



Gonzaga University Information Technology Policy and Procedure

SUBJECT: Workstation Security

Policy Number	Date Issued	Date Reviewed
IT115		

PURPOSE:

Gonzaga University is committed to ensuring the integrity of its information technology assets from unauthorized, illegal and malicious actions by individuals, intentional or otherwise. The Gonzaga Workstation Security policy is meant to ensure the integrity and security of the desktop computing environment. The security of information technology (IT) resources refers to maintaining the safety, integrity, and privacy of the university’s hardware, software, and information resources.

SCOPE:

This policy applies to all personnel within Gonzaga, including employees of affiliated third-party organizations. This policy applies to all equipment that is owned, leased, operated and maintained, or connected to the Gonzaga University administrative network, including personally owned equipment. Excluded from this policy are the residence hall and courtesy networks.

POLICY:

Gonzaga University workstation users (users) will use workstations in a manner appropriate to the sensitivity of the information contained on university IT assets and will minimize the possibility of unauthorized access to such information.

All persons who engage in use of workstations will have access to IT security policies, procedures, and training on the proper functions to be performed and the manner in which those functions are to be performed, in accordance with established policies and procedures.

Only authorized personnel will access electronic data, including the hardware and/or software on which the data is stored. Users must authenticate prior to use of resources.

Confidential and sensitive data should be stored on centralized server(s).

DEFINITIONS:

Personnel – Could include all faculty, staff, student employees, temporary employees or others.

Privileged access – Account settings that, in general, grant elevated access to resources or services.

Technical Staff - A person who is formally recognized to have a technical support role that, in addition to workstations, may require elevated privileges on servers or networking equipment in order to perform upgrades, relocate equipment, perform hardware or software installations, or make other changes in support of an area of the university.

User – Any person who uses a computer or related service.

Workstation Technician – A person who is formally recognized to have a technical support role that requires elevated privileges on workstations in order to perform upgrades, relocate equipment, perform hardware or software installations, or make other changes in support of a workstation or an area of the university.

PROCEDURE:

User Responsibilities

I. User Access

- a. All users must log out or lock their computers when they leave for the day.
- b. All computers should remain powered on in order to facilitate patching and upgrading computers with minimal impact to users.
- c. Auto lock screen savers will be utilized to lock the workstation after no more than thirty (30) minutes of inactivity.
- d. User access will be granted in accordance with the **Acceptable Use Policy**.
- e. User privileges on the workstation shall be restricted to the minimum necessary level of access for that user to perform their work, this is the default configuration for all users.
- f. Locking workstations does not prevent data loss. It is recommended that users save work frequently and prior to leaving their workstation.

Workstation Administrator and Technical Staff Responsibilities

II. Administrative Access

- a. Where appropriate, workstations shall be configured to use a password protected screen saver that will lock the workstation after no more than thirty (30) minutes of inactivity (IT recommends 10 minutes for personal workstations). Alternatively, auto-logout functionality may be employed where necessary.
- b. The primary administrator account (e.g. Administrator or root) shall not be used when a less privileged account will suffice.
- c. Approval for elevated privileges to a workstation must be conferred by the Workstation Technician for that workstation.
- d. An accounting record of additions, deletions and/or changes to privileged access user accounts must be maintained by the workstation administrator for that workstation.

III. Logging

- a. Workstation logs should be configured and available locally.
- b. Mission critical workstations should mirror logs to a network storage device.

- c. Log content must be configured to record, if possible:
 - Logon events (successful and failed)
 - Security configuration changes
 - Permission change

IV. Securing and Updating Operating Systems

- a. Operating System configuration should be in accordance with industry best practices.
- b. The most recent security patches must be installed in accordance with the Gonzaga University **Vulnerability Remediation policy**.
- c. Antivirus software must be installed and maintained in accordance with the Gonzaga University **Virus Protection and Prevention policy**.

Technical Staff Responsibilities

V. Standard Documentation

- a. The standard workstation installation, configuration, and maintenance processes must be documented by technical staff.
- b. An inventory of workstation's installed applications must be maintained.

VI. Authentication

- a. Authentication processes must be implemented in accordance with Gonzaga Information Technology policies.
- b. All authentication traffic must be secured or encrypted when possible.
- c. Some workstations such as kiosks may be exempted.

VII. Assessments and Audits

- a. As the university requirements change, assessment of the state of workstation security will be conducted by the Security Team according to the rules of the **Risk Assessment Policy** [*in development*].
- b. Audits of the state of workstation security will be conducted by the Security Team in accordance with the **Security Evaluation and Review Policy** [*in development*].

ENFORCEMENT:

Any machine found in violation of this policy may be removed from the network.

Any University personnel found to have violated this policy may be subject to disciplinary action, at the discretion of their supervisor, as described in the university's **Personnel Policies and Procedures Manual**.

For more information regarding workstation security please view policy **ITS120 Physical Access and Security** [*in development*].

Date:	President or Designee