ITS POLICIES AND GUIDELINES
CATEGORY: Information Technology, Security, Privacy, Information Access & Management
STATUS: Approved

POLICY TITLE: **Information Technology Security Policy**

POLICY PURPOSE:
The purpose of this Information Technology Security Policy is to ensure and describe the steps necessary to secure information resources and to establish protocol for the timely resolution of security incidents at Truman State University.

The University's mission and strategic initiatives are enhanced through the use of technology, the Internet, virtual classrooms, anytime-anywhere remote access, business, and student administration systems, and, strong, reliable high-speed network infrastructures. In many cases, the success of the mission depends on the availability of these resources, and ultimately on how well they are secured and protected.

Security breaches have become commonplace and universities are no exception due to the significant computing resources available on university campuses across the nation. As a result, critical university computing resources, such as research, patient care, and student data, are at risk, and university computing devices have been used by cyber-criminals to launch attacks both within and outside universities.

The campus has a responsibility to secure its computers and networks and to respond quickly to threats to the integrity of its systems and data. While it is not possible to anticipate and intercept all attacks, there are specific steps that can be taken to significantly reduce vulnerability. These steps are effective, however, only if they are taken for all devices in Truman's network. It only takes one vulnerable device to make the entire network vulnerable. A compromised computer in one department can easily be used as a springboard to launch attacks on computers in other departments or on the Internet.

APPLIES TO:
- All members of the Truman State University community
- Anyone granted access to Truman State University data, systems or networks
- This policy applies to any device owned by the University or used for University business by faculty, staff, students, and affiliates, or utilized by residents living in a University residence hall or other on-campus housing facility.

CONTENTS:

POLICY STATEMENT:
Truman's Information Technology Services office has the responsibility and authority to evaluate the seriousness and immediacy of any threat to campus information resources and to take action to mitigate that threat. Action that is taken will be based on the risk associated with that threat and the potential negative impact to the campus mission caused by making the offending computer(s) inaccessible. For major systems, units should request a security review before purchasing hardware, signing contracts, and before connecting systems to the network.

Examples of threats that are serious enough to invoke these procedures are: 1) the level of network activity is sufficiently large as to cause serious degradation in the performance of the network; 2) system administrative privilege has been acquired by someone who is not authorized to have it; 3) an attack on another information resource has been launched; 4) confidential, private, or proprietary electronic information or communications are being collected, destroyed, or disseminated inappropriately; or, there is reason to believe the possibility exists to collect electronic information inappropriately; 5) serious complaints have been received regarding inappropriate activity, or 6) any other threat that has been formally identified.

Campus units that maintain their own information resources are encouraged to add, with the approval of the unit head, unit-specific guidelines that supplement, but do not lessen the security intended by this policy. In addition, campus units must take any additional steps needed to comply with the requirements of state and federal laws pertaining to the security of electronic information and resources. Campus units must provide a copy of unit-level policy to the Chief Information Officer and the Office of General Counsel prior to implementation of unit-specific guidelines.

Truman is committed to compliance with applicable federal and state laws including but not limited to the: Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (Title 18 of the U.S. Code); Electronics Communications Privacy Act of 1986 (Public Law 99-474); Computer Security Act of 1987 (Public Law 100-235); and USA Patriot Act of 2001.

1. Responsibilities

1.1. Departments/Units

- Each department or unit is responsible for the technical security profile of the information resources that it owns and uses.

- Each department or unit will initiate and/or terminate access rights when authorized users change status (e.g., terminate employment, graduate, retire, change positions or responsibilities within the University, etc.). The department or unit is responsible for maintaining access protocols on their locally maintained information resources and informing University and appropriate system administrators of employee changes in status that affect access to central systems.

1.2. Information Technology Services Office

- The Information Technology Services Office (ITS) will investigate security incidents to determine severity of threats; make decisions on appropriate actions; and notify appropriate information technology personnel. ITS will coordinate and communicate with departments regarding necessary actions.

- ITS will track open incidents to ensure timely resolution.

- ITS will maintain individuals' privileges and respect their privacy to the extent reasonably possible when accessing others' files for the maintenance of networks and computer and storage systems, for example, creating backup copies of media.

- ITS will cultivate awareness of security issues and vulnerabilities within the University.

- ITS will approve the connection of critical and essential systems to the campus network.

- ITS will conduct Risk and Vulnerability Assessments on University systems as defined by this policy and upon request from department/unit staff.

1.3. Authorized Users of Information Technology

- Authorized users of information technology must become aware and acknowledge responsibilities for security when obtaining access to University information resources.

- Authorized users of information technology must accept responsibility for any authorized use of information resources and personal accounts. Computer accounts, access codes, passwords, and other types of authorization are assigned to individual users and must not be shared with others.

- Authorized users of information technology must protect the access and integrity of information resources by following the security practices recommended by Information Technology Services.

1.4. Vendors

- ITS will be responsible for educating vendors about the security protocols on University information resources and any federal laws that might apply. All staff employed by vendors who work on University information resources are required to sign the Information Technology Employee Privileged Access and Confidentiality Agreement and be certified by either their employer or ITS before accessing University systems. By contract, the Information Technology Employee Privileged Access and Confidentiality Agreement may be signed by a main University contact, with information conveyed by the employer to individual staff working on University systems. Vendors will only be granted the necessary access to fulfill tasks that have been predetermined. Agreed upon vendor work will be reviewed upon completion to ensure its quality, accuracy, and completeness.

2. Protocol

2.1. Blocking Network Access or System Isolation

The ability to quickly contact responsible departmental personnel and have them take appropriate action can mitigate the negative effects of an incident both locally in the department and more globally throughout the campus and the Internet.

When a problem is identified, ITS must be able to quickly contact the appropriate campus department who can take action. If the threat is immediate, ITS will block the offending information resource immediately (or isolate it) and will notify the department that the block has occurred. If the threat is not immediate, notification of the threat will be sent to the department. If a response is not received within four hours indicating that the department is taking action to mitigate the threat, the offending information resource will then be blocked (or isolated) until a response is received. In either case, ITS will work with the department to ensure that the information resource is properly re-secured. If a block (or isolation) has been put in place, it will be removed when the ITS is assured that the information resource is safe.

2.2. Reporting Security and Abuse Incidents

All authorized users are stakeholders and share a measure of responsibility in intrusion detection, prevention, and response.

All users and units have the responsibility to report any discovered unauthorized access attempts or other improper usage of Truman's information resources. If you observe, or have reported to you, a security or abuse problem with any University information resource, including violations of this policy, immediately notify the ITS Service Center at 785-4544 and take immediate steps as minimally necessary to ensure the security and integrity of information resources. The Service Center will notify the appropriate staff who will

coordinate the technical and administrative response to such incidents. ITS leads a Computer Incident Response Team (CIRT), composed of members appointed by the Chief Information Officer. The CIRT team is responsible for the identification, containment, eradication, and recovery of all devices during an incident. CIRT members will work with departments to ensure effective response time and communication. The CIRT is responsible for coordinating evidence gathering and documentation, and for seeking legal and public affairs advice when appropriate, during an incident.

2.3. Investigative contact by law enforcement

Refer the requesting agency to the Office of the General Counsel for guidance regarding appropriate actions to be taken.

EXCLUSIONS OR SPECIAL CIRCUMSTANCES:

CONSEQUENCES:
By failing to abide by this policy or policy procedures, individuals may be subject to sanctions, up to and including the loss of computer or network privileges, disciplinary action, suspension, termination of employment, dismissal from the University, and legal action. Some violations may constitute criminal offenses under local, state, and federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

CONTACTS:

Responsible Executive:	Provost and Vice President for Academic Affairs
Responsible Office:	Information Technology Services
Contact:	Chief Information Officer 111 McClain 660-785-4163
APPROVED BY:	Truman State University President
APPROVED ON:	2013/11/12
EFFECTIVE ON:	2013/11/12
REVIEW/CHANGE HISTORY:	2010/06/06, 2011/02/03, 2013/11/12
REVIEW CYCLE:	Annual

DEFINITIONS:
Authorized use of Truman-owned or operated information resources is use consistent with the education, research, and service mission of the University, and incidental personal use, provided that such use does not interfere with Truman's operations, does not generate incremental identifiable costs to Truman, and does not negatively impact the user's job performance.

Authorized users are (1) current faculty, staff, students, and affiliates of the University and (2) others whose temporary access furthers the mission of the University. Authorized users gain access to University resources through the hiring process, the student admissions process, designation as a University "affiliate", or as a guest or vendor upon approval by a University administrator.

Department includes academic and administrative organizational entities at Truman.

Information resources include any information in electronic, audio-visual, or physical form, or any hardware or software that makes possible the storage, transmission, and use of information. This definition includes but is not limited to electronic mail, voice systems, local databases, externally accessed databases, CD-ROM, motion

picture film, recorded magnetic media, photographs, and digitized information. This also includes any wire, radio, electromagnetic, photo optical, photo electronic, or other facility used in transmitting electronic communications, and any computer facilities or related electronic equipment that electronically store such communications.

Security incidents include any actions that have the potential to pose a serious risk to campus information system resources or the Internet. Examples include, but are not limited to, creating and propagating viruses and/or worms; obtaining or allowing unauthorized access to University resources; deliberate attempts to degrade the performance of a computer system or network; deliberate attempts to deprive authorized personnel of access to any University computer system or network; or otherwise intentionally disrupting services or damaging equipment, software, files, or data.

University affiliates are the people and organizations associated with the University through some form of formalized agreement.

RELATED DOCUMENTS:

Laws:

Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (Title 18 of the U.S. Code)
Electronics Communications Privacy Act of 1986 (PL 99-474)
Computer Security Act of 1987 (PL100-235)
*USA Patriot Act of 200*1

Password Policy
Information Security Incident Response Guideline

KEYWORDS: