5.2.5 Protection of Information Resources

Chapter 5 - Information Technology	Original Effective Date: June 2000
Section: 5.2 Infrastructure Solutions	Date Last Reviewed: May 2023
Responsible Entity: Vice President and Chief Information Officer	Date Last Revised: November 2009

I. Purpose

To establish the standard use and access of Information Resources of UT Health San Antonio.

II. Scope

This policy applies to all current and former faculty, staff, students, residents, healthcare providers, researchers, contractors, or any other third-party entities who have direct or indirect access to Information Resources created, held, or maintained by UT Health San Antonio or any controlled affiliate, including, but not limited to its clinics, hospitals, and research operations.

III. Policy

Information resources are an asset of UT Health San Antonio (UTHSA). As such, all users must act in a manner appropriate to preserve and protect the University's information resources.

A. Use of Information Resources

As a general rule, the personal use of any UTHSA asset is prohibited. Use of UTHSA information resources is intended to support authorized research, instruction, patient care, and administrative support activities. The incidental use of information resources, such as e-mail and the Internet, is permissible provided that the use complies with all applicable policies and that use does not result in additional cost to UTHSA. Additional guidance is provided in the Handbook of Operating Policies (HOP), Policy 5.8.10, Information Resources Acceptable Use and Security Policy.

B. Access to Information Resources

Access to UTHSA information resources must be managed to ensure users can access only those resources that are appropriate for their function. In general, UTHSA

network domain accounts provide the technology mechanism to implement this policy requirement. Users must use only those accounts which have been specifically authorized for their use. The negligence or naivete of another client in revealing an account name and password is not considered authorized use.

Users are responsible for all use of their domain accounts. They should make appropriate use of system-provided protection features and take precautions against others obtaining access to their accounts. Additional guidance is provided in the HOP, Policy 5.8.4, Access Management.

IV. Definitions

There are no defined terms used in this Policy.

V. Related References

There are no related documents associated with this Policy.

VI. Review and Approval History

A. The approving authority of this policy is the University Executive Committee.

B. The review frequency cycle is set for three years following the last review date, a time period that is not mandated by regulatory, accreditation, or other authority.

Effective Date	Action Taken	Approved By	Date Approved
06/2000	Policy Origination		
11/2009	Policy Revision		
07/2009	Policy Review		
05/2023	Policy Review		