LOS ANGELES PACIFIC UNIVERSITY
Azusa Pacific University System

2018- 2019 Policy & Procedure
Information Technology Information Security

POLICY

Information security is a process to ensure all personal identifiable information (PII) in LAPUs possession is safeguarded.

LAPU establishes and maintains a comprehensive information security program. This includes the administrative, technical, or physical safeguards the school uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information. The safeguards achieve the following objectives:

- Insures the security and confidentiality of customer information
- Protects against any anticipated threats or hazards to the security or integrity of such information, and
- Protects against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer

Federal law requires that an institution must ensure all PII is protected, secured and maintained. This policy is a brief summary of the requirements. For more information please see the Federal Register *16 CFR 313.3(n)* and *16 CFR 314.1-5*, Gramm-Leach-Bliley Act: Sections 501 and 505(b)(2), and U.S. Code: *15 USC 6801(b)*, *6805(b)(2)* and the 2018-2019 Federal Student Aid Handbook, Volume 1, Chapter 1.

PROCEDURE

Designated Coordinators. The school designates an employee or employees to coordinate its information security program.

- **Risk assessment.** The school identifies reasonable foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks. At a minimum, the school's risk assessment includes consideration of risks in each relevant area of operations including:
    - Employee training and management
    - Information systems, including network and software design, as well as information processing, storage, transmission, and disposal
    - Detecting, preventing, and responding to attacks, intrusions, or other systems failures
- **Safeguards testing/monitoring.** The school has implemented information safeguards to control the risks it identifies through risk assessment, and regularly tests or otherwise monitors the effectiveness of the safeguards' key controls, systems, and procedures
- **Evaluation & Adjustment.** The school evaluates and adjusts its information security program in light of the results of the required testing and monitoring, as well as for any material changes to its operations or business arrangements or any other circumstances that it has reason to know may have a material impact on the school's information security program.

Overseeing service providers. The school takes reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue and requires the service providers by contract to implement and maintain such safeguards.