



Electronic Data Backup Policy

Responsible Office: Information Technology Support & Services

Originally Issued: December 2005

Revised: Not applicable

1.0 Introduction

Georgia Health Sciences University maintains a large and growing body of data stored exclusively in electronic form. Much of these data are critical to the operation of the University, and it is clear that the University could suffer significant loss should an important set of data be permanently lost.

2.0 Purpose

The policy is intended to ensure the integrity, availability, and confidentiality of electronically maintained data, including but not limited to confidential, sensitive, or personally identifiable information and that GHSU units are able to resume operation in the event of any incident that causes data loss; equipment failure, inadvertent user error, fire, flood, vandalism, etc..

3.0 Scope

This policy applies to all Georgia Health Sciences University departments, units, and staff that develop, create and/or store critical data in electronic format.

4.0 Policy

In order to protect original business-critical data against loss or destruction, it is strongly recommended that such data shall be created and stored on an ITSS managed data storage device (e.g. storage area network space, a shared or home directory). Every department that establishes or creates electronic data outside of the ITSS storage service shall define, document, and implement a backup procedure, that meets or exceeds the minimum standards found in the ITSS [Implementation Guidelines and Standards for Electronic Data Back Up](#). Department Chairs will assume the role of [resource owner](#) for their department's data and will appoint a data administrator or coordinator.

5.0 Implementation

Details on how to implement this policy are provided in the [Implementation Guidelines and Standards for Electronic Data Back Up](#).

6.0 Related Documents

- [Implementation Guidelines and Standards for Electronic Data Backup](#)
- [Information Systems Security and Computer Usage Policy](#)
- [Information Security Glossary of Terms to Know](#)

This entry was posted in *Administrative, Information Technology Support & Services* and tagged *confidentiality, data loss, electronic data, electronic data backup, information security*. Bookmark the *permalink*. Both comments and trackbacks are currently closed.

INACTIVE