

**ADMINISTRATIVE PROCEDURES**

|  |  |
| --- | --- |
| **50.12 Network Security** | **Issued: May 17, 2022** |

1. GOVERNING REGULATIONS

This procedure is governed by the Texas Administrative Code, Title 1, Part 10, [Chapter 202](http://texreg.sos.state.tx.us/public/readtac$ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202), Information Security Standards.

1. DEFINITIONS

2.1 SSID – Service Set Identifier is the name of a wireless local area network (LAN). All wireless devices on a wireless LAN must employ the same SSID in order to communicate with each other.

2.2 Wireless Access – A type of local area network (LAN) that uses high-frequency radio waves rather than wires to communicate between nodes. A wireless LAN spans a relatively small area using one or more of the following technologies to access information resources systems:

a. Wireless local area network – based on the IEEE 802.11 family of standards.

b. Wireless personal area network – based on the Bluetooth and/or infrared technologies.

c. Wireless handheld devices – includes tablets, mobile devices, and smart phones.

1. PURPOSE

The information resource infrastructure at Texas A&M Forest Service continues to expand each year. As the dependence and need for network resources grows, it is important that the network infrastructure, supporting software, and devices be able to meet performance requirements while retaining the level of security required to protect agency information resources and users. This procedure describes the key elements for managing agency network resources.

1. FIREWALLS

Firewalls not only prevent unauthorized access to or from a private network, but are a fundamental element of information systems security infrastructure. Firewalls establish a perimeter where access controls are enforced.

4.1 All agency offices that maintain an active internet connection must maintain a perimeter firewall.

4.2 The procurement, installation, configuration, and modification of firewalls must be coordinated through the Information Resources (IR) Department.

4.3 Perimeter firewalls are configured to allow the following inbound and outbound internet traffic:

a. Allow all outbound or egress traffic to internet services outside of the office with exception of network traffic that violates applicable policy, state and/or federal laws.

b. Block all inbound or ingress traffic from outside the office by default. Some offices may allow inbound traffic from outside the office that supports the mission of TFS. Exceptions to this requirement must be coordinated and approved by the IR Department Head prior to implementation.

4.4 Where the functionality exists, alarms and alert functions as well as audit logging of any and all firewalls and/or other network perimeter access control systems will be enabled.

4.5 Firewalls that are configured to allow inbound traffic from outside the office are subject to auditing and testing to verify the firewall’s configuration, rule set accuracy, and effectiveness on a periodic basis but no less than quarterly. Such testing shall include a controlled penetration test. Web application vulnerability assessments are also conducted on public facing web application servers. Formal reports generated from these tests are delivered to the IR Department Head, and corrections are coordinated by the Systems Administrators or the Client Technologies Analyst, where applicable.

4.6 Most agency computing devices come with a pre-installed software firewall. These firewalls should be enabled and configured with agency specifications.

4.7 Users must not circumvent firewall controls and/or security mechanisms.

5. INTRUSION DETECTION

Intrusion detection plays an important role in implementing and enforcing an organizational security policy. With the proliferation of vulnerabilities introduced by the use of distributed systems, some type of assurance is needed that the systems and network are secure. Intrusion detection systems provide part of that assurance.

5.1 Operating systems, user accounting, and application software audit logging processes are enabled on all host and server systems where resources permit. Logging systems will be allocated with enough storage space to retain logs for a minimum of 90 days.

5.2 Audit logs for servers and applicable hosts are reviewed periodically based on risk management decisions. These logs shall remain protected by administrative access only and may only be reviewed by authorized Information Resources staff.

5.3 Audit logs will retain data about when actions occur on a given system (time and date), the type of event that occurred and on which unique system it took place, the user accounts involved with the event, and the outcome of the event.

5.4 Suspected and/or confirmed instances of successful intrusions should be immediately reported to the IR Department. Information resource users are encouraged to report any anomalies in system performance and/or signs of unusual behavior or activity to the IR Department.

6. NETWORK CONFIGURATION

6.1 The procurement, installation, configuration, and modification of network devices are coordinated through the IR Department.

6.2 Network devices should be configured to deliver at least the desired level of performance while maintaining a secure environment.

6.3 The network topology and standard configuration of Internet Protocol address spacing for agency field offices must comply with the Networking Standards procedure outlined in internal resources.

6.4 Where the functionality exists, the administrative credentials of network devices are changed from the default.

7. SECURITY MONITORING

Security monitoring is a method to confirm that the security practices and controls in place are being adhered to and are effective. Monitoring consists of activities such as review of user account logs, application logs, data backup, and recovery logs.

7.1 Automated tools will provide real-time notification of and appropriate response as necessary to detected wrongdoing and/or vulnerability exploitation. Where possible a security baseline is developed and the tools report exceptions. Areas that these tools will be deployed to monitor include but are not limited to:

a. E-mail traffic

b. Computer software and hardware inventory

c. Operating system security parameters

d. Missing patch status

e. User behavior analysis

f. Data access and sharing

7.2 The following files will be checked, as appropriate, for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:

a. Firewall logs

b. User account logs

c. Network scanning logs

d. System error logs

e. Application logs

f. Data backup and recovery logs

g. IR Help Desk trouble tickets

7.3 Any security issues discovered will be investigated by the IR Department and will be subject to remediation if applicable.

8. WIRELESS ACCESS

The main objective of the wireless network is to provide a network connection that can be used within limited areas; it is not intended to be a replacement for the wired infrastructure.

8.1 The procurement, installation, configuration, and modification of wireless devices must be coordinated through the IR Department.

8.2 Wireless access must be password-protected and encrypted using the latest technology standards.

8.3 The manufacturer default settings of the SSID must be changed upon initial configuration of any wireless access device.

8.4 Wireless security controls must not be bypassed or disabled.

8.5 Additional required configuration information is located in IR Internal Procedures documentation.

CONTACT: [Information Resources Department Head](mailto:cbryan@tfs.tamu.edu), (979) 458-6607