I understand that if I violate any of the above assertions concerning preserving the confidentiality of Pace University data and/or information, I will be subject to appropriate disciplinary action consistent with local, state and federal law, which may include counseling, a warning, probation, unpaid suspension from employment, termination of employment (and enrollment if also a student), and referral to proper law enforcement authorities for prosecution.

Definitions:

Information Technology Systems: *any* university system that contains *Personally Identifiable* or *Confidential University Information* including, but not limited ystems - the- hosted/cloud systems, Banner, Classes LMS (Learning Management System), and/or

Appendix 1: Security of Personally Identifiable Information

Use of Personally Identifiable Information (PII)

Personally Identifiable Information may only be used for the stated legal and/or Pace University business purpose for which it was collected. In addition, PII may not be shared with others and may only be disclosed as authorized by law or with specific consent from the individual from whom it was collected.

PII may only be used in a manner consistent with authorized access and the duties and

except that for which it was collected, and c) follow the guidelines below for the disposal of records. The objective is that private "data at rest", (i.e., "stored private data"), should be stored on a secure server as vetted by the Information Security Officer.

As a general practice, PII ***must not*** be stored on a local workstation or laptop, floppy disk, CD/DVD, PDA, USB flash drive, or other portable storage device. If storing PII on such a device is absolutely necessary for legal or business reasons, ***the information must be encrypted*** and ***the device must be physically secured***.

Computer applications requiring PII must store the information on a secure network server that is physically secure, as well as protected from unauthorized access and against malicious software. Encryption of the data is advised to add another layer of security.

On-site storage: tapes, disks, backups, and other electronic storage devices containing PII must reside in secure physical locations.

Off-site Storage: Any electronic storage media containing PII taken off-site must be protected by encryption.

Documents and forms containing PII should be stored in a restricted access area, such as secure cabinets or a locked desk, and made available on a limited basis.

Anyone working with paper documents that contain PII must take steps to protect the confidentiality of the information: desks and file cabinets should be locked when unattended.

Disposal of PII