Information Technology Standard (IT-1)

Document Title: Standard for IT Security Roles and Responsibilities
Approved By: IT Council
Approval Date: January 29, 2018
Version: 1.1

Introduction
The Board of Regents’ Information Technology policy and Section 12-112 of the Education article of the Maryland Code require that each institution within the University System of Maryland adopt policy that assigns roles and responsibilities with regard to information technology security.

Every member of the university community is responsible for the protection of the electronic data, applications, computer systems, networks, and accounts under their control. Users are expected to exercise the level of care appropriate to the sensitivity of the data stored on university systems and networks.

University Policy X-1.0(A) establishes that those using university information technology resources are responsible for complying with security standards set forth by the Vice President/Chief Information Officer (VP/CIO).

Roles and Responsibilities
All members of the university community play a role in the protection of the university’s data and Information Technology resources. In particular:

- The Vice President/Chief Information Officer, with consultation from the Information Technology Council, is charged with the development and maintenance of university-wide information security standards, the implementation of those standards on university systems, and compliance with those standards. The Division of Information Technology is responsible for the coordination of the university’s Information Security Program which includes deployment of protective measures, incident management and investigation, and promotion of security awareness.

- University Administrators (including Vice Presidents, Deans, Chairs, Directors) within the university are responsible for identifying the resources necessary to coordinate information technology security within their unit. These administrators are responsible for maintaining effective security within their organization. This includes the designation of an IT security contact that shall serve as a conduit for security information between the unit and the Division of Information Technology for purposes such as incident reports.

- Individuals whose duties include network administration, programming, and application or system operation at the university are responsible for implementing measures to minimize the probability of a security incident involving systems and programs under their control. Such measures include the use of malware protection software, installation...
of vendor security updates, adherence with university security standards, and the monitoring of systems to detect anomalous activity. Incidents resulting in the potential or actual compromise of university computing resources or data must be promptly reported to the Security Office in the Division of Information Technology.

- Individual users of the university network including those who access the network remotely are responsible for protecting their workstations, data, accounts, and passwords from unauthorized use and shall comply with the Policy for the Acceptable Use of Information Technology Resources. Incidents resulting in the potential or actual compromise of a user’s computing resources, data, or accounts must be immediately reported to the local department IT group or to the Security Office in the Division of Information Technology.

**Modification**
This standard will be reviewed and updated annually or as needed based on the recommendations of the Vice President/Chief Information Officer.

**History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>March 14, 2007</td>
<td>Initial version</td>
</tr>
<tr>
<td>1.1</td>
<td>January 29, 2018</td>
<td>Replace OIT with DIT; Reference UMD Policy X-1.0(A); Add data and applications as elements to be protected; Add incident reporting to user responsibilities</td>
</tr>
</tbody>
</table>