be required by their unit head to take the training.

Those required to have information security training must successfully complete it within 30 days to receive their two-year information security training certification. After two years, the training must be retaken and completed, again within 30 days, to maintain certification for another two years. Individuals who are within their 30 day training window will receive email notification of their requirement to complete the training, along with instructions on how to access the training materials.

It is the responsibility of unit heads to ensure that employees in the above EEO categories and graduate assistants complete the information security training. It is also the responsibility of unit heads to ensure that employees not in the above EEO categories and student workers who have access to sensitive information complete the training as appropriate. Employee orientation will be used to inform new personnel about the program and the requirement to complete training within 30 days of employment. Information security training records will be maintained to indicate who has completed the training and when, and a report will be available to unit heads to track compliance. Internal Audit will confirm compliance during departmental audits.

The Information Technology Council is responsible for periodic review of the information security training content and for recommending changes to ensure continued relevance and effectiveness.

3.2. **Awareness Campaign:** The second major element of the training and awareness program is a campaign targeted at student and employee protection of one's own personal information. The campaign will use a combination of informational Web sites, student awareness sessions during Freshmen Orientation, printed brochures, and posters. The content of these different types of media will focus on the importance of individuals protecting themselves by securing their personal information. Examples relevant to students such as their activities on social networks like Facebook will be used. Additionally, protection of important personal university credentials such as the MSU ID Card and NetPassword will also be stressed.

3.3. **Cyber Security Awareness Week:** The third major element of the training and awareness program is a Cyber Security Awareness Week which will be an annual event held during the fall semester. The event will employ a variety of resources such as information booths, seminars, and demonstrations. Specific aspects of information security such as identify theft will be highlighted, and information security experts from across campus will be employed. The goal of the Cyber Security Awareness Week is to provide a periodic reminder to the campus of the importance of information security, thus maintaining a high level of awareness among faculty, staff, and students.

4. **Summary:** Information security is a shared responsibility that cuts across all segments of the university. A number of units are collaborating to develop and implement the university's training and awareness component of the Information Security Program. Participating units include the Department of Human Resources Management, Dean of Students, Information Technology

Services, and the computer security program in Computer Science and Engineering.

Mississippi State University Information Security Program
Monitoring

1. **Purpose:** Security monitoring is the collection, analysis, and escalation of indications and warnings to detect and enable response to breaches of information security. It is also a method of confirming that existing security practices and controls are effective over time. Security monitoring consists of activities such as the review of user account logs, application logs, data backup and recovery logs, automated intrusion detection system logs, and operational procedures. The purpose of security monitoring is to ensure that information resource security controls are in place, are effective, and are not being bypassed.

2. **Scope:** This program applies to the following categories of security:

   - Computer system and application security: Central processing unit, peripherals, operating system software, application software, and data.
   - Physical security: The premises occupied by information technology personnel and equipment as well as storage facilities for analog or digital data.
   - Operational security: Environmental control, power equipment, operational activities.
   - Procedural security: Established and documented security processes for information technology staff, vendors, management, and individual users.
   - Network security: Communications equipment, personnel, transmission paths, and adjacent areas.
   - This program applies to all university information resources.

   The intended audience for this program consists of all data managers/owners and all individuals that are responsible for the installation of new information resources or the operation of existing information resources.

3. **Program:** Security monitoring of information resources shall be implemented based on risk management decisions made by the information resource manager/owner.

   - Category I and Category II information resource systems shall, at a minimum, have operating system and application logging features enabled.
   - Automated tools shall be used where deemed beneficial by the resource owner based on risk management decisions.

- Operating system and application software logging processes shall be enabled on all host and server systems containing Category I or Category II data. Where possible, alarm and alert functions, as well as logging and monitoring systems shall be enabled.
- Server, firewall, and critical system logs should be reviewed frequently. Where possible, automated review should be enabled and alerts should be transmitted to the administrator when a security intrusion or other anomaly is detected.
- Intrusion tools should be installed where appropriate and checked on a regular basis.
- All network attached systems should have a supported operating system installed which is current with all security patches. Obsolete or unsupported systems shall not be used for communication beyond the local network.
- Regular system integrity checks of host and server systems housing high risk university data should be performed.
- Category III information resource systems are not required to be monitored, but owners of the resources are encouraged to take all appropriate measures to secure them.
- Network security monitoring for the campus backbone network and for departmental networks operated by Information Technology Services will be conducted by ITS. Ancillary networks not operated by ITS must be monitored by the owner/manager of that resource.
- Logs and other data generated by security monitoring shall be reviewed periodically.
- Any significant security issues discovered and all signs of unauthorized activity shall be reported using the procedures detailed in the appropriate section of the Information Security Plan.

4. **Summary:** The assessment of potential risks, the application of appropriate mitigation measures, and the monitoring of these security measures are the responsibility of the information resource manager/owner or their designee.

Mississippi State University Information Security Program
Audit and Compliance

1. **Purpose:** The purpose of this section is to describe the role of auditing as an element of the Mississippi State University Information Security Program.

2. **Scope:** The audit and compliance program pertains to all information assets of the institution. The program includes a continuous systematic audit process that evaluates university-wide compliance with the Information Security Policy and Information Security Plan.

3. **Program:** In relation to the Mississippi State University Information Security Program, auditing can be defined as a systematic process of objectively obtaining and evaluating evidence in order to determine the degree of compliance by university units (collectively and/or individually) to the Information Security Policy and Information Security Plan.

   There are many methods and tools, several of which overlap, that can be used to audit information security. The specific timing and nature of audit techniques utilized will be dependent on resources available; however, audit efforts will be focused on those areas assessed as having the greatest risk and will coordinate with and compliment monitoring efforts. Areas that are subject to audit include but are not limited to the protection of sensitive data (electronic, paper, and other), university and department security policies and procedures, training and awareness programs, and systems administration procedures.

   Coordination of audit efforts will be the responsibility of the MSU Office of Internal Audit. MSU will utilize both self-audits and independent audits. Departments/units will be provided self-audit questionnaires, checklists, and/or other materials, approved by the Information Technology Council, that will be used to perform self-audits. Once the self-audit document is complete departments will be required to perform a self-audit every two years. Independent audits will be performed (jointly and/or separately) by the Office of Internal Audit, ITS, and/or other such appropriate units. External companies may also be engaged to perform independent audits. Audit procedures performed by the Mississippi Office of the State Auditor and the Mississippi Institutions of Higher Learning Internal Audit Office may also be relied upon as they relate to information security.

APPENDIX A
Minimum Security Standards for Computer Systems

1. **Purpose:** Adherence to minimum security standards for computer systems is critical to the protection of institutional information assets as well as the operational integrity of the university's information technology infrastructure. The standards outlined by this section cover the configuration and maintenance requirements for systems on the Mississippi State University (MSU) network.

2. **Scope:** Certain security configurations and standards are required for all systems that connect to the Mississippi State University data network. Additional operation and configuration standards are required where data is classified using the MSU data classification program.

3. **Authority:** The Policy and Procedure for Use of Computing and Network Resources at Mississippi State University (OP 01.12), requires users or administrators of computers systems to maintain the security of computing resources.

4. **Standards:** Software obsolescence is a critical problem for computer system security. All network attached systems should have a supported operating system installed which is current with all security patches. Obsolete or unsupported systems must not be used for communication beyond the local network.

   The following table outlines the minimum security standards for computer systems based upon the category of data stored on the system, as defined in the Data Classifications and Individual Responsibilities section of the Information Security Program. Category I data is protected specifically by law or by Mississippi State University policy. Category II data is not otherwise protected by statute, regulation, or policy, but could do harm to the university and its reputation if inappropriately released. Category III data is public information.

#	Configuration	Cat I	Cat II & III
1	All critical security patches should be applied. Updates set to download automatically for Microsoft OS and Mac OS	Required	Required
2	Anti-virus software must be installed and enabled with live update where practicable	Required	Required
3	Network Firewall protection for servers	Required	Required
4	Workstation access protected by login and password (excluding public access systems such as kiosks)	Required	Required
5	Workstation inactivity triggers password protected screen saver (excluding public access systems such as kiosks)	Required (20 min max)	Required (60 min max)
6	Host-based Firewall protection	Recommended	Recommended
7	Anti-spyware protection	Recommended	Recommended
8	Laptop and “flash drive” Whole Disk Encryption	Required	Recommended
9	Legacy protocols such as Telnet, FTP, pop, imap which do not encrypt passwords should be replaced with secure alternatives such as SSH, SFTP, pops, imaps (dedicated network devices such as printers excluded) Standard http auth should be replaced with https SSL protection	Required	Recommended
10	Services, applications and user accounts not in use should be disabled or uninstalled	Required	Recommended
11	Systems must be physically secure or encrypted with restricted access	Required	Recommended
12	Data backup must take place on a regular basis, with secure storage of media	Required	Recommended
13	System integrity checks performed on a regular basis, including backup media verification	Required	Recommended
14	System logging enabled and reviewed	Required	Recommended
15	Proactive vulnerability scans	Required	Recommended
16	SSL certificates should be from a recognized authority.	Required	Recommended
17	Enterprise passwords must be protected by encryption during use and encrypted at rest.	Required	Required

5. **Summary:** Use of Mississippi State University's computer and network resources is not a matter of right, but rather all use of Mississippi State University's computer and network resources must be consistent with the mission of the university in support of public education, research, and public service. Minimum standards for system configuration and maintenance allow for the protection of university data, the protection of other systems connected to the university network, and help prevent the improper use of campus resources.

APPENDIX B
End User Best Practices

1. **Critical Security Patches:** Operating system patches should be loaded automatically. Microsoft Windows provides "Automatic Update" to automatically download and install patches on a schedule. Best practice would be to do this daily to insure that all critical updates and service packs are installed in a timely manner. Apple Macintosh users under OSX are provided with "Software Update" where OSX checks for operating system updates may be scheduled. Software such as media players, browser plug-ins, office applications and others are often overlooked but can have significant security issues and must be patched regularly.

2. **Viruses:** As required by MSU Policy 01.12, personal computers must be protected by anti-virus software and virus definitions must be kept current. Best practice is to enable the automatic update service for daily updates. Anti-virus software that has expired is of little value and must be replaced. ITS provides, at no charge, Sophos Anti-Virus which is available at http://www.its.msstate.edu, under the software downloads sections.

3. **Firewalls:** The MSU campus network is protected from external threats by a system of firewalls. However, attacks can originate from computers within the MSU campus network (e.g., a roommate's infected PC). Best practice recommends use of a host firewall product to guard against this level of threat. Modern operating systems such as Windows and OSX provide reasonable firewall services.

4. **File Sharing:** Peer to Peer (P2P) file sharing software can provide a method of entrance for many types of infected and prohibited software and an exposure risk to University data. Users should be aware of the university acceptable use policy MSU Policy 01.12 and read http://filesharing.msstate.edu for additional information before usage of any P2P software on university owned equipment.

5. **Spyware:** Spyware is another category of malicious software that must be guarded against. ITS recommends the free Spybot – Search and Destroy product available at http://www.its.msstate.edu, under the software downloads section. Other free products such as Microsoft Windows Defender or commercial products such as Malwarebytes are also available.

6. **Passwords:** Per MSU Policy 01.12, passwords should be obscure, hard to guess, changed regularly, and never shared. Avoid using words found in the dictionary and obvious passwords like the name of a pet or family member. Strong passwords contain a mixture of upper and lower case letters, numbers, and special characters. A good, memorable password might be formed from

the letters of a phrase along with some special characters. For example, "My dog Spot is a great dog" could yield the password MdSiaGd! **WARNING:** As noted above, the sharing of passwords is a violation of university policy and could result in disciplinary action being taken.

7. **Awareness:** Users should be aware of sensitive data that may exist on their computers. Tools such as Cornell "Spider" can help find some sensitive data that might be stored inadvertently. This free software is available at http://www.its.msstate.edu, under the software download section.

8. **Email:** Users must be aware that email typically transmits information in "clear" text and should never be used to send unencrypted sensitive data. Always be careful of links and never respond to requests for personal information. http://www.infosecurity.msstate.edu/faqs/

9. **Web Space:** Sensitive data must never be stored in a publicly accessible Web space. Even if no direct link to the information exists, search engines and Web "crawlers" can discover such information and enable direct access to it from anywhere on the Internet.

10. **File Storage:** ITS provides general purpose network storage for units that it supports. The J:\Everyone folder is shared by the entire unit, and everyone in the unit can access documents stored in that folder. You should be aware of this and understand that ITS can also provide restricted access, shared folders on the J: drive. Other units may also provide network file storage, and users in those units should understand who has access to the files stored thereon.

11. **Cloud Services: As the popularity of cloud-based services** such as Dropbox.com, Google, Box.net, Amazon, and iCloud grows, users should exercise caution when storing or transmitting information with any cloud service. Consider legal, regulatory, and University policy requirements in areas such as:

    - FERPA and HIPPA
    - Grant restrictions
    - Human Subject restrictions
    - Intellectual Property restrictions
    - Export restrictions
    - Data Classification of information.

12. **Paper Shredding:** Always shred documents containing sensitive information when disposing of them, and use a cross-cut or high security paper shredder instead of the more common strip-cut shredder. Use of a cross-cut or high security shredder makes it virtually impossible to reconstitute a document from its shredded remains.

13. **Purchases:** Employees should consult with their local information technology support staff about security considerations when evaluating new IT goods and services.

14. **Software:** Be careful what you install on your work machine. Many users say "Yes", to all options when installing software and end up with additional "toolbars", multiple anti-virus packages or other extraneous software that will often conflict with existing software.

15. **Backup:** Users should store critical files on network folders where regular backup is provided by their unit's information technology support staff. Users should protect their mobile devices from theft and make sure that data stored on these devices is being backed up regularly.

16. **Encryption:** Sensitive data should never be transmitted across the network without encryption. SSL is a method used to protect data passed between a web browser and web server and is identified via the "lock" symbol on your browser. Web pages that collect or display sensitive data and everywhere you login via the web should be protected via encryption. SSH is a secure replacement for protocols such as TELNET and FTP. It uses strong encryption to protect the data transfer between a client computer and a server.

17. **Disk/File Encryption:** Sensitive data should not be carried on a portable electronic device such as a jump drive or laptop that could easily be lost or stolen. However, in situations where this is a requirement, the sensitive data must be encrypted. On mobile systems such as laptops the best practice is to encrypt the entire hard drive via whole-disk encryption software. **WARNING: Installation of whole-disk encryption software should only be done after consultation with your IT support person. As a precaution, it is recommended that you make a copy of your hard drive before installation. Losing the decryption key will lose all data.** Unit supervisors are responsible for maintaining all decryption keys in secure locations in the event of an emergency. Further information about campus-supported disk encryption products can be found on the ITS webpage at http://www.its.msstate.edu/software/dept/.

18. **VPN Remote Access:** A Virtual Private Network (VPN) provides a secure encrypted network connection over the Internet between a workstation and a private network. ITS provides VPN services to faculty and staff to enable access to restricted services. Best practice restricts certain services to campus address ranges. Examples include remote desktop control or remote management (SSH) access.

APPENDIX C
System Administration Best Practices

In addition to the best practices outlined in Appendix B, the following should also be adopted by system administrators for servers under their control.

1. **Physical Security:** Servers must be housed in physically secure locations with restricted access. Best practice would be to control and monitor entry via the university's electronic card access system. These locations should have suitable HVAC, electrical and fire protection systems based upon server requirements.

2. **Backup:** A data backup/restoration process must be in place to protect against accidental loss of data. Best practice would call for daily backup with secure storage of backup media. Backups should be inherently off-site or carried off-site on a regular schedule to be determined by the requirements of the data housed.

3. **Disaster Recovery:** Depending upon the criticality of the system, a formal disaster recovery and business continuity plan may be required to protect the institution in the event of a catastrophic system failure.

4. **Logging:** Appropriate levels of system logging must be enabled and the output reviewed on a regular basis to facilitate the detection of unusual activity that might adversely impact system performance or security. Automated log analysis and exception reporting is recommended.

5. **Firewall Exceptions:** Firewall exceptions that expose system services to the outside world should only be done when necessary. Best practice is to open only the necessary ports required by the service(s) being provided. Servers and end-user workstations should reside in logically separate networks to limit exposure as much as possible.

6. **Vulnerability Scanning:** Vulnerability scans that look for exploitable weaknesses should be performed on a regular basis and action taken to remediate or mitigate exposed vulnerabilities.

7. **Secure Protocols:** Legacy protocols such as TELNET, FTP, POP and IMAP are inherently insecure because they transmit unencrypted passwords. Best practice replaces these protocols with their secure alternatives e.g. SSH, SFTP, POPS and IMAPS.

8. **Test Systems:** For servers that are critical to the business of the university, separate systems should be employed to allow staging and testing of changes before moving them to production servers.

9. **Least Privilege:** Systems and user roles should be configured on a "least privilege" basis so that the minimal required authority or access is granted. This

ensures that systems and users are less likely to cause harm, whether accidently or maliciously.

10. **Restricted Remote Access:** Best practice restricts certain services to campus network address ranges, thus limiting exposure of critical systems from the public Internet. ITS provides a Virtual Private Network (VPN) service to facilitate remote access to such restricted services. Examples of services that are restricted to the MSU network, thus requiring VPN access from off-campus, include remote desktop control and Administrative Banner.

APPENDIX D
Foreign Software Exception Form

Please provide the following information concerning a request to install foreign software that is neither commercially available nor open source on Mississippi State University systems.

System Name:

System Purpose:

Synopsis of Data contained on system/Data Classification:

Describe the Research/Teaching/Service Mission that requires the installation of such software:

Approval: ____
Information Technology Council (Mailstop 9697)