ALABAMA STATE UNIVERSITY

Office of Technology Services

Policies and Procedures Manual

VP, Diane Alexander

Revised: October 2014
Board Approved: November 2014

ALABAMA STATE UNIVERSITY
Office of Technology Services

POLICIES AND PROCEDURES MANUAL

TABLE OF CONTENTS

ALABAMA STATE UNIVERSITY
Office of Technology Services

Unauthorized Use Policy

Purpose

This policy sets forth the University's policy regarding Unauthorized Use of the University Information Technology Network.

Scope

This policy covers all Unauthorized Use of the University Information Technology Network, and applies to all parties when accessing ASU hardware, software, data or any network related resources. Any person who exceeds the limits of granted authorization permitted by the University is considered an "Unauthorized User".

Policy

All Unauthorized Users are prohibited from using University Information Technology Network for any purpose whatsoever. Authorized Users are prohibited from using the University Information Technology Network in any way that exceeds the limits of their individual authorization.

Enforcement

Unauthorized Users may be subject to criminal prosecution and/or civil suits in which the University seeks damages and/or other legal and/or equitable remedies. Unauthorized Users who are employees of the University may also be subject to disciplinary action, up to and including termination of employment. Unauthorized Users who are Students at the University may also be subject to disciplinary action, up to and including expulsion from the University.

Common Examples of Unauthorized Usage

- Reading another user's files (protected or not)
- Deliberate, unauthorized attempts to access or use ASU computers, systems, or data
- Deliberate, unauthorized use of another user's account or files
- Removing or use of any equipment (hardware, software, data) without authorization
- Copying or attempting to copy data or software (protected or unprotected) without proper authorization
- Interfering with legitimate work of another user (via computer or in person)
- Using computer accounts for work not authorized for that account
- Removal or deletion of software without authorized permission
- Unauthorized attempts to replace ASU owned technology

University Confidentiality Policy

Purpose

Confidential information may be developed or obtained by University employees/interns/work study students as a result of that person's relationship with the University.

Scope

All Authorized Users who have contact with and access to confidential information must keep such information confidential. Confidential information includes, but is not limited to, the following types of information:

- Student and employee information, such as address, telephone number, social security number, birth date and other private information.
- Operations manuals, University practices, marketing plans, techniques and materials, development plans, and financial information
- Student or applicant lists, grades, personnel and payroll records, records regarding vendors and suppliers, records and files of the University, and other information concerning the business affairs or operating practices of the University.

Policy

Confidential information must never be released, removed from the University premises, copied, transmitted, or in any other way used by the Authorized User for any purpose outside the scope of their University employment, nor revealed to non-University employees, without the express written consent of University a member of the Executive Council. Information stored on the University information Technology Network is confidential and may not be distributed outside the University except in the course of the University's business or as otherwise authorized by management personnel. Authorized Users may not remove or borrow from the University premises any computer equipment, disks, or related technology, product or information unless authorized to do so.

Enforcement

Any User found to be in violation of this policy will subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.

Authorized Use Policy

Overview

This policy is intended to protect the University's faculty, employees, Students and employees as well as the University from the consequences of illegal or damaging actions by individuals using the University Information Technology Network. The University Information Technology Network includes: Internet /Intranet/Extranet-related systems, including but not limited to computer/Networking equipment, Software, Operating Systems, storage media, Network accounts providing electronic mail, Instant Messaging, student information system, WWW browsing, and FTP, which are the property of the University. They are to be used for University business purposes and to serve the interests of the University, and as well as all Authorized Users. Effective computer Security is a team effort requiring the participation and support of every University faculty member, employee, student and Authorized User who deals with information and/or information systems. It is the responsibility of every computer user to know the University Information Technology Policies and Procedures, and to comply with the University Information Technology Policies and Procedures.

Purpose

This policy describes the Authorized Use of the University Information Technology Network and protects the University and Authorized Users. Unauthorized uses expose the University to many risks including legal liability, Virus attacks, and the compromise of Network systems, Services, and information.

Scope

This policy applies to all persons with an Alabama State University-owned, third party-owned, or personally-owned computing device that is connected to the University Information Technology Network.

Policy

A. General Use and Ownership

1. Data created by Authorized Users that is on the University Information Technology Network is the property of the University. There is no guarantee that information stored on the University Information Technology Network device will be confidential.
2. Authorized Use includes reasonable personal use of the University Information Technology Network by Authorized Users. University departments are responsible for creating guidelines concerning personal use of the University Information Technology Network. In the absence of such guidelines, employees should consult their supervisor, manager, or the Information
3. Any information that an Authorized User considers to be sensitive or vulnerable should be encrypted. For guidelines on encryption requirements, see Acceptable Encryption Policy.
4. Authorized University employees may monitor the University Information Technology Network traffic at any time, in accordance with the Information Security Audit Policy.
5. The University reserves the right to audit Networks and systems on a periodic basis to ensure compliance with the University Information Technology Policies and Procedures.

B. Security and Proprietary Information.

1. Authorized Users are required to classify the user interface for information contained on the University Information Technology Network as "confidential" or "not confidential," as defined by University Confidentiality Policy. Confidential information includes, but is not limited to: University private data, specifications, student information, and research data. Employees are required to take all necessary steps to prevent unauthorized access to this Sensitive Information.
2. Authorized Users are responsible for the Security of their passwords and accounts and must keep passwords confidential and are not permitted to share accounts.
3. Authorized Users are responsible for logging out of all systems and accounts when they are not being used; they must not be left unattended.
4. All workstations that are part of or connected to the University network must be protected with a protected screensaver with the automatic activation feature set at 15 minutes or less, or by logging-off when the device will be unattended.
5. Encryption of information must be used in compliance with Information Security's Acceptable Encryption Use Policy.
6. Authorized Users are required to exercise special care to protect all mobile devices (i.e. laptop, tablet, smartphone) that are part of or connected to the University Information Technology Network in accordance with the Wireless Communications Policy.
7. Postings by Authorized Users from a University Email address must contain a disclaimer stating that the opinions expressed are strictly those of the author and not necessarily those of the University, unless posting has been done in the course of University business.
8. All computers used by Authorized Users that are connected to the University Information Technology Network, whether owned by the individual or the University, must be continually executing approved Virus-scanning Software with a current Virus Database.
9. Authorized Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain Viruses, e-mail bombs, or Trojan Horse codes.

C. Unacceptable Use of the University Information Technology Network.

The following activities are prohibited, although University employees who are Authorized Users may be exempted from these restrictions during the performance of their legitimate job responsibilities. Under no circumstances is an Authorized User permitted to engage in any activity that is illegal under local, state, federal or international law while utilizing the University Information Technology Network.

D. Unacceptable use includes, but is not limited to the following activities:

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other Intellectual Property, or similar laws or regulations, including, but not limited to, the installation or distribution of copyrighted or other Software products that are not licensed for use by the University.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted

music, and the installation of any copyrighted Software for which the University or the Authorized User does not have an active license is strictly prohibited.

3. Exporting Software, technical information, Encryption Software or technology, in violation of international or regional export control laws, is illegal. University management must be consulted prior to export of any material that is in question.
4. Introduction of Malicious Software into the University Information Technology Network (e.g., Viruses, Worms, Trojan Horses, e-mail bombs, etc.).
5. An Authorized User's revelation of that person's account password to others or allowing use of an Authorized User's account by others, including family and other household members when an Authorized User's computer is connected to the University Information Technology Network from home or other non-University locations.
6. The use of a component of the University Information Technology Network or other computing asset to actively engage in procuring or transmitting material that violates sexual harassment or hostile workplace laws or that violates any University policy. Pornographic material is a violation of sexual harassment policies.
7. Making fraudulent offers of products, items, or services originating from any University account or otherwise made from a computer connected to the University Information Technology Network.
8. Causing Security breaches or disruptions of communication over the University Information Technology Network. Security breaches include, but are not limited to, accessing data or other communications of which the Authorized User is not an intended recipient or logging into an account that the Authorized User is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, Network Sniffing, traffic floods, Packet Spoofing, Denial of Service, etc.
9. Port Scanning or Security Scanning is expressly prohibited unless prior notification to Information Security is made.
10. Executing any form of Network monitoring which will intercept data not intended for the Authorized User is expressly prohibited, unless this activity is a part of the Authorized User's normal job/duty.
11. Circumventing User Authentication or Security of any device, Network, or account.
12. Interfering with or denying Service to any user other than the individual's Host (for example, a Denial of Service attack).
13. Using any Program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, via any means locally or remotely.
14. Providing information about or lists of University employees or Students to non-University parties.

Email and Communications Activities

1. Sending unsolicited Email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (Email SPAM).
2. Any form of harassment via Email, instant messenger, telephone, or pager, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of Email header information.
4. Solicitation of Email for any other Email address, other than that of the Authorized User's own account, with the intent to harass or to collect replies.
5. Creating or forwarding Chain email, Phishing, or other scams of any type.

6. Use of the University's name in any unsolicited Email on behalf of, or to advertise, any service or product without the explicit written permission of the University.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup SPAM).

Enforcement

Any User found to be in violation of this policy will be subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.

ALABAMA STATE UNIVERSITY
Office of Technology Services

Student Privacy Policy

Overview

Alabama State University complies with all of the requirements of the Family Educational Rights and Privacy Act (FERPA). We are committed to protecting the privacy of a student's educational record regardless of delivery method. The Registrar is the point of contact for all FERPA related issues, and all employees are informed and trained of their responsibilities of unauthorized release of confidential records or information. Because an online environment creates a record of student activity, it is subject to FERPA privacy rights, unlike verbal exchanges in a physical classroom.

Scope

This policy applies to any ASU faculty, staff, students, or University affiliates who have contact with and access to confidential student records.

Policy

Identity Verification in Distance Learning Courses

The identity verification process for online courses protects student's privacy through the use of a secure portal, with a secure login and student-selected password.

Faculty Responsibility

Faculty and staff understand and carry out a commitment to confidentiality, integrity, and security to protect the privacy of students who participate in distance learning activities. Students' records are kept private by the instructor, except in cases where academic or administration staff accesses the course, with legitimate educational interest under FERPA guidelines.

In order to maintain course security and protect student privacy, faculty do not access or attempt to access another employee's or student's account without authorization.

In order to maintain confidentiality, portal login passwords are generated by the student and any password reset is completed through "secret question" protocol. It is the student's responsibility to keep their password confidential.
Only work submitted to open forums, like discussion boards, can be accessed by other students; other assignments, grades and correspondence are not viewable by other students.

ALABAMA STATE UNIVERSITY
Office of Technology Services

Workstation Configuration Security Policy

Purpose

The purpose of this policy is to establish standards for the base configuration of workstations that are owned or operated by the University. Effective implementation of this policy will minimize unauthorized access to the University Information Technology Network and other Proprietary Information and technology.

Scope

This policy applies to all University Information Technology Network workstation equipment owned or operated by the University, and to workstations registered under any University-owned internal Network domain.

Policy

Ownership and Responsibilities

All workstations must be registered with and approved by the Office of Technology Services to gain authorized access to the University network. Approved workstation configuration standards must be established and maintained by the University and may only be altered based on business needs. Operational groups are responsible for monitoring configuration compliance in their respective areas and may request exceptions to the established configuration standards.

A Guest User is an Authorized User when utilizing the University's information technology resources in compliance with the University Information Technology Policies and Procedures and as long as the use remains within the limits of the Guest User's individual authorization. The Guest User may be authorized to use computers in the University's computer labs and selected Software. The Guest may also be permitted to selected areas of the University's Information Technology Network. Guest access must be granted by a University official. (I.e. Director of Human Resources, Dean, Chair, Department Head, a member of the Executive Council)

Upon registration of a workstation the following information is required and must be kept current to positively identify the point of contact:

- Workstation contact(s) and a backup contact
- Location of equipment
- Hardware and Operating System (OS) version numbers
- Main functions and applications, if applicable

General Configuration Standards

- OS configuration must be approved by the Office of Technology Services.
- Services and applications that are unused must be disabled where practical. Exceptions must be noted and approved by authorized Information Security personnel.
- Access to Services must be protected through authorized access-control methods (e.g. VPN), if possible.

- The most recent Security Patches must be installed on the system as soon as practicable, the only exception being when immediate application would interfere with business requirements.
- The standard Security principle of Least Required Access (privilege) must be utilized when performing a function.
- If a methodology for Secure Channel connection is available (Le. technically feasible), privileged access must be performed over Secure Channels (e.g. encrypted Network connections using VPN, FTP, etc.)

Monitoring

Security-related events must be reported to the Office of Technology Services. Corrective measures are prescribed as needed. Security-related events include (but are not limited to):

- Port scan attacks
- Evidence of unauthorized access to privileged accounts or data
- Malicious attacks such as hacking, viruses, malware, adware, etc.

Compliance

Internal workstation audits may be performed at any time by OTS personnel. External workstation audits may also be conducted, in accordance with the Audit Policy. Findings not related to a specific operational group will be filtered by OTS personnel, and then presented to the appropriate support staff for remediation or justification.

Enforcement

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.

ALABAMA STATE UNIVERSITY
Office of Technology Services

Email Usage Policy

Overview

This policy addresses internal e-mail, Internet e-mail, and other external e-mail. The policy is based on the expectation that e-mail users will exercise common sense and discretion in the use of e-mail.

Purpose

To establish policies for use of e-mail services for Alabama State University, while protecting University security and assets.

The content of an entire e-mail message, including attachments, is most analogous to a letter or official memo because a record of the contents of the email may be preserved by the sender, recipient, any parties to whom the e-mail may be forwarded, or by the e-mail system itself. It is important also to remember that once an e-mail message is sent, the sender has no control where it may be forwarded. Deleting a message from the user's computer system does not necessarily delete it from the system. Email users are advised that e-mail communications are not subject to personal privacy and may be disclosed pursuant to public disclosure laws and rules of discovery in the event of lawsuits.

Scope

This e-mail policy applies to all Alabama State University e-mail users who are provided access to the Alabama State University e-mail system. Third parties should only be provided access to the University e-mail system as necessary for a business purpose with the University and only if all applicable rules are followed.

A. General E-mail usage Guidelines

- E-mail is to be used to conduct official University business.
- The use of University equipment for personal gain, personal business, commercial advantage, solicitation for any person or non-profit, advocacy of a cause or special interest, political advantage, or any unlawful purpose is prohibited.
- Large attachments (over 25MB) to e-mail messages should be avoided; other means of distribution should be used.
- University wide messages are reserved for officially approved Alabama State University publications. Contact the Media Relations & Public Information department to arrange for distribution of global e-mail messages.
- It is the responsibility of each user to maintain the security of the e-mail system by not leaving computers unattended when the e-mail system is active and by not sharing-passwords.
- Incidental personal use of e-mail which is infrequent or brief in duration is allowed unless the content of the e-mail otherwise violates this policy.
- Use of e-mail for social communications (i.e. Facebook, Instagram, Twitter), which improve organizational effectiveness or serve department goals, is allowed.

B. Privacy Rights and Data Ownership

ASU owns the rights to all University email data sent or received using the University e-mail system or using the University's access to any computer network, to the extent that such rights are not superseded by applicable laws relating to intellectual property. The University also reserves the right to monitor email and their content, as well as any and all use by employees of the Internet and of computer equipment used to create, view, or access e-mail and Internet content. Employees must be aware that the electronic mail messages sent and received using University e-mail or University-provided Internet access, including web-based messaging systems used with such systems or access, are not private and are subject to viewing, downloading, inspection, release, and archiving by University officials at all times. The University has the right to inspect any and all files stored in the University e-mail system to assure compliance with University policies and state and federal laws.

The University uses software in its electronic information systems that allows monitoring by authorized personnel and that creates and stores copies of any messages, files, or other information that is entered into, received by, sent, or viewed on such systems. There is no expectation of privacy in any information or activity conducted, sent, performed, or viewed on or with University equipment or Internet access. Accordingly, employees should assume that whatever they do, type, enter, send, receive, and view on University electronic information systems is electronically stored and subject to inspection, monitoring, evaluation, and University use at any time. Further, employees who use University systems and Internet access to send or receive files or other data that would otherwise be subject to any kind of confidentiality or disclosure privilege thereby waive whatever right they may have to assert such confidentiality or privilege from disclosure. Employees who wish to maintain their right to confidentiality or a disclosure privilege must send or receive such information using some means other than ASU e-mail system or the University-provided Internet access.

Enforcement

Any User found to be in violation of this policy shall have their e-mail privileges revoked and shall be subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.

ALABAMA STATE UNIVERSITY
Office of Technology Services

Password Policy

Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Alabama State University's (ASU) resources. All users, including contractors and vendors with access to ASU systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any ASU facility, has access to the ASU network, or stores any non-public ASU information.

Policy

Password Creation

- All user-level and system-level passwords must conform to the Password Construction Guidelines.
- Users must not use the same password for ASU accounts as for other non-ASU access (e.g. personal ISP account, option trading, benefits, etc).
- Where possible, users must not use the same password for various University access needs.
- User accounts that have system-level privileges granted through group memberships or programs such as sudo or domain administrator must have a unique password from all other accounts held by that user to access system-level privileges.
- Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines.

Password Changes

- All system-level passwords (e.g. Root, enable, NT admin, application administration accounts, etc.) must be changed quarterly.
- All user-level passwords (e.g. Email, web, desktop computer, etc.) must be changed every ninety (90) days.
- Password cracking or guessing may be performed on a periodic or random basis by the Office of Technology Services (OTS) Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

Password Protection

- Passwords must not be shared with anyone. This includes administrative support personnel, managers, co-workers, family member. If additional access or rights must be granted to an ASU employee or affiliate to conduct business contact the Office of Technology Services.
- All passwords are to be treated as sensitive, Confidential ASU information and actions must adhere to the University Confidentiality Policy.
- Passwords must not be written down or stored within your assigned areas.
- Passwords are not to be stored in a computer, phone, or tablet file unless encrypted.
- The "Remember Password" application feature must not be used for any ASU accounts. (e.g. Gmail, Internet Explorer, Google Chrome, etc.)

If an account or password is suspected to be compromised, the incident must be reported to the Office of Technology Services and the password must be changed immediately.

Application Development

Application developers must ensure that their programs contain the following security precautions:

- Applications must support authentication of individual users, not groups.
- Applications must not store passwords in clear text or in any easily reversible form.
- Applications must not transmit passwords in clear text over the network.
- Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access. Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks." A good passphrase is relatively long and contains a combination of upper and lower case letters and numeric and punctuation characters. An example of a good passphrase: "R34d car3fu!!y. B3 h0n3$t."

All of the rules above that apply to passwords apply to passphrases.

Enforcement

Any User found to be in violation of this policy shall have their e-mail privileges revoked and shall be subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.

ALABAMA STATE UNIVERSITY
Office of Technology Services

Password Construction Guidelines

Overview

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or the Alabama State University (ASU) network. These guidelines provide best practices for creating secure passwords.

Purpose

The purpose of construction guidelines is to provide best practices for the creation of strong passwords in order to protect University related data and systems.

Scope

These guidelines apply to employees, contractors, and consultants, temporary and other workers at ASU including all personnel affiliated with third parties. These guidelines apply to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

Statement of Guidelines

The following listing details the characteristics of strong password. All passwords should meet or exceed the following guidelines:

- Contain at least 12 alphanumeric characters. (ASU requires a minimum of 8 alphanumeric characters)
- Contain both upper and lower case letters.
- Contain at least one number.
- Contain at least one special character (e.g.,!$%^&*()_+|~-=\`{}[]:";'<>?,/).

Your password does not meet ASU password security requirements if the password:

- Contains less than eight characters.
- Can be found in a dictionary, including foreign languages, or exists in a language slang, dialect, or jargon.
- Contains personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contains work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contains number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contains common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Contains a variation of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation. ***NOTE:*** *Do not use any examples listed above as this is now public knowledge.*

ALABAMA STATE UNIVERSITY
Office of Technology Services

Guest User Policy

Purpose

The University promotes sharing and learning within the academic community. In doing so, the University often grants to University guests and visitors the right to use its information technology resources in compliance with the University Information Technology Policies and Procedures. Such authorized persons are Guest Users and are also Authorized Users to the extent of their authorization.

Scope

This policy applies only to any Guest Users and does not include faculty, staff, or Students.

Policy

A Guest User is an Authorized User when utilizing the University's information technology resources in compliance with the University Information Technology Policies and Procedures and as long as the use remains within the limits of the Guest User's individual authorization. The Guest User may be authorized to use computers in the University's computer labs and selected Software. The Guests may also be permitted to selected areas of the University's Information Technology Network. Guest access must be granted a University official. (i.e. Director of Human Resources, Dean, Chair, Department Head, a member of the Executive Council)

Enforcement

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.

ALABAMA STATE UNIVERSITY
Office of Technology Services

Acceptable Encryption Policy

Purpose

This policy describes the Authorized Use of the University Information Technology Network and protects the University and Authorized Users. Unauthorized uses expose the University to many risks including legal liability, Virus attacks, and the compromise of Network systems, Services, and information.

Scope

This policy applies to all persons with an Alabama State University-owned, third party-owned, or personally-owned computing device that is connected to the University Information Technology Network.

Policy

Algorithm Requirements

Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalog, or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.

Signature Algorithms

Algorithm	Key Length (min)	Additional Comment
ECDSAP	256	Cisco Legal recommends RFC6090 compliance to avoid patent infringement.
RSA	2048	Must use a secure padding scheme. PKCS#7 padding scheme is recommended. Message hashing required.
LDWM	SHA256	Refer to LDWM Hash-based Signatures Draft

Hash Function Requirements

In general, ASU adheres to the NIST Policy on Hash Functions.

Key Agreement, Authentication & Generation

All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider. End points must be authenticated prior to the exchange or derivation of session keys. Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash. All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider. Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).

Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise. Generation must be seeded from an industry standard random number generator (RNG). For examples, see NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2.

Enforcement

Any User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.

ALABAMA STATE UNIVERSITY
Office of Technology Services

Wireless Communication Policy

Overview

Mobile devices, such as smartphones, tablet computers, laptops and smart devices are important tools for the organization and their use is supported to achieve business goals. However, mobile devices also represent a significant risk to information security and data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorized access to the organization's data and IT infrastructure. This can subsequently lead to data leakage and system infection.

Purpose

The purpose of this policy is to secure and protect the information assets owned by Alabama State University. Alabama State University provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. Alabama State University grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to Alabama State University network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the Office of Technology Services are approved for connectivity to an Alabama State University network.

Scope

All employees, contractors, consultants, temporary and other workers at Alabama State University (ASU) and its subsidiaries must adhere to this Policy. All routers and switches connected to ASU production networks are affected.

Policy

General Requirements

1. Devices must use an OTS approved operating system. Please contact the Service Desk at 334.229.4560 for verification
2. Devices must store all user-saved passwords in an encrypted password store.
3. Devices must be configured with a secure password that complies with Alabama State University's password policy. This password must not be the same as any other credentials used within the organization
4. With the exception of those devices managed by OTS, devices are not allowed to be connected directly to the internal university network.
5. Devices must maintain a hardware address (MAC address) that can be registered and tracked.
6. Devices must not interfere with wireless access deployments maintained by other support organizations. (e.g. Unauthorized routers, Access Points and extenders)

User Requirements

1. Users must only load data essential to their role onto their mobile device(s).
2. Users must report all lost or stolen devices to the Office of Technology Services immediately.
3. If a user suspects that unauthorized access to University data has taken place via a mobile device they user must report the incident devices to the Office of Technology Services immediately.
4. Devices must not be "jailbroken"* or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
5. Users must not load pirated software or illegal content onto their devices.
6. Applications must only be installed from official platform-owner approved sources. Installation of code from un-trusted sources is forbidden. If you are unsure if an application is from an approved source contact Alabama State University Technology Services.
7. Devices must be kept up to date with manufacturer or network provided patches. As a minimum patches should be checked for weekly and applied at least once a month.
8. Devices must not be connected to a PC which does not have up-to-date and enabled antimalware protection and which does not comply with corporate policy.
9. Devices must be encrypted in line with Alabama State University's Acceptable Encryption Policy.
10. Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that university data is only sent through the ASU email system. If a user suspects that university data has been sent from a personal email account, either in body text or as an attachment, they must notify the Office of Technology Services immediately.
11. Users must not use university workstations to backup or synchronize device content such as media files unless such content is required for legitimate business purposes.*To jailbreak a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software.

*To jailbreak a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software.

Enforcement

Any User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.

ALABAMA STATE UNIVERSITY
Office of Technology Services

Wireless Services Procedure

Effective December 1, 2014, Alabama State University will no longer purchase mobile wireless devices or contract with wireless/cellular providers for monthly service; nor will the University provide wireless service for tablets. Those employees who have a documented and approved business requirement for a cellular phone, smartphone and/or mobile hotspot device can utilize the wireless service provider of choice and the University will as appropriate provide a taxable allowance for such service as described below.

1. **Cellular/PDA/Wireless Aircard/Hotspot Service Allowance:**

    a. The amount of monthly allowance is based upon a typical contract necessary to meet institutional expectations for either wireless voice or data services.

    b. The University offers three levels of taxable monthly allowances for wireless plans based on approval:

Approved Usage	Monthly allowance
Data/ Email Capable Phones	$60
Voice and Text Only	$50
Aircard/Hotspot	$40

    c. No additional reimbursement will be provided to those receiving a monthly allowance even if the monthly charges to the employee exceed the allowance amount. However, allowances can be changed at any time should circumstances or expectations change. The Vice President of the appropriate division must approve any allowance adjustments.

2. **Support for Wireless Devices**

    a. All support for wireless devices will be provided by the chosen wireless service company. Alabama State will **not** offer support for individually owned wireless devices. However, Technology Services will provide support, as appropriate, for University provided software that is used on those devices to synchronize them with University calendar and email accounts.

a. Changes to Wireless Service Contracts

    a. The University reserves the right to change or terminate this Procedure regarding allowances for wireless services and equipment. Individuals in receipt of an allowance are personally liable for required deposits, activation fees, monthly charges or termination fees,

regardless of any change in employment status (whether voluntary or involuntary) or any change in this reimbursement Procedure.

b. Notwithstanding the foregoing, if, prior to the end of the cell phone contract period, a University decision (unrelated to employee misconduct) results in the need to end or change the cell phone contract, for example, the employee's supervisor has changed the employee's duties and the cell phone is no longer needed for University purposes. If the employee does not want to retain the current contract, change or cancellation fees will be reimbursed by the University.

b. Procedure

a. All employees with a ***business-related*** requirement for wireless services must complete the "Wireless Allowance Request Form." An allowance may be authorized if at least one of the following three criteria is met:

1. The job function of the employee requires considerable time outside of their assigned office or work area and it is important to the University that they are accessible during those times.
2. The job function of the employee requires them to be accessible via voice and/or e-mail outside of scheduled or normal working hours.
3. The job function requires substantial real-time communication that cannot be reasonably accomplished by other means.

b. The Departmental Director and Divisional Vice President must approve the Wireless Allowance Request Form. Once completed, the signed form must be forwarded to the Office of Human Resources. Once received and processed by the Office Human Resources, a taxable monthly allowance will be added to the employee's first paycheck of each month. The allowance does not constitute an increase to the employee's base pay and will not be included in the calculation on percentage increases to base pay due to annual raises, job upgrades, etc. If the employee's job functions are modified such that the job function no longer meets the above criteria, the allowance shall be terminated immediately.

c. Neither an employee's corporate credit card nor the departmental purchase orders may be used to pay for wireless service charges.

d. Each Departmental Vice President will conduct a fiscal year-end review of wireless allowances to determine if existing cell phone allowances should be continued as-is, changed or discontinued and to determine if any new allowance should be established.

e. A copy of the Wireless Allowance Request and Equipment Reimbursement Request forms and the employee's related cell phone contract must be kept on file at the department. Department files are subject to audit by the internal, external, or the Examiners of Public Accounts upon request.

c. Use of Phone

a. The employee must retain an active cell phone contract as long as a cell phone allowance is in place. Because the cell phone is owned personally by the employee, and the allowance provided is taxable income, the employee may use the phone for both business and personal purposes, as needed. The employee may, at his or her own expense, add extra services or equipment features, as desired.

ALABAMA STATE UNIVERSITY
Office of Technology Services

WIRELESS ALLOWANCE REQUEST FORM

EMPLOYEE INFORMATION
NAME :
ASU ID NUMBER :
TITLE :
REASON FOR ALLOWANCE :

REQUEST INFORMATION		
TYPE	**MONTHLY ALLOWANCE**	**SELECTION**
Email/Data Plan (Smartphone)	$60	☐
Voice & Text only plan	$50	☐
Mobile Hotspot/Data Plan	$40	☐

Annual Allowance:
(Calculate the annualized allowance or pro rata portion for remainder of current fiscal year)

ACCOUNT INFORMATION
ACTIVATE ☐ DEACTIVATE ☐
DEPARTMENT :
ACCOUNT CODE :

EMPLOYEE ACKNOWLEDGEMENT	
I certify that I have read, understand and intend to comply with Alabama State University's "Wireless Services Policy & Procedure". I further certify that I understand that the allowance amount shown above will be added to my paycheck on a monthly basis, it does not represent an increase in my base pay, that appropriate payroll taxes will be withheld, and that the amount of the Allowance will be shown on my year-end W2.	
Employee Signature:	**Date:**

SUPERVISOR ACKNOWLEDGEMENT	
I certify that the requested allowance is needed by the employee for business related purposes. I acknowledge that the amount of the allowance will be taken from the operating budget listed above, and that I have the authority to approve such a budget request I agree to review the need for this allowance at least annually.	
Supervisor's Name*(Print)***:**	**Title:**
Supervisor Signature:	**Date:**

VICE PRESIDENT SIGNATURE	
Vice President Signature:	**Date:**

ALABAMA STATE UNIVERSITY
Office of Technology Services

Remote Access Policy

Purpose

The purpose of this policy is to state the requirements for remote access to computing resources hosted at Alabama State University using remote access technologies.

Motivation

In order to access computing resources hosted at Alabama State University from off-campus, use of ASU remote access services is required. A remote access connection is a secured private network connection built on top of a public network, such as the Internet. Remote access provides a secure, encrypted connection, or tunnel, over the Internet between an individual computer (such as a computer off campus) and a private network (such as ASU's). Use of remote access allows authorized members of the ASU community to securely access ASU network resources as if they were on the campus.

Allowing such connections is not entirely without risk. Remote access connections, by definition, allow an outside computer to connect directly to the University's network. This arrangement provides convenience for the remote worker, but bypasses any firewall restrictions that may be in place. This risk is particularly pronounced for remote access connections from privately owned computers, as the University cannot ensure the computer has sufficient protection configured (e.g. anti-virus, anti-spyware). The risk posed by ASU-owned computers is still present, but to a lesser degree.

Scope

This policy applies to all persons accessing ASU's Network and Systems remotely regardless of relationship with the University.

Responsibilities

The Office of Technology Services is responsible for implementing and maintaining the University's remote access services. Therefore, OTS is also responsible for activities relating to this policy. Accordingly, OTS will manage the configuration of the University's remote access Service.

Policy

ASU employees, and authorized third parties (customers, vendors, etc.) may, under some circumstances, utilize remote access to access ASU computing resources for which they have been granted access.

Regular, full-time ASU faculty or staff employees that have a valid ASU Domain User Account may request remote access to the ASU network by completing a Remote Access Request Form. A letter of justification must accompany the request. The letter should address, in sufficient detail, what resources will be accessed and how they cannot be accessed by conventional means. Requests omitting a letter of justification will be returned to the requestor as incomplete.

Remote access is valid for a set period of time. Requestor should indicate the date remote access should take effect and the date access should expire. Remote access may be granted for a period of up to twelve months, after which remote access for the account will expire. Requestors will be notified via phone or email approximately thirty (30) days before remote access expires. Account holders may resubmit a Remote Access Request Form up to thirty (30) days before the remote access expiration date to continue remote access without disruption.

Guidelines for Access:

- Departmental Accounts shall not be granted remote access due to lack of accountability. These accounts are typically shared among several users and there is no way to trace a specific user back to the account at any given time. See Acceptable Use and Password Policy for more information.
- Temporary Accounts shall not be granted remote access.
- Student accounts shall not be granted remote access.
- Clerical or Support accounts shall not be granted remote access without prior telecommuting approval (VP endorsement required).
- Faculty and Administrative accounts may be granted remote access.
- Vendor Accounts may be granted remote access. Vendor accounts are setup specifically for vendors to access ASU resources for support purposes. Vendor accounts must be sponsored by an ASU employee. The account sponsor bears responsibility for the account and its use by the vendor. If the vendor account does not already exist, a request to establish one must be made at the same time remote access is requested.

All remote access account holders are subject to the Remote Access Terms of Use.

Operational Procedures

ASU currently implements two separate remote access solutions:

- Microsoft Remote Desktop Protocol (RDP)
  - Allows you to log in to your ASU computer from off-campus
  - Requires no software installation
  - Presents a lower security risk
  - Does not expire (subject to periodic review)
- Palo Alto VPN
  - Allows you to connect to the ASU network from off-campus
  - Requires software installation
  - Presents a higher security risk
  - Expires, at minimum, every 12 months

Experience has demonstrated that RDP fulfills the needs of the majority of remote access users.

In order to use remote access, you need a connection to the Internet from your off-campus location. ASU does not provide you with an Internet connection, your Internet Service Provider does. While dialup Internet connections may utilize a remote access connection, performance is very slow and is not recommended or supported.

- Remote access users will be automatically disconnected from the ASU network after 30 minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes to keep the connection open are prohibited.
- Support will only be provided for remote access clients approved by ASU's Office of Information Technology.
- If you have any questions related to the use of ASU remote access, please contact the OTS Service Desk at 334-229-4650 or ots@alasu.edu

Remote Access Terms of Use

Any user found to have violated the terms of use may be subject to loss of privileges or services and other disciplinary action.

1. It is the responsibility of all ASU employees and authorized third parties with remote access privileges to ensure that unauthorized users are not allowed access to internal University networks and associated content.
2. All individuals and machines, including university-owned and personal equipment, are a de facto extension of ASU's network, and as such are subject to the University's Acceptable Use Policy.
3. All computers connected to ASU's internal network via remote access or any other technology must use a properly configured, up-to-date operating system and anti-virus software; this includes all personally-owned computers. Antivirus software may be available for ASU faculty and staff.
4. Redistribution of the ASU remote access installers or associated installation information is prohibited.
5. All network activity during a remote access session is subject to ASU policies.
6. All users of the ASU remote access services shall only utilize resources for which they have been granted permission and rights to use.

Enforcement

Any User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.

ALABAMA STATE UNIVERSITY
Office of Technology Services

Server Security Procedure

Overview

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation procedures ownership and configuration management are all about doing the basics well.

Purpose

The purpose of this procedure is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Alabama State University (ASU). Effective implementation of this procedure will minimize unauthorized access to ASU proprietary information and technology.

Scope

All employees, contractors, consultants, temporary and other workers at ASU and its subsidiaries must adhere to this Procedure. This Procedure applies to server equipment that is owned, operated, or leased by ASU or registered under an ASU-owned internal network domain.

This procedure specifies requirements for equipment on the internal ASU network. For secure configuration of equipment external to ASU on the Demilitarized Zone (DMZ), see the Internet DMZ Equipment Procedure.

Procedure

All internal servers deployed at ASU must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by Office of Technology Services (OTS). Operational groups should monitor configuration compliance and implement an exception Procedure tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by OTS. The following items must be met:

- Servers must be registered with the Office of Technology Services. At a minimum, the following information is required and must be kept up-to-date to positively identify the point of contact:
    - Server contact(s) and location, and a backup contact
    - Hardware and Operating System/Version
    - Main functions and applications, if applicable
- Configuration changes for production servers must follow the appropriate change management procedures

For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic.

Configuration Requirements

- Operating System configuration should be in accordance with approved OTS guidelines.
- Services and applications that will not be used must be disabled where practical.

- Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.
- Always use standard security principles of least required access to perform a function. Do not use "root" when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved. All security related logs will be kept online for a minimum of 1 week.
- Security-related events must be reported to OTS, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port scan attacks
    - Evidence of unauthorized access to privileged accounts or data
    - Malicious attacks such as hacking, viruses, malware, adware, etc.

Enforcement

Any User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.

ALABAMA STATE UNIVERSITY
Office of Technology Services

Physical Security Policy

Overview

Physical Security means providing environmental safeguards for, and controlling physical access to equipment and data on the University Information Technology Network in order to protect information technology resources from Unauthorized Use, in terms of both physical Hardware and data perspectives.

Purpose

The purpose of this policy is to establish standards for granting, monitoring, and terminating physical access to the University Information Technology Network and to protect equipment on the University Information Technology Network from environmental factors.

Scope

This policy applies to the entire University Information Technology Network, including but not limited to computer labs, Network Closets, and the Information Technology Services Network Operations Center.

Policy

Environmental Safeguards

1. Adequate air conditioning must be operational in University Information Technology Network facilities that house information technology resources, to prevent long-term heat damage and equipment failure.
2. All University Information Technology Network facilities must have adequate fire extinguishing devices present in the office area. These devices must be inspected by University Public Safety personnel.
3. All University Information Technology Network information technology resources must be fitted with effective Surge Protectors to prevent power spikes and subsequent damage to data and Hardware.
4. Critical University Information Technology Network information technology resources must each be connected to an Uninterrupted Power Supply (UPS) in order to prevent power spikes, brownouts, and subsequent damage to data and Hardware.
5. Electrical outlets must not be overloaded by connecting too many devices. Proper and practical usage of extension cords are to be reviewed annually.
6. Water sensors must be placed under any raised floor.

Physical Access

1. All University Information Technology Network physical Security systems must comply with all regulations, including, but not limited to, building codes and fire prevention codes.
2. Physical access privileges to all University Information Technology Network facilities must be documented and managed by Information Technology Services.
3. All facilities that house University Information Technology Network information technology resources must be physically protected in proportion to the importance of their function.
4. Access to University Information Technology Network restricted facilities will be granted only to University staff and affiliates whose job responsibilities require access to that facility.
5. The process for granting card or key access to University Information Technology Network facilities must include approval from the Vice President of Technology Services & Innovation.
6. Secured access devices (e.g. access cards, keys, combinations, etc.) must not be shared with or loaned to others by Authorized Users.
7. Secured access devices that are no longer needed must be returned to the Office of Technology Services, and logged appropriately before they are re-allocated to another Authorized User.
8. Lost or stolen University Information Technology Network secured access devices must be reported to OTS personnel immediately.
9. The University Employees responsible for University Information Technology Network facilities must remove the secured access device rights of individuals that no longer require access.
10. University Visitors and other invitees must be escorted and monitored while in restricted University Information Technology Network facilities.
11. University Employees responsible for University Information Technology Network facilities must review access records and visitor Logs for the facility on a periodic basis, and investigate any unusual access.
12. All spaces housing information technology resources must be kept locked when not occupied by a University Employee, in order to reduce the occurrence of unauthorized entry and access.
13. Any piece of University Information Technology Network equipment which resides in a public access area must be secured to a piece of furniture, counter-top, or other suitably deterrent object with a theft-inhibiting device. Portable computers that are part of the University Information Technology Network must also be secured with theft-inhibiting devices.

Enforcement

Any User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.

ALABAMA STATE UNIVERSITY
Office of Technology Services

Internet De-militarized Zone Equipment Procedure

Purpose

The purpose of this procedure is to define standards to be met by all equipment owned and/or operated by Alabama State University (ASU) located outside ASU's Internet firewalls. These standards are designed to minimize the potential exposure to ASU from the loss of sensitive or company confidential data, intellectual property, damage to public image etc., which may follow from unauthorized use of ASU resources.

Devices that are Internet facing and outside the ASU firewall are considered part of the "de-militarized zone" (DMZ) and are subject to this procedure. These devices (network and host) are particularly vulnerable to attack from the Internet since they reside outside the University firewalls.

The procedure defines the following standards:

- Ownership responsibility
- Secure configuration requirements
- Operational requirements
- Change control requirement

Scope

All equipment or devices deployed in a DMZ owned and/or operated by ASU (including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) domain owned by ASU, must follow this procedure.

This procedure also covers any host device outsourced or hosted at external/third-party service providers, if that equipment resides in the "alasu.edu" domain or appears to be owned by ASU.

All new equipment which falls under the scope of this procedure must be configured according to the referenced configuration documents, unless a waiver is obtained from Office of Technology Services (OTS). All existing and future equipment deployed on ASU's un-trusted networks must comply with this procedure.

Procedure

Ownership and Responsibilities

Equipment and applications within the scope of this procedure must be administered by support groups approved by OTS for DMZ system, application, and/or network management.

Support groups will be responsible for the following:

- Equipment must be documented and registered with the Office of Technology Services. At a minimum, the following information is required:
    - Host contacts and location.
    - Hardware and operating system/version.
    - Main functions and applications.
    - Password groups for privileged passwords.

- Network interfaces must have appropriate Domain Name Server (DNS) records (minimum of A and PTR records).
- Password groups must be maintained in accordance with the university wide password management process.
- Immediate access to equipment and system logs must be granted to members of OTS upon demand.
- Changes to existing equipment and deployment of new equipment must follow and corporate governess or change management processes/procedures.

To verify compliance with this procedure, OTS will periodically audit DMZ equipment.

General Configuration Procedure

All equipment must comply with the following configuration procedure:

- Hardware, operating systems, services and applications must be approved by OTS as part of the pre-deployment review phase.
- Operating system configuration must be done according to the secure host and router installation and configuration standards.
- All patches/hot-fixes recommended by the equipment vendor and OTS must be installed. This applies to all services installed, even though those services may be temporarily or permanently disabled. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.
- Services and applications not serving business requirements must be disabled.
- Trust relationships between systems may only be introduced according to business requirements, must be documented, and must be approved by OTS.
- Services and applications not for general access must be restricted by access control lists.
- Insecure services or protocols (as determined by OTS) must be replaced with more secure equivalents whenever such exist.
- Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks. Where a methodology for secure channel connections is not available, one-time passwords must be used for all access levels.
- All host content updates must occur over secure channels.
- Security-related events must be logged and audit trails saved to OTS-approved logs. Security-related events include (but are not limited to) the following:
    - User login failures
    - Failure to obtain privileged access
    - Access procedure violations

OTS will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

New Installations and Change Management Procedures

All new installations and changes to the configuration of existing equipment and applications must follow the following policies/procedures:

- Configuration changes must follow the Change Management Policy.
- OTS must be invited to perform system/application audits prior to the deployment of new services.
- OTS must be engaged, either directly or via change management, to approve all new deployments and configuration changes.

Equipment Outsourced to External Service Providers

The responsibility for the security of the equipment deployed by external service providers must be clarified in the contract with the service provider and corresponding security contacts. Escalation procedures must be documented. Contracting departments are responsible for third party compliance with this procedure.

Enforcement

Any User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.

ALABAMA STATE UNIVERSITY
Office of Technology Services

Router and Switch Security Procedure

Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of Alabama State University.

Scope

All employees, contractors, consultants, temporary and other workers at Alabama State University (ASU) and its subsidiaries must adhere to this Procedure. All routers and switches connected to ASU production networks are affected.

Procedure

Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers and switches must use TACACS+ for all user authentications.
2. The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organization.
3. The following services or features must be disabled:
    a. IP directed broadcasts
    b. Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses
    c. TCP small services
    d. UDP small services
    e. All source routing and switching
    f. All web services running on router
    g. Discovery protocols on Internet connected interfaces
    h. Telnet, FTP, and HTTP services
    i. Auto-configuration
4. The following services should be disabled unless a business justification is provided:
    a. Cisco discovery protocol and other discovery protocols
    b. Dynamic trunking
    c. Scripting environments, such as the TCL shell
5. The following services must be configured:
    a. Password-encryption
    b. NTP configured to a university standard source
6. All routing updates shall be done using secure routing updates.
7. Use University standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.
8. Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.
9. Access control lists for transiting the device are to be added as business needs arise.

10. The router must be registered with the Office of Technology Services with a designated point of contact.
11. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.
12. Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.
13. The University router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:
    a. IP access list accounting
    b. Device logging
    c. Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped
    d. Router console and modem access must be restricted by additional security controls

Enforcement

Any User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.

ALABAMA STATE UNIVERSITY
Office of Technology Services

Security Audit Policy

Overview

The Office of Technology Services utilizes various methods to perform electronic scans of the University's Networks and Firewalls, or any system connected to the University Information Technology Network. The Office of Information Technology is authorized to conduct audits to:

- Ensure integrity, confidentially and availability of information and resources
- Investigate possible Security incidents
- Ensure compliance to ASU's OTS Policies and Procedures documentation.

Scope

This policy covers all computer and communication devices owned or operate by the University. This policy also covers any computer and communications device that are connected to the University Information Technology Network, but which may not be owned or operated by the University.

Policy

Only the Office of Technology Services or other specifically authorized parties may audit devices that are owned by the University or are connected to the University Information Technology Network. Third-party organizations may only perform audits with the explicit written permission of the Office of Technology Services department. OTS personnel shall be granted access to the following in order to effectively perform audits:

- User level or system level access to any computing or communications device
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on the University Information Technology Network
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and Log traffic on the University Information Technology Network

OTS personnel will report all results to the appropriate supervisory personnel and will follow up with the processes necessary to resolve any exceptions.

Enforcement

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.

ALABAMA STATE UNIVERSITY
Office of Technology Services

Change Management Policy

Purpose

This policy describes a systematic process to document and manage changes to the University Information Technology Network in order to permit effective planning by the University Information Technology Services to serve the University use – base.

Scope

This policy applies to all Authorized Users that install, maintain, or operate University information technology resources, including, but not limited to: computer Hardware, Software, and Networking devices.

Policy

Any change to a University Information Technology Network information technology resource is subject to this policy, and must be performed in compliance with the Change Management Policy. All changes affecting University Information Technology Network computer-based environmental facilities, including but not limited to air-conditioning, water, heat, plumbing, electricity, and alarms, must be reported to or coordinated with the Information Technology Services department.

A formal written change request must be submitted to the Information Technology Services department for all changes, both scheduled and unscheduled. All scheduled change requests and supportive documentation must be submitted in compliance with the Change Management Procedure. The request will then be reviewed by the Office of Technology service, and a decision will be made whether to allow or delay the request. The Office of Technology Services may deny a scheduled or unscheduled change for reasons that include, but are not limited to, the following: inadequate planning, inadequate reversion plans, negative impact of change timing on a key business process, or inadequate resource availability.

Customer notification must be completed for each scheduled or unscheduled change, in compliance with the Change Management Policy. A Change Review must be completed for each change to the University Information Technology Network, whether scheduled or unscheduled, successful or not. A Change Management Log must be maintained for all changes. The Log must contain (but is not limited to):

- Date of submission
- Requestor of change
- Date of change
- Implementer of change
- Nature of the change
- Results of the change

Enforcement

Any User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.