Information Security Policy

Updated and Effective of: 10/1/2016
Responsible University Officer: Vice-President, Chief Information Officer (VP-CIO)
Policy Owner: Information Security Officer (ISO)

I. Purpose

The University's information assets are essential resources in delivering the University's core mission. These assets include information and data of any kind and in any medium, whether created, acquired, entrusted to, maintained by, or disposed of by the University or others, and any information and communications technology (ICT) equipment (e.g. hardware and operating systems), software, and applications provided by the University or external Third-Party vendors that store, access, process, or transmit the information and data.

It is University policy to reasonably and appropriately protect the confidentiality, integrity and availability of the information assets commensurate with their risk and value while at the same time maintain accessibility.

All members of the University community (Users), are responsible for safeguarding the information assets which they use, access, and interact with, even if they do not have responsibility for managing them, and for complying with this policy.

By implementing this policy the University will:

a. integrate information security principles into all aspect of the University's activities,
b. ensure reasonable security policies, standards, controls, processes, practices, and procedures are established and used to manage information security issues and safeguard the assets,
c. follow a risk-based approach to protect the confidentiality, integrity, and availability of the assets as business needs and the ICT systems change, and that information security activities operate effectively, responsibly, and ethically,
d. comply with all Federal, State, local laws, regulations, University policies, and applicable agreements binding the University,
e. ensure this policy is consistently applied and monitored through the use of a compliance program.
II. Scope

This policy applies to all University information assets, resources, and Users in all locations, both on- and off-campus.

III. Responsibilities

a. The Vice-President, Chief Information Officer (VP-CIO) designates the Information Security Officer (ISO) to be responsible for the development and maintenance of this policy with consultation from the Office of the General Counsel (OGC).

b. The VP-CIO is responsible for approving and ensuring ongoing compliance with this policy with oversight from the Board of Trustees (BoT) Committee on Information Technology Strategy (CITS).

c. The University Leadership Team are responsible for championing this policy and information security practices in their respective Divisions, Schools, and Colleges, and any substantive revisions as recommended by the VP-CIO.

d. The VP-CIO is responsible for ensuring the information assets are secure from unauthorized access (to maintain appropriate confidentiality), unauthorized alterations (to maintain integrity), and available to authorized Users (to maintain availability) enabling the University to meet its mission in an effective and timely manner.

e. The ISO is responsible for establishing and maintaining an information security program aligned to the information asset's risk and value which includes developing, deploying, and maintaining reasonable security policies, processes, practices, procedures, guidelines, and technologies to protect the assets. The ISO will ensure the information security program complies with applicable laws, regulations, and University policies, and that this program and policy, and other related IT security policies, are reviewed and updated as necessary. The ISO will assist with training to support this policy, and ensure that this policy is reviewed and updated as necessary.

f. The ISO coordinates the ITS response to information security incidents, violations, or crimes committed under this policy. The Department of Public Safety is responsible for working with ITS, for conducting investigations, for preparing reports for the appropriate authorities, and providing support to authorities conducting their own investigations.

g. All Users, including Third-Parties entrusted with the University's information, are responsible for being familiar with, and complying with, this policy. All Users have individual and shared responsibilities to protect the confidentiality, integrity, and availability of the information assets in accordance with University policies, Federal, State, and local laws, regulations, and agreements binding the University. Users are required to take information security and awareness training appropriate to their role in support of this policy.

h. Users should understand that the University does not guarantee the privacy of information and should seek further guidance from the ISO if they are unsure of their responsibilities under this policy. The information assets are for University use and must not be used for non-University purposes without prior approval.

i. The OGC will provide legal guidance to this policy.
j. Failure to comply with this policy can result in actions to limit, suspend, or revoke access to the University's network, email, and other information assets. Members of the University community who knowingly violate this policy may be subject to disciplinary actions that include but are not limited to the policies and procedures contained in the Staff Handbook, the Student Handbook (Fogcutter), applicable Collective Bargaining Agreements, and laws which may include civil and criminal prosecution.

IV. See Related Policies

a. Electronic Communications Policy.
b. Technology Acquisition Life Cycle Management Policy.
c. Technology Resources Appropriate Use Policy.