Statement for Users, Administrators, and Operators of All Information Technology Systems

Version 2.0 – Dated November 1, 2015

Pace University reserves the right to amend or otherwise revise this document as may be necessary to reflect future changes made to the I.T. environment. You are responsible for reviewing this Policy periodically to ensure your continued compliance with all Pace University I.T. guidelines.

I have been granted access to Pace University's ***Information Technology systems***. In the course of performing my job responsibilities, the systems' access granted to me may enable me to view, input, and edit ***Confidential University information***, and ***Personally Identifiable Information (PII)*** relating to University applicants, students, parents/guardians of applicants/students, alumni, donors, employees, vendors, contractors, affiliated entities and governmental units. Use, transmission, storage and disposal of ***Personally Identifiable Information*** are detailed in **Appendix 1 – Security of Personally Identifiable Information.**

In connection with such access to ***Confidential University information and Personally Identifiable Information***, I understand that I am required to become familiar with and to follow all applicable University policies, procedures and protocols set forth in the University's Employee Handbook, other catalogs and bulletins of the University, University Web pages, and directives issued by Information Technology Services (ITS), as well as the rules and regulations of federal, state, provincial, and local governments, and other appropriate private and public regulatory agencies, regarding ***Confidential University Information*** and ***Personally Identifiable Information***.

Further, because of having been granted such access, I certify to Pace University that in the course of my employment:

1. I will treat all ***Personally Identifiable Information*** on University applicants, students, parents/guardians of applicants/students, alumni, donors, employees, vendors, contractors, affiliated entities and governmental units confidentially. I will only use and/or disclose such information when required to perform my job duties or when legally obligated to do so, and I will only disclose such information to personnel who are authorized to receive it. I will not use ***Personally Identifiable Information*** acquired in the course of my work for personal advantage or share it with unauthorized third parties.

2. I will not use or instruct or enable others to send unencrypted[i] or unsecured[ii] electronic mail, faxes, file transport protocol (ftp), queries or other file copying techniques to transmit ***Confidential University Information*** and ***Personally Identifiable Information*** at Pace University. I will protect paper and/or electronic copies of ***Confidential University Information*** and ***Personally Identifiable Information*** from improper or unintended

disclosure in accordance with the provisions of the Employee Handbook and other pertinent policies. Contact http://help.pace.edu or telephone 914-773-3333 for further information.

3. I will not store or save unencrypted or unsecured ***Confidential University Information*** and ***Personally Identifiable Information*** on local storage devices attached to Laptops, Desktop Computers, local servers, or other devices in the performance of my duties. Instead, I shall make a reasonable effort to redact or mask PII data before storing it on secure server shares maintained by Information Technology Services. Contact http://help.pace.edu or telephone 914-773-3333 for further information.

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 to, "shadow systems" (either "off-the-shelf" or custom developed), Banner, Blackboard, and/or any uploads/downloads to desktop or server based applications from these systems. Administrative information technology systems encompass, on the widest scale, Student Information, Financial Aid, Finance, Human Resources, Philanthropy, Document Imaging, and Facilities Management.

Personally Identifiable Information (PII): includes name and any combination of social security number, credit card numbers, date of birth, passport number, and/or driver's license number.

Confidential University Information: includes information that must be guarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorized access, modification, transmission, storage, or other use.

Questions concerning this or any other Information Technology Services Policy can be directed to http://help.pace.edu.

---

i That is, clear text that, if intercepted by an unintended recipient, could be read and understood.
ii That is, not password protected.

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 responsibilities of the position.
- PII may not be provided to anyone without proper authorization. You may not delegate your authorization/access to to anyone.
- Copies of PII must not be made except as required in the performance of duties.
- PII will be destroyed or disposed of securely when there is no longer a business need to keep the information. Please see Disposal guidelines below.
- PII must not be used for any personal or commercial purposes.
- Any unauthorized access to PII must be reported immediately to the appropriate supervisor.
- Unauthorized use of PII will result in the removal of access privileges and could also result in appropriate administrative action, including, but not limited to, disciplinary and/or legal action.

Transmission of PII

Sending PII over the Internet or by email is prohibited unless it is done in a secure environment. Steps must be taken to protect the confidentiality of fax and paper transmissions containing PII.

- All electronic transactions and transmissions containing PII must be encrypted. All files should be password protected using strong passwords. Ensure that the connection is secure (by use of industry standard security protocols, such as ssl, ssh, sftp). The Pace University ITS HelpDesk (http://help.pace.edu) can provide information on encryption and/or using standard security protocols to transmit PII.
- PII should not be included in email text or attachments unless the attachment is encrypted or password protected environment.
- PII should be removed/redacted from paper forms and faxes unless required by law or determined to be necessary by the appropriate data trustee.
- Fax transmission over telephone lines is secure if appropriate safeguards exist when faxing PII; that is, making sure the recipient's fax number is correct and the fax is not left in an unsecured area. Fax transmissions involving computer networks are not secure and should not include PII.
- When it is determined that PII must be shared with a third party, a written agreement to protect the confidentiality of the PII must be in place.

Storage of Personally Identifiable Information (PII)

Units must actively work to remove PII data from local electronic files, databases, images, and paper documents. Any University office that collects and maintains PII must: a)ensure that it is stored in a secure and confidential environment, b) eliminate the use of the PII for any purpose 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

The following standards should be followed to ensure the secure disposal of information.

- Prior to recycling or disposal, desktop, laptop, and server disks containing PII must be physically destroyed or securely overwritten using the **DOD 5220.22M standard** for overwriting data to make it forensically unrecoverable. The Pace University ITS HelpDesk (http://help.pace.edu) can provide help with this.
- Prior to disposal, steps must be taken to physically destroy or overwrite the information on portable electronic storage devices, including USB drives, disks, CD/DVDs, etc.
- Paper documents must be shredded locally or otherwise disposed of securely.

Questions concerning this or any other Information Technology Policy can be directed to http://help.pace.edu.