Cyber Security Checklist for Student Records (PER)

University of Florida
Office of
IT Security Management

PER is private information in student records such as:

- Name of the student's parent or other family member
- Address of student's family
- Personal identifier, such as the student's social security number
- A list of personal characteristics that would make the student's identity easily traceable
- Evaluations, forms, essays, memos, or correspondence to and about the student
- Financial – aid, tuition, payments, account balances
- Grades, exam scores, or GPA (grade point average)
- Applications and admissions information
- Disciplinary status
- Class rosters
- Schedules
- Birth date
- Gender
- Citizenship
- Marital status
- Religion

PER Safeguards:

- ✓ Do not access student records without authorization
- ✓ Access student records only on authorized applications such as ISIS and WebCT
- ✓ Report exposed data immediately to the UF Privacy Office
- ✓ Unless you have special permission, do not transmit student records in:
  - Email
  - Instant messaging
- ✓ Unless you have special permission, do not store student records on:
  - A desktop computer
    - Position screen so that it's not viewable to others
  - Any computer that is not professionally managed, such as your home computer
    - Maintain current software updates
    - Maintain current anti-virus updates
    - Use a firewall
  - A laptop, PDA or smart phone or other portable devices
    - Do not remove from campus without authorization
    - Don't synchronize with home computer.
    - Protect device as you would a wallet or purse.
  - Removable media such as CDs, DVDs and USB thumb drives
    - Protect media as you would a wallet or purse.
- ✓ Regardless of the use, practice the following safeguards
  - Obtain approval for all devices, media and software used with student records
  - Use strong passwords to access student records
  - Password-protected screensaver with a short time-out
  - Minimize the amount of data stored
  - Minimize the length of time data is stored
  - Encrypt stored data, preferably using whole-disk encryption
  - Only use applications that encrypt transmitted data
  - Encrypt backups and minimize backup retention time
  - Render all media unreadable prior to reuse or disposal