5. As a general rule, do not store PNPI locally.

- ❑ The two greatest threats to the security of PNPI are an unsecured, non-password-protected or compromised computer and paper documents containing PNPI.
- ❑ Make sure that your computer is protected with a strong password.
- ❑ Whenever possible, use the central systems (CAS, HR, and SIS) to retrieve or process PNPI. Those systems provide secure storage.
- ❑ When disposing of PNPI data, shred paper copies, delete e-mail, and remove SSNs and other PNPI data from any computer files.
- ❑ Faculty and staff must delete SSNs from all roster and grade information downloaded to a personal computer.
- ❑ Encrypt grade information stored on faculty or staff computers.
- ❑ If your department needs to store PNPI locally, contact the IT Help Center (x6000) to arrange an appointment to discuss your needs.

6. Take your personal responsibility seriously.

- ❑ The secure handling of PNPI is a critical part of every employee's responsibility.
- ❑ Some transactions related to government agencies, medical records, admissions, employment, and financial aid require the acquisition of PNPI. However, it is the personal responsibility of each employee who handles these transactions to secure that information.
- ❑ Every employee must discuss his or her PNPI responsibilities with his or her supervisor at least once a year.

7. Review your department's PNPI practices annually.

- ❑ Each year, every department and unit on campus must review its procedures for processing PNPI, PNPI retrieval practices, and PNPI retention practices.

Protecting Personal Non-Public Information (PNPI)

UNIVERSITY DEPARTMENTS MUST ACT

- Any information that uniquely identifies a person and provides confidential information about that individual or that can be used to acquire such confidential information is considered Personal Non-Public Information (PNPI).
- State and Federal laws and regulations govern the safeguarding of PNPI.
- All University of Delaware departments must reduce their reliance on Social Security Numbers (SSNs) and use alternative forms of identification whenever possible.
- All University employees must follow good practices in safeguarding all PNPI.
- Each department must re-examine its use of PNPI, including its practices for retaining or storing this sensitive information.
- Annually, each department must review all processes that use or require access to PNPI.
- For more information, visit http://www.udel.edu/pnpi

University Guidelines for Protecting Personal Non-Public Information

Examples of PNPI include, but are not limited to

- Social Security Numbers (SSNs);
- Credit card and bank account numbers;
- Medical, financial or educational records;
- Grades used in context with personally identifiable information;
- Other sensitive, confidential or protected data.

Published information and public records (e.g., telephone or address directories) are not considered PNPI.

Follow these University of Delaware guidelines for safeguarding PNPI.

1. Do not collect and store PNPI unless doing so is an essential or required element of your job.

2. Seek out old documents, electronic and paper, that contain PNPI.

- ❑ Destroy documents or remove the PNPI from old data files.
- ❑ Look for PNPI in archived material and destroy documents no longer needed. Common documents to seek include
  - Old class rosters and grade records,
  - Employee evaluations,
  - Old timecards,
  - Other payroll records that duplicate information stored by HR.
- ❑ Look for PNPI in computer files and either delete the files or delete the PNPI from the files. Two examples:
  - Faculty should seek out old class rosters and grade records and delete the SSNs from those files.
  - After a hiring search is completed, individual search committee members should delete computer files containing PNPI about the candidates, and departments should safeguard the one copy retained per University policy.

3. Do not use PNPI such as SSNs as unique identifiers for individuals unless required to do so by law.

- ❑ Do not use SSNs or partial SSNs as identifiers or default passwords.
- ❑ Ask employees to use their employee ID number (EMPLID) whenever possible.
- ❑ Don't use SSNs to grant student, faculty, or staff access to restricted web sites. Use the University's Central Authentication Service (CAS). CAS uses each person's UDelNet ID for verification.
- ❑ When having students use scan forms to submit test answers, do not allow them to code their SSNs on the forms.
  - Effective November 1, 2005, test-scoring jobs with SSNs will no longer be accepted.
  - You may post or track grades by assigning students a substitute number known only to you and the student. Students can use that number in the "Student ID Number" space.
  - To uniquely identify students' scan forms, ask them to enter their UDelNet IDs in the "Last Name" space and the first 7 characters of their last names in the "First Name" space.
  - If students mistakenly fill in their SSNs in the "Student ID Number" section, you must shred the brown response forms when you dispose of them.

4. Use secure, encrypted communication for all electronic transactions that require use of PNPI.

- ❑ Do not use a plain "telnet" client to log into the University's servers. Use a secure program like SSH.
- ❑ Do not send PNPI in e-mail messages. An exception: Some government agencies require PNPI be sent via e-mail.
- ❑ Faculty may only e-mail grade information to a student after receiving that student's explicit permission. Grade information and graded assignments should be sent only to a student's official UD e-mail address. Faculty who plan to use e-mail for grade notification on a regular basis may ask students to submit a form or an e-mail message granting that permission.
- ❑ Do not collect SSNs, credit card numbers, or other PNPI without using a secure web application.
- ❑ When setting up a secure on-line application, use the University's CAS system for authentication when the audience/clients are members of the University community and use SSL or secure certificates when the audience includes people outside the University.
- ❑ Do not type PNPI into a web site unless the site is secure. The site's URL will begin with https. Many browsers have an icon representing a lock at the lower right of the browser window. If you are unsure about the authenticity of the site, you can double-click the lock icon.