1. GENERAL

The University’s network and telecommunications infrastructure is provided as a central utility for all users of University information resources. It is important that this infrastructure, which includes media (e.g., copper cable, fiber optics), active electronic equipment (i.e., multiplexers, wireless access points, routers, phone switches, etc.), and supporting software be able to meet current performance requirements while retaining the flexibility to allow emerging developments in high speed networking technology and enhanced user services. The purpose of this Procedure is to establish the rules for the secure maintenance, expansion, and use of the network infrastructure.

2. APPLICABILITY

This Procedure applies to all individuals with access to the University’s network or telecommunications infrastructure.

The purpose of the implementation of this Procedure is to provide a set of measures that will mitigate information security risks associated with network infrastructure management. There may also be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee.

Please also refer to Procedure 29.01.03.C2.25 “Exceptions from Risk Mitigation Measures.”

3. DEFINITIONS

Please refer to University Procedure 29.01.03.C2.01 Definitions of common terms. The definitions below apply only to this Procedure.

The network infrastructure – all the University-owned or -managed hardware devices (“infrastructure devices”), media (e.g., fiber optic cables, copper cables), and software that permit the exchange of electronic information between two network nodes. The network infrastructure does not comprise traditional endpoint devices such as phone handsets, workstations, printers, faxes, etc., unless those devices are configured to further extend network connectivity to other devices. The infrastructure includes, but is not limited to:

- All in-wall, above ceiling, or buried voice, data, and video cabling;
- Any network addresses (e.g., IP addresses);
• All devices that retransmit or extend network connectivity, e.g., repeaters, multiplexers, switches, hubs, routers, wireless access points, etc.

4. PROCEDURES

4.1. The IRM shall designate a Custodian (“the network infrastructure Custodian”) for the network infrastructure.

4.2. The network infrastructure Custodian shall manage all developments and enhancements to the network infrastructure.

4.3. Nobody shall make any change to the network infrastructure configuration or to any component of the network infrastructure without the express, prior approval of the network infrastructure Custodian.

4.4. The network infrastructure Custodian shall have the right to undo, without any prior notice, any unapproved changes to the network infrastructure. Such right shall include the disconnection and seizure of unapproved devices connected to the network infrastructure.

4.5. All infrastructure cabling shall be installed and maintained by the network infrastructure Custodian or a contractor approved by the network infrastructure Custodian.

4.6. The network infrastructure Custodian shall maintain the network addresses and name spaces for the network infrastructure and provide a central service for allocation of these resources.

4.7. The network Custodian shall ensure that all University-provided wireless access shall be password protected and that access to that wireless service shall be linked to an individual through authentication mechanisms.

4.8. The network infrastructure Custodian shall ensure that Service Set Identifiers (SSID) values are changed from the manufacturer default setting for wireless local area networks (LAN).

4.8. All users shall ensure that if they send confidential information over any wireless network, either 1) the data itself is encrypted, 2) the link is encrypted (e.g., VPN, HTTPS, Secure FTP), or 3) both the data and link are encrypted.

4.9. The network infrastructure Custodian shall routinely scan for unapproved network devices (e.g., rogue wireless access points).

4.10. Changes to the infrastructure must follow the procedures outlined by University Procedure 29.01.03.C2.06 Change Management, 29.01.03.C2.23 System Development and Acquisition, and any departmental procedures developed and published by IT.
5. CONSEQUENCES FOR VIOLATIONS

All University employees to include staff, tenured and non-tenured faculty, graduate assistants, student workers, interns, guests, volunteers, and probationary, temporary, or wage employees as well as contractors, consultants, and vendors required to adhere to this university procedure may be subject to criminal, civil, or disciplinary actions consistent with federal and state laws, system policies, and university rules.

Individuals found in violation of this University Procedure are subject to loss of access privileges to university information resources (e.g. servers, workstations, email, etc). In addition, contracts associated with contractors, consultants, or vendors are subject to review and possible termination. Any device, system, or software found in violation of this Procedure may be confiscated and temporarily stored by the Information Resources Manager or a representative of the office.

Additional guidance may be found, but is not limited to, the following policies and rules.

- Texas A&M System Policy
  - 01.03 Appointing Power and Terms and Conditions of Employment
  - 07.01 Ethics Policy, TAMUS Employees
  - 32.02 Discipline and Dismissal of Employees
  - 32.02.02 Discipline and Dismissal Procedure for Nonfaculty Employees
  - 33 Employment, Standards of Conduct

- Texas A&M University-Corpus Christi Rule
  - 12.01.99.C3 Faculty Dismissals, Administrative Leave, Non-Reappointments and Terminal Appointments
  - 13.02.99.C1 Student Disciplinary Proceedings

Contact for Interpretation: Information Security Officer

Office of Responsibility: Office of the Associate VP for Information Technology and CIO