University of Baltimore

III-2.1 Information Technology Security Policy

Revised: 9/15/04
Last Reviewed: 11/16/2020

Rationale:

Innovations in digital technologies have markedly increased the use of information technologies in all facets of university life. As such, information and information systems are increasingly perceived as vital assets, enabling the accomplishment of the University's mission and strategic priorities.

While administrative systems are centrally managed at the University of Baltimore, much of the overall information technology infrastructure is a distributed and shared environment. At the same time, much more administrative and academic information is being stored, accessed, and manipulated electronically, increasing the risk of unauthorized disclosure or modification of personal, proprietary, or institutional data. The University of Baltimore must, therefore, maintain effective security programs to mitigate the risks posed to its information technology resources.

Purpose:

The purpose of this policy is to establish a framework for ensuring that the University's information technology resources are managed securely. These resources include information, information systems, computing platforms, and networks.

Scope:

This security policy applies to all University information resources and all users who access those resources. While the policy applies to all information resources, it especially pertains to University systems that support vital business functions and those that maintain sensitive personal or institutional information.

General Policy:

It is the policy of the University of Baltimore to establish and maintain a security program that enhances and protects the integrity, confidentiality, and availability of information resources as well as promotes compliance with applicable laws. This program will encompass the following elements:

- Risk assessments of information technology resources;
- Access controls to computing environments and information;
- Network security;
- Monitoring, incident response and reporting;
- Media disposal and reuse;
- Backup and recovery;
- Security awareness, education, and training; and
- Organizational responsibilities.

Equally important, the University recognizes its responsibility to promote an open computing environment that allows access to University computing resources to individuals for authorized purposes. The University has

separate policies that add acceptable use of information technology resources; sanctions for the misuse or abuse of university information resources; privacy of electronic information; use of email; disaster recovery; and others. In addition, the Chief Information Officer or designate has the authority to logically isolate a system from accessing University services or the network if warranted.

Related Policy References

1. Email Policy
2. Network Security Policy

Definitions:

Information Technology Resources includes all University-owned devices, applications software, systems software, databases, and peripheral equipment; the data communications infrastructure; the voice communications infrastructure; technologies; communication services and devices, including email, voice modems, smartphones, tablets and multimedia equipment. The components may be stand-alone or networked and may be single-user or multi-user systems.