Statement for Back Office Users, Administrators and Operators of All Administrative[i] Information Technology Systems

Version 1.9 Draft Dated August 17, 2006
(Under review by Legal Counsel)

Policy
Procedure
Plan
Form

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 Administrative 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***[ii], and ***personally identifiable information***[iii] 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*** known as Social Security Number and Credit Card Information are detailed in **Appendix 1 – Security of Social Security Number and Credit Card 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 the University's Division of Informational Technology (DoIT), 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; that is, 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, instruct or enable others to send unencrypted[iv] or unsecured[v] 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. Contact http://doithelpdesk.pace.edu or telephone 914-773-DOIT for further information.[vi]

3. I will not store or save unencrypted or unsecured ***confidential University information and personally identifiable information*** on local storage devices attached to Personal Digital Assistants (PDAs), Laptops, Desktop Computers, or local servers in the performance of my duties. Instead, I will manipulate such information on secure server shares maintained by the Division of Information Technology. Contact http://doithelpdesk.pace.edu or telephone 914-773-DOIT for further information.[vii]

I understand that if I violate any of the above assertions concerning preserving the confidentiality of Pace University's Administrative Systems 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.

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

Policy No.: P28

This is an official page/publication of Pace University, Division of Information Technology.

[i] These include, but are not limited to, legacy mainframe applications, "shadow systems" (either "off-the-shelf" or custom developed), Project SPARTA systems, and 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.

[ii] (including, but not limited to, University business plans and financial information)

[iii] (including, but not limited to, dates/places of birth, social security numbers, credit card information, maiden names, home addresses and home/personal cell phone numbers)

[iv] That is, clear text that, if intercepted by an unintended recipient, could be read and understood. As versus encrypted, or "encoded", requiring a key to decode.

[v] That is, not password protected. Passwords in Microsoft Office, for example, give a minimum level of security (but are better than nothing).

[vi] The Division of Information Technology is investigating numerous technologies for encrypting and securing electronic transmissions, if users deem essential to their business practices. For now, we recommend uploading to our secure storage site and pointing intended recipients there via email.

[vii] The Division of Information Technology recommends that users store confidential information on our secure storage site.

Appendix 1
Security of Personally Identifiable Information Known as Social Security Number and Credit Card Information

Version 1.9 Draft Dated August 17, 2006

Policy
Procedure
Plan
Form

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.

Use of Social Security Number and/or Credit Card Information

Social Security Number (SSN) and Credit Card Information data may only be used for the stated legal and/or Pace University business purpose for which it was collected. In addition, Social Security Number and Credit Card Information data 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.

- The Social Security Number and Credit Card Information may only be used in a manner consistent with authorized access and the duties and responsibilities of the position.
- The Social Security Number and Credit Card Information may not be provided to anyone without proper authorization. You may not delegate your authorization/access to Social Security Number and Credit Card Information data to anyone.
- Copies of Social Security Number and Credit Card Information data or records will not be made except as required in the performance of duties.
- Social Security Number and Credit Card Information data for which there is no longer a business need will be destroyed or disposed of securely. Please see Disposal guidelines below.
- Social Security Number and Credit Card Information data will not be used for any personal or commercial purposes.
- Any unauthorized access to Social Security Number and Credit Card Information data will be reported immediately to the appropriate supervisor.
- Unauthorized use of Social Security Number and Credit Card Information data 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 Social Security Number and/or Credit Card Information

Sending Social Security Number and Credit Card Information over the Internet or by email is prohibited unless it is done in a secure environment, and steps must be taken to protect the confidentiality of fax and paper transmissions containing Social Security Number and Credit Card Information.

- All electronic transactions and transmissions containing Social Security Number and Credit Card Information must encrypt the confidential information, password protect the file using strong passwords and ensure that the connection is secure (by use of industry standard security protocols, such as ssl, ssh, sftp). The Pace University DoIT HelpDesk (http://doithelpdesk.pace.edu) can provide information on encryption and/or using standard security protocols to transmit Social Security Number and Credit Card Information.
- Social Security Number and Credit Card Information should not be included in email text or attachments unless the attachment is encrypted or password protected environment.
- Social Security Number and Credit Card Information should be removed from paper forms and faxes unless required by law or determined to be necessary by the appropriate data trustee.
- When Social Security Number and Credit Card Information is exchanged on paper, steps must be taken so the number is not revealed. For example, Social Security Number and Credit Card Information must not appear in an envelope window.
- Fax transmission over telephone lines is secure if appropriate safeguards exist when faxing Social Security Number and Credit Card Information; 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 Social Security Number and Credit Card Information.
- When it is determined that Social Security Number and Credit Card Information must be shared with a third party, a written agreement to protect the confidentiality of the SSN Social Security Number and Credit Card Information must be in place.

Storage of Social Security Number and/or Credit Card Information

Units must actively work to remove Social Security Number and Credit Card Information data from local electronic files, databases, images, and paper documents. Any University office that collects and maintains an individual's Social Security Number and Credit Card Information must ensure that the Social Security Number and Credit Card Information is stored in a secure and confidential environment, eliminate use of the Social Security Number and Credit Card Information for any purpose except that for which it was collected, and follow the guidelines below for the disposal of records containing the Social Security Number and Credit Card Information. The objective is that private "data at rest", i.e., "stored private data", should be encrypted unless it has been password protected using strong passwords, transmitted and stored on a secure server as vetted by the Chief Information Security Officer.

- As a general practice, Social Security Number and Credit Card Information ***may not*** be stored on a local workstation or laptop, or on a floppy disk, CD/DVD, PDA, USB flash drive, or other portable storage device. Several recent information security incidents at universities have involved the theft of such devices containing Social Security Number and Credit Card Information. If storing Social Security Number and Credit Card Information 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 the Social Security Number and Credit Card Information must store the Social Security Number and Credit Card Information on a secure network

server that is physically secure (in a secure environment), 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 must reside in secure physical locations.
- Off-site Storage: Any electronic storage media containing Social Security Number and Credit Card Information taken off-site must be protected by encryption.
- Documents and forms containing Social Security Number and Credit Card Information should be stored in a restricted access area, such as secure cabinets or a locked desk, available on a limited basis.
- Anyone working with paper documents that contain Social Security Number and Credit Card Information must take steps to protect the confidentiality of the information: desks and file cabinets containing Social Security Number and Credit Card Information data should be locked when unattended.

Disposal of Social Security Number and/or Credit Card Information

As a Social Security Number is replaced by a University ID (UID) Number as the common key and eliminated from the routine course of business, units will need to follow standards for secure disposal.

- Prior to recycling or disposal, desktop, laptop, and server disks containing Social Security Number and Credit Card Information must be physically destroyed or securely overwritten using the **DOD 5220.22M standard** for overwriting data to make it forensically unrecoverable. The Pace University DoIT HelpDesk (http://doithelpdesk.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. containing Social Security Number and Credit Card Information
- Paper documents containing Social Security Number and Credit Card Information must be shredded locally or otherwise disposed of securely.

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