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

Subject/Title: Data Security Plan
FPU Policy Number: FPU-11.00111P
_X_ New Policy __ Major Revision of Policy __ Minor Technical Revision of Policy
Date First Adopted: August 30, 2015
Date Revised:
Responsible Division/Department: Information Technology Services
Initiating Authority: Tom Hull, Vice President and Chief Information Officer

A. APPLICABILITY/ACCOUNTABILITY:

This policy applies University wide to all Users (as defined below) of University Information Technology ("IT") Resources ("Users") whether the User is using the University IT resources on campus or using the University IT Resources from a remote location.

B. POLICY STATEMENT:

The University's Information Security Plan ("Security Plan") establishes procedures to protect the confidentiality, integrity and availability of the University IT Resources. The President or designee is responsible for ensuring that appropriate and auditable security controls are in place on campus. This Security Plan identifies the responsibilities of Users, University Information Technology Services and the Information Security Manager ("ISM") to secure the data contained in and accessed via University IT Resources.

1. <u>User responsibilities for safe computing</u>. Users are expected to exercise due diligence and reasonable care when using University IT Resources and comply with University IT security policies. Users should implement appropriate administrative, technical and physical safeguards to maintain the privacy and security of sensitive confidential data. Users are responsible for keeping all data held or accessed secure in compliance with applicable federal and state laws and regulations as well as contractual obligations related to privacy and security. It is the responsibility of all Users to practice "safe computing" by guarding their passwords, changing passwords regularly and securing all University IT Resources. Although IT ensures the back up of system data every night and maintains a secure server, Users must take steps to prevent unauthorized access and to protect data from damage, loss, alteration, tampering and fraudulent use. These safeguards shall include methods for the storage, retention and disposal of restricted data, subject to state laws governing public records and record retention.

   a. <u>Physical security</u>. Users are responsible for maintaining physical security of data and assets and are required to:

      i. lock or log off of unattended computing devices;

      ii. lock away sensitive or critical business information when leaving the work area;

iii. lock cabinets or rooms that contain critical equipment;
iv. lock doors with limited key distribution;
v. use screen protectors in work areas where screens may be visible to the public or position screens or minimize screens to limit public view;
vi. protect facsimile machines;
vii. use access codes on copiers and scanners;
viii. remove sensitive documents from printers immediately; and
ix. secure computing devices both in and out of the office.

b. Inventory of confidential information. Users accessing, using or transmitting sensitive/confidential information (such as social security numbers, student records, research data) that is not backed up on the University server, must create and maintain an inventory of unknown stores of sensitive/confidential information, identify who has access to the information and provide this information to their respective Vice President and the ISM.

c. E-Commerce. When using University IT Resources for official University business conducted via e-commerce, Users must comply with University procedures for Credit and Debit Card transactions that incorporate Payment Credit Card Industry Data Security Standards.

d. Security for data containing electronic personal identity information. Electronic personal identity information ("PII") (electronically stored personal identity information such as a social security number; date of birth; driver's license number; personal financial information; and individually identifiable insurance information such as the policy or group number) may be collected, stored and accessed only when required for official University business purposes.

e. Computing with mobile devices. Users may store, access or transmit PII on mobile devices (smart phones, tablets, laptops flash drives, CDs, external hard drives), only if there is a business necessity for doing so. Users are responsible for employing best practices to back up and keep the PII secure, including storing the mobile devices in a safe, secure environment in accordance with manufacturer's specifications. Users are strongly encouraged to use encryption when storing sensitive or confidential information/PII on mobile devices. If the device is a University device, when the User no longer needs the device, the User surrenders the device to his/her supervisor who will update the mobile device log. If an office will no longer use the mobile device, the User delivers the device to IT for erasing any PII stored on a device or for disposing of the device, if the device will be no longer be used by the University.

Users that fail to follow University IT policies may face penalties and disciplinary action, including but not limited to termination of employment if the User is an employee, or including but not limited to expulsion if the User is a University student; and/or revocation of User's access to University IT Resources or other legal sanctions.

2. Information Security Manager duties. The Information Security Manager ("ISM") administers the information security program/policies/procedures of the University and:

a. annually reviews and updates the University's information security plan, based on best practices acquired from resources such as Educause, National Institute of Standards (NIST), Information Systems Audit and Control Association (ISACA) or other recognized sources of information security practices and procedures including instituting processes for verifying adherence to the information security plan and associated policies and procedures;

b. institutes processes for verifying adherence to the information security plan and associated policies and procedures including:
    i. conducting training at new employee orientation;
    ii. conducting annual training for updates;
    iii. auditing accounts on a quarterly basis to verify that accounts have been deactivated for Users who no longer need accounts; and
    iv. reviewing quarterly reports prepared by Vice Presidents/designees verifying the level of access for each User.

3. <u>Assigning/terminating User accounts</u>. The University segregates the individual(s) responsible for initiating the assignment/termination of a User's account from the individual in IT who activates and closes a User's accounts. When activating a User account, IT ensures that each User's account is uniquely identifiable and provided to an authenticated User whose capabilities within the account are appropriate to the User's role requirements, responsibilities and specific needs.

a. Employees. Directors and other managers restrict User's access to uses appropriate for the system or service by following the approval process for access and a termination process for when access is no longer appropriate. Human Resources ("HR") initiates the assignment and the termination of an employee's User account by notifying IT when a new employee begins work and by notifying IT when an employee is no longer employed by the University.

b. Students. A new student receives an email notification containing instructions for activation of the User's account.

4. <u>Password controls</u>. Password controls include requiring the use of "strong" passwords that are changed by the User every one hundred eighty days (180) days or more often if necessary. The use of auto logs or "remember me" applications is prohibited except when using non-domain joined computers.

C. DEFINITIONS:

1. **University IT Resources-** encompasses the University Network, technology and telecommunication resources, computing devices, or software including but not limited to computers, laptops, smart phones or other computing devices.
2. **User-** anyone accessing/using the University IT Resources including employees, faculty, staff, students and visitors/vendors given temporary access, whether affiliated with the University or not.

D. PROCEDURES:

1. <u>Risk and self-assessment</u>. IT manages the University's Information Security Plan Risk Management Program, including the risk/self-assessment components. IT audits the use of the University network and IT Resources on a regular and on an as-needed

basis. IT observes activity logs and general usage patterns of activity for intrusion attempts in order to protect the integrity and security of data. Before an individual account is monitored, the appropriate Vice President provides the authorization in consultation with the General Counsel and the CIO and Vice President of Information Technology or designee.

2. Safeguarding information when an employee leaves the University. When an employee terminates employment with the University, the User's supervisor must notify HR immediately and the User's supervisor must collect the employee's keys that allowed the employee access to restricted areas. HR notifies IT of the termination of employment so that IT can terminate the employee's access to electronic data.
3. Physical Security. The ISM, in collaboration with the University Public Safety and Police, reviews physical security measures for all areas having access to sensitive data and or using IT Resources and periodically monitors the operation of motion detectors that enable the tracker video cameras in secured areas.
4. Reporting and Managing Security Incidents. The ISM through University policies and trainings distributes procedures for reporting and handling security incidents or violations and the consequences for violating security policies and procedures. Prior to each employee receiving access to the University network or receiving a University issued computing device, HR provides each employee a statement for the employee to sign acknowledging that the employee has read the University IT policies and procedures and agrees to keep all devices and data secure. The IS web page has contact information for the Helpdesk for urgent email notification of a data breach or security violation using the Security Incident Reporting Form.
5. No retaliation for reporting security violations. The University will not retaliate against any individual or entity that reports a security breach. Retaliation, or otherwise taking adverse action, against any member of the University Community because that individual reported or filed a complaint alleging a security violation, testified or participated in an investigation or proceeding, or opposed a security breach, is strictly prohibited. Individuals violating this provision will be subject to disciplinary and other action up to and including expulsion (for students) or termination (for employees).

POLICY APPROVAL

Policy No.: FPU-11.00111P

______________________________ ____________

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