# University of Baltimore

## III-2.1 Information Technology Security Policy

Revised: 12/18/2025
Last Reviewed: 2/26/2026

**Purpose:**

The purpose of this policy is to protect University Information and Information Resources that must be protected throughout their lifecycle, including when created or collected, stored, transmitted or transferred, and destroyed.

To accomplish this objective, administrative, technical, and physical safeguards must be in place to adequately protect Information Resources, while supporting their use in furthering the University of Baltimore's mission.

**Scope:**

- This policy applies to Information Resources residing in University of Baltimore internal or external environments that store or process University of Baltimore Data.
- This policy and its supporting standards and procedures apply to all Users who use or have access to University of Baltimore Information and Information Resources.
- This policy applies to any Information System or Information Resource that is owned or managed by the University.

**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. The University System of Maryland (USM) IT Security Standards shall serve as the framework for the University of Baltimore's Information Security Program. 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.