Electronic Communications Policy

Updated and Effective of: 10/1/2016

Responsible University Officer: Vice-President, Chief Information Officer (VP-CIO)

Policy Owner: Associate Vice-President, Information Technology

I. Purpose

The University recognizes the value and benefit of electronic communications (EC). The ability to access and use EC is provided to authorized members of the University community (Users) to enable them to share information and ideas, collaborate, communicate, and perform university business. EC includes the use of such functions and services as email, calendar, text and voice messaging, and University provided telephone service, hereafter collectively referred to as ‘EC services’.

Email is an official means of communication at the University and messages should be managed appropriately in terms of their content whether sent or received (either as a direct recipient or copied). Users are required to comply with normal acceptable standards of professional and personal ethics and conduct, and with the terms of the University's Appropriate Use Policy when using EC services.

While the University takes reasonable measures to protect the privacy and confidentiality of EC, and comply with applicable laws, regulations, and other University policies, the University does not guarantee this. The content of the EC services may be subjected to legal electronic discovery and public release.

By implementing this policy the University will:

a. provide EC services to authorized Users who must use the provided services to conduct all University business,

b. ensure reasonable security policies, standards, controls, processes, practices, and procedures are used to maintain the privacy, confidentiality, integrity and availability of EC services,

c. restrict or deny access to EC services as a result of policy violations, or unacceptable and inappropriate use, and if warranted inspect, monitor, or disclose email, text, and voicemail messages when circumstances indicate such actions are necessary or required by law,

d. comply with all Federal, State, local laws and 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 authorized Users who have a University provided email address (name@usfca.edu), use of University a provided telephone and voicemail, and text messaging, whether used from an on- or off-campus location.

III. Responsibilities

a. The Vice-President, Chief Information Officer (VP-CIO) designates the Associate Vice-President, Information Technology (AVP) 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 EC services and associated 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. The VP-CIO may delegate responsibility for this policy to the AVP.

e. The AVP is responsible for incorporating and maintaining reasonable security processes, practices, procedures, guidelines, and technologies to protect the EC services and assets, and ensure that this policy is reviewed and updated as necessary.

f. The Information Security Officer (ISO) is responsible for establishing and maintaining an information security program to support this policy and coordinate with the AVP on 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. Users have individual and shared responsibilities to protect the confidentiality, integrity, and availability of the EC assets in accordance with University policies, Federal, State, 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 AVP if they are unsure of their responsibilities under this policy.

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 user 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. Information Security Policy.
b. Technology Acquisition Life Cycle Management Policy.
c. Technology Resources Appropriate Use Policy.