1. GENERAL

1.1 Firewalls are a critical component of any information systems security infrastructure. Firewalls prevent unauthorized access to or from a private network (e.g., the University Network) and thus are essential in preventing external attacks on the private network.

1.2 A firewall’s ruleset determines which traffic the firewall will allow or “pass” and which traffic the firewall will deny or “drop.” A firewall’s ruleset typically is changed from time to time in order to e.g., accommodate changing user needs or react to changing security threats.

1.3 Any change to a firewall ruleset comes with risks, e.g., the change will permit new attacks on the private network, or the change will impair the private network users’ abilities to perform legitimate work. Because firewalls are so important to information security, these risks can be significant.

1.4 As such, any changes to a firewall ruleset must be carefully reviewed, thoroughly documented, implemented only by specified personnel, and periodically reviewed by those specified personnel to make sure that the changes are still required. Furthermore, the ongoing operation of a firewall must be carefully monitored, and the physical and remote administrative access to a firewall must be carefully controlled.

2. APPLICABILITY

2.1 This procedure applies to all users of the University Network.

2.2 The purpose of the implementation of this procedure is to provide a set of measures that will mitigate information security risks associated with connectivity between networks, e.g., connectivity between the University Network and the Internet. 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.

2.3 In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this procedure based on
information security risk management decisions and business functions. Such risk management decisions must be documented in the annual security assessment report (See University Rule 29.01.03.C2 Security of Electronic Information Resources).

3. DEFINITIONS

Please refer to University Procedure 29.01.03.C2.01 Definitions.

4. PROCEDURES

4.1. All connectivity between University information resources and the Internet will be provided solely by the Network Services division of the Information Technology Department. Individual divisions, departments, and/or colleges shall not establish independent Internet connectivity without the express prior approval of the Information Resources Manager/Chief Information Officer (“IRM/CIO”).

4.2. Network Services shall ensure that all connectivity between a University information resource and the Internet passes through one or more firewalls (“University Firewall(s)”).

4.3. The default ruleset for any new University Firewall will be to deny all inbound traffic and allow all outbound traffic. Only Network Services shall make changes to the ruleset of a University Firewall. Every change to a University firewall ruleset shall be narrowly tailored, i.e., changes shall apply only to those ports, services, users, hosts, etc., that need the change. Network Services shall make a change to a University Firewall ruleset only pursuant to a written request approved, at a minimum, by the IRM or his/her designee(s). In emergency situations, Network Services may make changes (e.g., blocking of certain types of inbound or outbound traffic) to a University firewall ruleset without a written request or IRM approval. Network Services shall document each and every change made to a University Firewall ruleset. Network Services shall periodically review all University Firewall rulesets to determine whether any changes need to be made or reversed.

4.4. Network Services shall enable alarm, alert, and audit logging functions on all University Firewalls and shall be responsible for the monitoring and analysis of log files generated.

4.5. The Information Security Office (“ISO”) shall conduct periodic audits of University Firewall rulesets, firewall change documentation, and firewall log files. The ISO also shall conduct periodic tests of the University Firewall rulesets via, e.g., a controlled penetration test performed by a third party. The ISO shall distribute the formal reports generated by these periodic tests to Network Services and the IRM/CIO for possible remediation.
4.6. All University Firewalls shall be located in a physically secure location, the access to which shall be controlled by the Information Technology Department.

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 procedure may be subject to criminal, civil, or disciplinary actions consistent with federal and state laws, system policies, and university rules.

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
  - 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 Office

Office of Responsibility: Office of the Associate Vice President for Information Technology