FLORIDA ATLANTIC UNIVERSITY

Office of the President
University Policy

SUBJECT: System and Data Classifications	**Effective Date:** 09-20-16	**Policy Number:** 12.7	
	Supersedes: New	**Page** 1	**Of** 3
	Responsible Authority: Associate Provost and Chief Information Officer		

APPLICABILITY/ACCOUNTABILITY:

This policy applies to all university computing, network, and telecommunications resources or data, whether stored, hosted and/or maintained on university resources or third party servers or sites.

POLICY STATEMENT:

This policy creates standard classifications for computing, network, and telecommunications resources and data to maximize consistent identification in university policies and procedures. Classifications are based upon the impact of the system or data to the university as a whole, and not specifically to the Office of Information Technology (OIT) or other individual university units or departments. The classifications for systems and data are as follows:

I. System Classifications (Computer Systems, Servers, and Infrastructure):

A. *Level 1 System:* Level 1 systems are those systems that, if unavailable, create a significant impairment to the mission or general services of the university. These systems may be classified as critical during certain times, and a lower classification at other times. Level 1 systems include those servers that provide university-wide email services, the university web-presence, learning support for a large number of students, administrative systems such as Banner, Workday, phone systems, or the core network.

B. *Level 2 System*: Level 2 systems are those systems that are generally expected to be available and provide important services to large portions of the campus community but the University may still carry out its primary mission if the systems are not available. Level 2 systems include instructional computers in multimedia classrooms or labs, or university-wide servers that provide behind-the-scenes support for the university.

C. *Level 3 System*: Level 3 systems are those systems utilized by a single department and optionally shared with other departments or units which, if unavailable, create a significant impairment to the functioning of the department or providing important services to end users. Level 3 systems include EMR or EHR systems used by Health-providers, and departmental streaming media servers providing recorded or streamed classroom instruction.

D. *Level 4 System:* Level 4 systems are those systems that are used by a small to moderate number of users and do not represent a significant impairment to the University mission or delivery of instruction by individual departments if they are unavailable. Level 4 systems include most departmental servers and user desktops.

Computer systems and servers may provide multiple services that fit into multiple classifications.

II. Data Classification (Stored or Transmitted Data)

A. *Level 1 Health Information:* Level 1 Health Information is information that the University collects in relation to healthcare treatment or health insurance billing that the University is under an obligation to protect. This information may include Protected Health Information (PHI or ePHI) protected under the Federal Health Insurance Portability and Accountability Act (HIPAA), health information protected by the Florida Information Protection Act (FIPA), or records relating to healthcare functions related to students and covered under the Federal Family Educational Rights and Privacy Act (FERPA).

B. *Level 1 Non-health Information*: Level 1 Non-health Information is highly sensitive information that may be used to open or access financial accounts belonging to another individual. This information includes personal identifiers including Social Security Number, Bank Account Numbers, Passport Numbers, Credit Card Numbers, Driver License Numbers and other information that can be used in conjunction with a person's name to open a financial account.

C. *Level 2 Information*: Level 2 Information is information that the university has an obligation to protect under law or regulatory requirements not included covered in Level 1 Information. This includes, but is not limited to information defined under FERPA, and the Gramm-Leach-Bliley Act (GLBA).

D. *Level 3 Information*: Level 3 information is information that would adversely affect the institution's physical or cyber security if disclosed, but may not necessarily be protected by the University's obligations under law or regulatory requirements. This may include information such as detailed building diagrams, risk assessments, fraud procedures and police procedures.

E. *Level 4 Information*: Level 4 information is any information that is created and stored during the normal course of business that is not protected by law or specific obligations of the university.

Data may fall into multiple classification levels. Such data may include social security numbers included in Level 1 Health Information.

PROCEDURES:

Detailed policies and standards on the storage, transmission, and other protections of University data will be implemented though a committee comprised of the following representatives:

- The Information Security Officer
- The University Compliance Officer
- A manager of the University Enterprise Systems group
- A manager of the University User Support Services group
- A representative from Financial Affairs or applicable ERP Security Group

Additional representatives may be added at the discretion of the Associate Provost and Chief Information Officer. Policies and standards will be made available at the FAU Information Security website at: http://www.fau.edu/security and communicated to OIT and departmental IT staff around the university.

RELATED INFORMATION: Florida Information Protection Act; Federal Educational Rights and Privacy Act (FERPA) Information; Federal Health Insurance Portability and Accountability Act (HIPAA) Information; Federal Gramm-Leach-Bliley Act (GLBA) Information

INITIATING AUTHORITY: Associate Provost and Chief Information Officer

---

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

Policy Number: __12.7___

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