FLORIDA	**OFFICIAL**
POLYTECHNIC	**UNIVERSITY**
UNIVERSITY	**POLICY**

Subject/Title: Electronic Communications and Data Transmission
FPU Policy Number: FPU-11.0017P
_X_ New Policy __ Major Revision of Policy __ Minor Technical Revision of Policy
Date First Adopted: August 29, 2015
Date Revised:
Responsible Division/Department: Information Technology Services
Initiating Authority: Tom Hull, Vice President and Chief Information Officer

A. APPLICABILITY/ACCOUNTABILITY:

This policy provides for the security of electronic communications and data transmission and applies to all Users accessing the University network ("Users").

B. POLICY STATEMENT:

For the purposes of this policy, electronic communications, such as e messaging, includes the creation, storage, exchange, and management of text, images, voice, fax , email, and Electronic Data Interchange ("EDI") over a communications network (collectively referred to as "Electronic Communications"). Electronic Communications play an increasingly important role in University communications. Electronic Communications have different risks than paper-based communications so Users must follow best practices when using Electronic Communications. Information contained in Electronic Communications must be appropriately protected by following the security guidelines outlined here.

1. User responsibilities. Users are responsible for practicing secure and appropriate Electronic Communication practices and to ensuring that all forms of Electronic Communication are used in a lawful, ethical and responsible manner. Employee Electronic Communications sent or received for official University business are subject to being accessed, copied, deleted, reviewed or retained by the University as outlined in applicable University policies. The University employees' business related Electronic Communications are subject to Public Records laws, except for limited exceptions, and subject to record retention requirements. User authentication is required to access University email so Users may not share passwords. Users should exercise caution when using instant messaging for file transfers and avoid sending sensitive information in text messages or by cell phone photographs. Users shall not use peer-to-peer file sharing networks for transmission of sensitive or confidential information.

2. Email public record notice. Employee emails sent for University business should contain the following:

   Due to Florida's broad public records law, most written communication to or from University employees is considered a public record. Therefore, the contents of this

email, including personal email addresses, may be subject to disclosure in the event a request is made.

3. Email sent in error message. When using University Information Technology ("IT") resources to send sensitive or confidential information, User should add a message, such as the following to the communication:

   This communication may contain information that is legally protected from unauthorized disclosure. If you are not the intended recipient, please note that any further dissemination, distribution or copying of this communication by you is strictly prohibited. If you have received this message in error, you should notify the sender immediately by telephone or by return email and delete this message from your computer.

4. Redacting sensitive information. Before using any form of Electronic Communication to transmit confidential or sensitive information, employees should take steps to protect confidential or sensitive information: encrypt the transmission; scrub/redact the confidential/sensitive material; or password protect the attached document. If password protected, do not send the password in the same transmission as the protected document. Confirm the email address is correct before sending the message and watch for auto fill errors to prevent an incorrect email address from being supplied by auto fill. Whenever possible, redact personally identifiable information ("PII") (examples listed below); any protected health information ("PHI") as defined under the Health Insurance Portability and Accountability Act ("HIPAA") and any proprietary data or confidential research data. PII includes an individual's first name or first initial and last name when combined with any one of the following:
   a. social security number;
   b. passport number;
   c. alien registration number;
   d. student identification number
   e. military identification number;
   f. credit card number;
   g. bank account number;
   h. medical record;
   i. insurance policy/member account number;
   j. substance abuse and mental health/counseling record; or
   k. user name or email address in combination with a password or security question and answer that would allow access to an online account.

5. PolyAll messages. Users may not transmit mass messages using PolyAll without receiving prior approval from the President/designee or Chief Information Officer.

6. Secure transmission. Users should consult University Information Technology Services for assistance with encryption and digital certificates. Users should follow these best practices to secure messages:

a. When using Internet Services outside those provided by the University, Users must review the general reliability and availability of the Internet service provider and network.
b. Users should review any legal considerations with the University's General Counsel, relating to the requirements for electronic signatures before conducting any transactions involving electronic signature.
c. Users must employ the VPN to access network resources when off campus.
d. Users must update the virus protection for all computing services.

7. Consequences of policy violations. Violations of this policy may lead to suspension of the User's account and or disciplinary action up to and including termination of employment if the violator is an employee, or up to and including expulsion from the University, if the violator is a student. In addition, the University may refer suspected violations of applicable law to the appropriate law enforcement agencies. Unauthorized distribution of copyrighted material, including peer-to-peer file sharing, may subject the User to civil and criminal liabilities.

POLICY APPROVAL

Policy No.: FPU-11.0017P

_____	_____
Initiating Authority	Date
_____	_____
Policies & Procedures Review Committee Chair	Date
_____	_____
President/Designee	Date
Approved by FPU BOT, if required	_____
	Date

EXECUTED SIGNATURE PAGES ARE AVAILABLE IN THE OFFICE OF THE GENERAL COUNSEL