Office of the President
University Policy

SUBJECT:	Effective Date:	Policy Number:	
Privacy of Electronic Communications	09-20-16	12.5	
	Supersedes:	**Page**	**Of**
	IRM Tech Policy V-D	1	2
	Responsible Authority: Associate Provost and Chief Information Officer		

APPLICABILITY/ACCOUNTABILITY:

This policy is applicable to all users of University technology resources, including without limitation, telecommunications, networks, email, computing resources and instructional technology resources.

POLICY STATEMENT:

No Expectation of Privacy: Users will be granted appropriate access to all computing resources necessary in conducting University-related business, communications, research and classwork; however, users shall have no expectations of privacy with respect to the use of such resources.

Monitoring or Review of Communications: Communications from University-owned devices, across university network infrastructure, or stored communications on University-owned equipment are subject to review or monitoring for any educational or business reason, including but not limited to the following:

- To protect the University's rights or obligations under law
- To investigate allegations of misconduct or abuse
- To identify potential compromise of university resources
- To monitor communications made by outside or inside attackers
- To investigate or monitor potential performance issues or impacts to University resources
- When it appears reasonably necessary to protect the University from liability arising from the use of University resources
- When it is necessary to do so to protect the safety, integrity, security, or functionality of any component of the University community or its computing resources
- When users have voluntarily made his or her use of these resources accessible to the public by means of a web page, posting to online bulletin boards or newsgroups, or similar display in the public realm

- When an account or device appears to be engaged in unusual or unusually excessive activity
- When it is required by law, specifically including without limitation the Florida Public Records laws and the Federal Electronics Communications Privacy Act.

Any monitoring other than the specified situations described above will be authorized by the University President, Chief Information Officer or designee.

SANCTIONS:

Violations of the university's regulations, policies and/or state or federal laws by an employee or student are grounds for disciplinary action up to and including termination or expulsion in accordance with applicable university and the Florida Board of Governors regulations and/or collective bargaining agreements. Violations by any user shall constitute grounds for terminating his/her use of University technology resources and other appropriate sanctions.

Disciplinary or other action taken by the University does not preclude the possibility of criminal charges, as appropriate. The filing of criminal charges similarly does not preclude action by the University.

RELATED INFORMATION:

Florida Public Records Law; Federal Electronic Communications Privacy Act (ECPA); Acceptable Use of Technology Resources:

INITIATING AUTHORITY: Associate Provost and Chief Information Officer

---

POLICY APPROVAL
(For use by the Office of the President)

Policy Number: 12.5

Initiating Authority
Signature: _____ Date: _____
Name: Jason Ball

Policies and Procedures Review Committee Chair
Signature: _____ Date: _____
Name: Elizabeth Rubin

President
Signature: _____ Date: _____
Name: Dr. John Kelly

Executed signature pages are available in the Office of the General Counsel