FLORIDA	OFFICIAL
POLYTECHNIC	UNIVERSITY
UNIVERSITY	POLICY

Subject/Title: Data Classification and Protection
FPU Policy Number: 11.00122P
_X_ New Policy __ Major Revision of Policy __ Minor Technical Revision of Policy
Date First Adopted: April 9, 2020
Responsible Division/Department: Information Technology Services
Initiating Authority: Mark Mroczkowski, CFO

A. APPLICABILITY/ACCOUNTABILITY:

This policy applies to any person accessing or using University information technology (IT) resources. This policy complies with the applicable Board of Governors Regulations 3.0075 Security of Data and Related Information Technology Resources. This policy establishes a framework for classifying University Data based upon its level of sensitivity, value, and criticality to the University and for securing information from risks including, but not limited to unauthorized use, access, disclosure, modification, loss, or deletion.

B. DEFINITIONS:

1. **Affiliate.** For the purpose of these Roles and Responsibilities this is defined as any third-party that has been contracted by the University to provide a set of services and who stores, processes or transmits University Data as part of those services.
2. **Authorize.** Grant permission to access certain resources.
3. **Availability.** Timely and reliable access to and use of information.
4. **Confidentiality.** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
5. **Data.** All data owned or licensed by the University. Alphanumerical or other information represented in either physical form or digital form suitable for electronic processing that are stored on University information technology systems; maintained by a "University official" as defined in FPU-3.001 Confidentiality of Student Records and Applicant Records; or related to institutional processes on- or off-campus.
6. **Integrity.** Guarding against improper modification or destruction of information and ensuring non-repudiation and authenticity.
7. **Personally identifiable information (PII)**. Information that, alone or in combination, is linked or linkable to a specific individual and that would allow a reasonable person in the University community who does not have personal knowledge of the relevant circumstances to identify the individual with reasonable certainty and includes but is not limited to: an individual's name; date of birth; address; email address; student or employee ID number, telephone number; driver's license number or non-driver's identification number; social security number.
8. **Sensitivity.** The required level of protection from unauthorized disclosure, modification, fraud, waste, or abuse due to potential adverse impact on an individual, group, institution, or affiliate. Adverse impact could be financial, legal, or reputational.
9. **User.** Any person accessing or using University IT resources who has access to University Data including, but not limited to, employees, faculty, staff, students,

volunteers, contractors, vendors, and visitors given temporary access, whether affiliated with the University or not.

C. CLASSIFICATION OF DATA:

1. Classification of data determines the baseline security controls the University requires for the data confidentiality, integrity and availability of information assets and systems which are classified according to the risks associated with the data being stored or processed. The University classifies its data as highly restricted, restricted, or unrestricted.

   a. Highly restricted data: Includes any confidential or personal data in any format collected, developed, managed, maintained by or on behalf of the University or within the scope of University activities that could circumvent or undermine other University management controls. Access to highly restricted data is limited to only those Users a legitimate business purpose for accessing this data.

   The unauthorized disclosure, alteration, or destruction of highly restricted data could circumvent or undermine other University management controls, and could cause a significant level of risk to the University or its affiliates, impair the functions of the University, cause significant financial or reputational loss, or lead to likely legal liability; and will generally require notification to affected parties under the guidelines of state and federal breach notification laws.

   Some examples of highly restricted data include without limitation:

   i. User's first name and/or last name in combination with social security number, driver's license or identification card number, passport number, military identification number, financial account number, or other similar number issued on a government document used to verify identity.
   ii. Username and/or email address in combination with a password or security question and answer that would permit access to an online account.
   iii. Data used to authenticate or authorize individuals to use electronic resources, such as encryption keys, biometric data, personal digital certificates, and other electronic tokens.
   iv. Financial account numbers covered by the Payment Card Industry Data Security Standard (PCI-DSS), which controls how credit card information is accepted, used, and stored. PCI-DSS also protects technical configuration information for systems on which such information is stored, such as IP addresses and routing information.

   b. Restricted data: Includes any confidential or personal data in any format collected, developed, managed, maintained by or on behalf of the University or within the scope of University activities that is restricted from disclosure by contract or federal or state laws, rules, or regulations. Access to restricted data is limited to Users who have a legitimate business purpose for accessing this data.

   The unauthorized disclosure, alteration, or destruction of restricted data could cause a significant level of risk to the University or its affiliates, impair the functions of the University, cause significant financial or reputational loss, or lead to likely legal liability;

and will generally require notification to affected parties under the guidelines of state and federal breach notification laws.

Some examples of restricted data include:

i. Protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA), which sets standards for protection of medical records and patient data.
ii. Confidential student and applicant records as defined in FPU-3.001 Confidentiality of Student Records and Applicants Records, including student information subject to the Family Education Rights and Privacy Act (FERPA).
iii. Limited-Access Records as defined in rule 6C13-6.008 Personnel Records and Limited-Access Records such as faculty records that contain information reflecting "academic" evaluations of employee performance.
iv. Research data that is not disclosed in a publication, except when research data is highly restricted
v. Personally Identifiable Information (PII).

c. Unrestricted data. Unrestricted data includes data that does not fall into any of the other information classifications, is a public record as defined under the Florida Public Records law and described in FPU-1.0123P Public Records Policy, or is not protected by law or contract.

Unrestricted data is not presumed to be publicly available and public access may be subject to the processes described in FPU-1.0123P Public Records Policy, or to other relevant University policies or procedures.

The unauthorized disclosure, alteration, or destruction of unrestricted data would result in little or no risk to the University and its affiliates. Unrestricted data is not considered sensitive; however, the integrity of data must still be protected. Users must use moderate controls to protect unrestricted data from unauthorized modification or destruction.

Some examples of unrestricted data include:

i. University course schedules, catalogs descriptions / listings and pre-requisites
ii. Regulations and policies
iii. Research publications
iv. Public websites

D. ROLES AND RESPONSIBILITIES:

Roles and responsibilities are essential to the implementation of the University's Information Security Policy. These roles and responsibilities apply to all "University officials" (as defined in FPU-3.001 Confidentiality of Student Records and Applicant Records) authorized to access University Data.

These roles and responsibilities will be reviewed by the University's Information Security Office every five (5) years or sooner as deemed appropriate based on changes in technology or regulatory

requirements. Individuals who are authorized to access University Data must adhere to the appropriate roles and responsibilities, as defined in documentation approved by the (Committee on Information Systems) COIS and maintained by the Information Security Office. These roles and responsibilities are defined as follows.

1. Committee on Information Systems

The Committee on Information Systems (COIS) is the forum for executive consideration of University-wide computing strategy with authority to oversee information security policy implementation.

The COIS includes members of the senior leadership of the University, the Chief Information Officer (CIO), and the Director of Information Security (DIS). In practice, the COIS is formed when the President's Cabinet meets with the CIO and/or the Director of Information Security to consider subjects within the scope of this policy.

COIS's specific oversight responsibilities related to implementation of this policy include the following:

a. Reviewing and recommending strategies to implement this policy.
b. Analyzing the business impact of proposed strategies on the University.
c. Approving proposed strategies.
d. Reviewing and approving Information Security Policy exceptions.
e. Overseeing maintenance of the data security classification schema and definition of University Data collections.
f. Resolving of data classification or ownership disputes.
g. Defining risk tolerance and accepting or rejecting risk related to security threats that impact the confidentiality, integrity and availability of University Data.
h. Participating as appropriate in any response to unauthorized disclosure, alteration or destruction of highly restricted data.

2. **Director of Information Security (DIS)**

The DIS is a senior-level employee of the University who oversees the University's information security program. Responsibilities of the DIS include the following:

a. Serving as a champion for accepted strategies within respective business units and/or colleges.
b. Collaborating with the University community in data access control and providing oversight, advice, and guidance on information and information technology security policies and standards.
c. Developing and implementing a University-wide information security program.
d. Documenting and disseminating information security policies and procedures.
e. Coordinating the development and implementation of a University-wide information security training and awareness program.
f. Maintaining the data classification schema and identifying University Data collections.
g. Recommending Information Security Policy exceptions.
h. Coordinating a response to actual or suspected breaches in the confidentiality, integrity, or availability of University Data.

3. **Data Security Steward**

A Data Security Steward is a senior-level employee of the University such as a director, department chair, or administrator who oversees the data security of one or more sets of University Data. A Data Security Steward's responsibilities include the following:

a. Assigning an appropriate classification to University Data.
b. Assigning day-to-day administrative and operational security responsibilities for University Data to one or more Data Security Custodians.
c. Approving standards and procedures related to day-to-day administrative and operational security management of University Data.
d. Determining the appropriate criteria for obtaining access to University Data.
e. Ensuring that Data Security Custodians implement reasonable and appropriate security controls to protect the confidentiality, integrity, and availability of University Data.
f. Understanding and approving how University Data is stored, processed and transmitted by the University and by third-party Affiliates of the University.
g. Defining responses to risk to the confidentiality, integrity, and availability of University Data that reduce those risks to an acceptable level.
h. Understanding how University Data is governed by University policies, state and federal regulations, contracts, and other legal binding agreements.

4. **Data Security Custodian**

A Data Security Custodian is an employee of the University who has administrative and/or operational responsibility over University Data. In many cases, there will be multiple Data Security Custodians. An enterprise application may have teams of Data Security Custodians, each responsible for varying functions within their areas of responsibility. A Data Security Custodian is responsible for the following:

a. Understanding and reporting on how University Data is stored, processed, and transmitted by the University and by third-party Affiliates of the University.
b. Implementing appropriate physical and technical safeguards to protect the confidentiality, integrity, and availability of University Data.
c. Documenting and disseminating administrative and operational procedures to ensure consistent storage, processing, and transmission of University Data.
d. Provisioning and deprovisioning access to University Data as authorized by a relevant Data Security Steward.
e. Understanding and reporting on security risks and how they impact the confidentiality, integrity, and availability of University Data.
f. Understanding how University Data is governed by University policies, state and federal regulations, contracts, and other legal binding agreements.

5. **User**

A User is responsible for the following:

a. Adhering to policies, guidelines, and procedures pertaining to the security of University Data.
b. Reporting actual or suspected breaches in the security of University Data to the Information Security Office.

E. GENERAL PROCEDURES:

Users with any level of access to University Data are responsible for that data's security, must meet requirements for privacy and confidentiality, must comply with protection and control procedures, and accurately present the University Data in any type of reporting function.

Highly restricted data:

i. Individuals may access highly restricted data only as required in the course of University duties and must treat highly restricted data as completely confidential.
ii. Highly restricted data must not be discussed or disclosed to others, except as necessary in the course of performing a University function.
iii. The highest level of access and security controls and protection will be applied both in storage and in transit.

Restricted data:

i. Individuals accessing restricted data must access the data only when required to do so for official University business and keep restricted data secure from unauthorized access and alteration.
ii. A high level of access and security controls will be applied to restricted data in order to protect against unauthorized access, modification, transmission, storage, or other use.
iii. The unauthorized disclosure, alteration, or destruction of that data could result in a high level of risk to the University or its affiliates and will generally require notification of affected parties; breach or disclosure of certain restricted data covered by law or regulation may require notification of an appropriate governmental agency.
iv. Unauthorized access to or disclosure of restricted data that are the subject of contractual protections will generally require notification to the contracting party.
v. By default, all information assets that are not explicitly classified as highly restricted or unrestricted data must be treated as restricted data and a high level of security controls must be applied.

F. ADDITIONAL RESOURCES:

Additional resources and guidelines can be found on the policies and procedures page and the Technology Services website.

POLICY APPROVAL

Policy No.: FPU-11.00122P

_____	_____
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