1. GENERAL

Workstations and their software applications present an attractive target to attackers. Because of their greater numbers, workstations tend to be less closely monitored and managed than servers. A poorly secured network workstation poses a risk not only to itself and the data it holds, but also to all other resources on that network. Indeed, the attacker may have no interest in the workstation other than as a stepping stone to a server or other data store. Thus, a network often is only as secure as its most insecure workstation.

As Custodian of the University Network, the University’s Information Technology Department (“IT”) uses centralized tools (e.g., Active Directory, centralized anti-virus) to monitor and manage workstations attached to that network. However, these tools are effective only if each and every attached workstation has these tools installed, and workstation Custodians have clear guidelines on workstation configuration.

This Procedure defines the University’s workstation configuration policy and specifies the responsibilities of various parties in ensuring that all workstations are in compliance with those guidelines.

2. APPLICABILITY

This Procedure applies to all workstations that communicate with the Internet and/or other University information resources via the University Network, all Custodians of those workstations, and all users of those workstations.

The purpose of the implementation of this Procedure is to provide a set of measures that will mitigate information security risks associated with workstations. 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 see Procedure 29.01.03.C2.25 – “Exceptions to Risk Mitigation Measures.”

3. DEFINITIONS

Please refer to University Procedure 29.03.01.C2.01 Definitions for definitions of common terms. The following definitions apply to this document only.
Update refers to a revised version of a software application or operating system that does not involve a major change in functionality. Typically, updates are point releases (e.g., Application X Version 5.2 is an update to Application X Version 5.1).

Upgrade refers to a revised version of a software application or operating system that does involve a major change in functionality. Upgrades are typically full version changes (e.g., Application X Version 5.0 is an upgrade to Application X Version 4.0).

Custodian refers to a person or group that is responsible for the management of any hardware or software component of a workstation. A workstation may have multiple Custodians, e.g., for one machine, IT may manage the hardware, operating system, and core application set, while Distributed IT manages certain departmental applications, and the workstation users manage those applications that they have installed on the workstation. In another scenario, Distributed IT might be responsible for hardware and all installed applications.

Workstation refers to a computing device which can be attached to a network, the resources of which computing device typically are not shared over the network with other network users.

4. PROCEDURES

4.1. IT’s Responsibility to Issue Workstation Configuration Guidelines. IT, in consultation with Distributed IT and other University constituencies, shall issue workstation configuration guidelines for each University network. All workstations connected to a given University network shall comply, where technically feasible, with the workstation configuration guidelines for that network.

4.2. Required Workstation Configuration Guidelines for Internal Networks. Workstation configuration guidelines for a University internal network must contain, at a minimum, the following guidelines:

   a. All operating system patches, service packs, updates, etc. shall be applied, and shall be applied in an amount of time commensurate with the priority of the patch, service pack, update, etc.

   b. All software application patches, service packs, updates, etc. shall be applied, and shall be applied in an amount of time commensurate with the priority of the patch, service pack, update, etc.

   c. Each workstation shall be joined to an Active Directory domain designated by IT where technically feasible.
d. Each workstation will be configured with the security application(s) (e.g., centralized anti-virus, centralized whole-disk encryption) designated by IT for that particular type of workstation.

c. Each workstation shall be named in accordance with the University’s designated workstation naming scheme.

e. Either 1) a list of prohibited software applications and versions (an “application blacklist”) or, 2) a list of allowed software applications and versions (an “application whitelist”).

f. For University-owned workstations, no internal hardware components (e.g., NIC cards, hard drives, video cards) shall be added or removed without the express prior approval of IT or its designees (e.g., Distributed IT).

4.3. Exemptions from the Workstation Configuration Guidelines. Anyone may request an exemption from the workstation configuration guidelines for a given workstation. Such request shall be in writing and shall identify 1) the workstation for which the exemption is requested, 2) the specific workstation configuration guideline that the workstation is to be exempted from, 3) the reason for the exemption, and 4) the duration of the exemption. The request must be approved by both the requester’s unit head (e.g., Dean, Director) and the IRM or his or her designee(s). Approved exemptions must be renewed annually.

4.4. Rights and Responsibilities of Workstation Custodians with Regards to Non-Compliant Workstations. The Custodian(s) of a given workstation shall be responsible for ensuring that the workstation is in compliance with the workstation configuration guidelines applicable to that workstation, and for rectifying any identified non-compliance.

Once a Custodian has notice that a non-exempted workstation under their control is out of compliance with the workstation configuration guidelines (a “non-compliant workstation”), the Custodian shall have a reasonable amount of time to bring the non-compliant workstation back into compliance, which amount of time will depend on the severity of the non-compliance.

4.5. Rights and Responsibilities of IT with Regards to Non-Compliant Workstations. If a non-compliant workstation is not brought back into compliance within a reasonable amount of time, IT may disconnect the non-compliant workstation from the University network. IT will not connect a non-compliant workstation to a University network unless and until that workstation is in compliance with the workstation configuration guidelines.

IT has the right to use automated mechanisms to ensure compliance with
workstation configuration guidelines. In particular, IT has the right to download and install operating system and application upgrades/updates to a workstation, and to force the reboot of that workstation to ensure that the upgrades/updates are applied.

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 disconnected from the University Network.

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