PURPOSE
This policy contains requirements and recommendations for all system passwords, including servers, personal machines, and network devices, for the University of Tennessee at Martin. Each user and/or administrator is required to implement the system password definitions listed in this document.

SCOPE
This policy applies to all students, faculty, staff and others (users as defined in Glossary A) while accessing, using, or handling the university’s information technology resources. All users are required to be familiar with and comply with this policy. This policy applies to all applications, operating systems, and network operating systems requiring a user ID and password. Any system that is considered sensitive, vital, or critical or that stores internal use only, proprietary, confidential, or highly confidential information must meet the requirements defined in this policy prior to connection to UT Martin’s infrastructure.

GENERAL POLICY
1. PROTECTION OF PASSWORDS
Passwords must never be written down or recorded. No user should ever share or divulge their password to anyone. Each user is accountable and responsible for any action taken with that user's UserID/username and password. No university employee or administrator should ever ask a user for their password, and if such an action takes place, the user should not reveal it to anyone, no matter how plausible the reason. Any password that is known to be compromised or suspected to be compromised must be changed immediately.

2. PASSWORD SELECTIONS
Users must select passwords that do not contain words generally found in a dictionary. Easy to guess words, such as the university name, product names, the user's proper name or the user's UserID or username, must not be used at any time. Strong passwords should include at least three of the four following characteristics:
• At least one numeric character
• At least one special character (/, [ , - , = , !, $, etc.),
• At least one lower case character
• At least one upper case character.

Passwords issued for temporary IDs, password resets, and locked out IDs, must also conform to this standard. Choose a password that is easy to remember. Mnemonics provide the ability to associate user meaningful data with a password. For example, “one fish two fish red fish blue fish” becomes ()F2f2Fbf. Books and movies provide great passwords, as do phrases such as “I-40 was slow as molasses this morning”, which becomes I40W$aMtM. Examples include:

• May5th#20 – May 5th, 20th wedding anniversary
• MsI#5YOld – My Son is 5 years old
• IhliCf#5yN – I have lived in California for 5 years now
• Fa$t4Ward – Fast Forward
• Great!de@ – Great Idea
• BB#s4034 – Basketball numbers 40 and 34

Passwords issued for automated accounts, system accounts, and other accounts not requiring a regular login must conform to a stricter standard to be determined by the Security Administrator and Campus Security Team.

3. PASSWORD LENGTHS
Each password must be a minimum of eight (8) characters.

4. Password Expiration
All passwords generated within the UT Martin system for access to Internal Use Only or Proprietary information must be set to expire at a maximum of every 180 days. All passwords generated within the University of Tennessee system for access to Confidential information must be set to expire at a maximum of every 60 days. Passwords issued for temporary IDs, password resets, and locked out IDs must all be reset to expire immediately. The recipients of temporary passwords will then be forced to change their passwords at their first login opportunity.

5. PASSWORD ENCRYPTION
For security purposes, passwords used for access to Proprietary or Confidential information will not be sent across the network in 'clear text' format. Passwords used for or access to Proprietary or Confidential information must not be listed in clear text for the purpose of automating a login sequence. All passwords must be stored in an encrypted format by the OS, DBMS, or application.

NOTE: All encryption methods and technology must comply with any international regulations governing this technology.
6. Account Lockouts
An account will be set to 'lock out' a user after a maximum of 5 bad password or login attempts.

7. PASSWORD UNIQUENESS
Where technically feasible, a history of at least ten (10) passwords must be kept within the system for each password generated. This uniqueness forces users to select a password (when generating a new password) that is unique over a longer time period.

8. PASSWORD HACKING
Users must not attempt to "break", "hack", "crack", or otherwise determine another users' password. This applies to passwords for students, faculty, staff, and friends and accounts on systems reached through the Internet.

9. PASSWORD DISPLAY AND PRINTING
The display and printing of passwords must be masked, suppressed, or otherwise obscured such that unauthorized parties will not be able to observe or subsequently recover them.

10. PASSWORD RETRIEVAL
Computer and communication systems must be designed, tested, and controlled to prevent the retrieval of stored passwords, whether they appear in encrypted or plain text form. Electronic or automated means must not be used to record and retrieve a password instead of keying it in through a keyboard when logging on or authenticating a user.

RESPONSIBILITIES
Users are responsible for creating and maintaining their password in accordance with this standard.

System Administrators are responsible for creating and maintaining system passwords in accordance with this standard. System Administrators should also provide guidance to users concerning the implementation of this policy on systems they manage.

REFERENCES TO APPLICABLE UNIVERSITY OF TENNESSEE INFORMATION TECHNOLOGY DOCUMENTS
Information Technology Security Strategy – Defines the basics for information technology security at the University of Tennessee.
IT-0110 Acceptable Use of Information Technology Resources Policy (Pending) – This policy implements the general principles regarding appropriate use of information technology resources.
IT-0115 Information Classification Policy (Pending) – Policy to classify information and govern the use and transmission of such information.
IT-0125 Strong Password Policy (Pending) – University of Tennessee System-wide policy for the creation and handling of passwords.
IT-0130 Access Termination Policy (Pending) – Outlines the process for terminating and restoring access to network devices.
**IT-0135 Host/Server Security Policy (Pending)** – Defines the required components for server setup, physical conditions, and security.

**IT-0140 Network Access Policy (Pending)** – Protects the integrity of and mitigate the risks and losses associated with security vulnerabilities to information technology resources.

**IT-0145 Secure Desktop Policy (Pending)** – Provides rules for security of desktop devices including but not limited to, the requirement for screen saver passwords, not writing passwords down and posting them in places where they can been seen or found, and limited access to the operating system.
APPENDIX A
UNIVERSITY OF TENNESSEE INFORMATION TECHNOLOGY SECURITY
GLOSSARY OF TERMS

Applicable Laws of the State of Tennessee and the Federal Government – Any law in the state of Tennessee or from the federal government that applies to security and information technology, information technology resources, or electronic information transmission technologies.

Applications and Systems Assessment Process – The process by which assigned personnel from the Information Security Office perform vulnerability assessments on information technology resources.

Audit and Consulting Services – The department responsible for proactive reviews of computer systems and services for compliance with information technology security standards and policies, other internal university policies and standards, and the requirements of external regulatory bodies.

Campus/Institute Security Lead – The person assigned by the Campus/Institute Senior Information Technology Officer who is responsible for information technology security for that respective campus.

Campus/Institute Senior Information Technology Officer – The person assigned the duties as the information technology authority for that respective campus or institute. This position is responsible for the creation of procedures, guidelines, best practices, and standards that define the implementation of information technology security policies at the respective campus. The Campus/Institute Senior Information Technology Officers include representation from the following:

- University of Tennessee Knoxville Campus Chief Information Officer
- University of Tennessee Chattanooga Campus Chief Information Officer
- University of Tennessee Martin Campus Chief Information Officer
- University of Tennessee Health Sciences Center Chief Information Officer
- University of Tennessee Space Institute Chief Information Officer
- University of Tennessee Institute of Agriculture Director of Information Technology
- University of Tennessee Institute for Public Service Director of Information Technology

Computer System – An electronic device that uses common storage and executes code for designated data manipulation that is user-written. This includes all portable devices including, but not limited to, laptop computers, personal digital assistants, all mobile email devices, and the associated storage devices.

Contingency planning – Outlines the process of establishing strategies to minimize the effects of a disruption and ensure timely resumption of operations.

Defense in Depth – The creation of layers of security as a mechanism to protect information technology resources.

Electronic Information – Refers to information in electronic form and the computer systems on which the information resides. This does not apply to information in paper form.

Family Educational Rights and Privacy Act (FERPA) – The Family Educational Rights and Privacy Act of 1974, commonly referred to as the Buckley Amendment,
protects the rights of students by controlling the creation, maintenance, and access to educational records. It guarantees students' access to their academic records while prohibiting unauthorized access by others.

**Gramm-Leach-Bliley Act (GLBA)** – Requires financial institutions to protect the confidentiality and integrity of their customer’s information.

**Health Insurance Portability and Accountability Act (HIPAA)** – Creates a standard for healthcare providers and institutions to protect the confidentiality and integrity of personal health information.

**Incident Response** – Is the process where information technology professionals respond to information technology resources compromises, vulnerabilities, and attacks.

**Information Security Office** – The entity that is responsible for the information technology security oversight and administration for the University of Tennessee.

**Information Technology Resources** – Includes any computers, computer systems, network devices, telephony systems, or software applications.

**Information Technology Security Awareness and Education Program** – Provides documentation, information, guidelines, and direction related to information technology security protection methods, principles, and responsibilities for all users of information technology resources.

**Information Technology Security Council (ITSC)** – Provides the direction and guidance for information technology security for the University of Tennessee. This council reviews and approves all polices as related to information technology security that apply to the University of Tennessee.

**Network Infrastructure** – Refers to the architecture in terms of equipment and connections that comprise a network. It includes fixed equipment consisting of wireless transceivers, routers, antennas, switches, cabling, management information systems, and other equipment. This does not include workstations, printers, or file, print, or application servers.

**Office of Public/University Relations** – The office, under the leadership of the Vice president for Public Relations and Government Relations, produces communication vehicles for high profile university initiatives such as student recruitment and alumni relations, while also serving the communication needs of other university departments. In addition the office provides overall public relations coordination for marketing and communications offices at the University of Tennessee at Chattanooga, the University of Tennessee at Martin, the University of Tennessee Health Science Center in Memphis, the Institute of Agriculture, the Institute for Public Service, and the Space Institute.

**System Chief Information Officer** – The person responsible for University of Tennessee’s information technology planning and direction.

**University of Tennessee Policy Committee** – The group responsible for ensuring the consistency of University of Tennessee policies and ensuring that conflicts between polices are resolved.

**Users** – Refers to all students, faculty, staff and others while accessing, using, or handling the University of Tennessee’s information technology resources. “Others” includes, but is not limited to, subcontractors, visitors, visiting scholars, potential students, research associates, grant and contract support personnel, media representatives, guest speakers, and non-university entities granted access.