Protecting Personally Identifiable Information (PII)

Policy Owner	V. Clark, Administrative Applications Support Group, Office of Information Technology
Policy Approver(s)	Gary Miller, Chief Information Officer (CIO), Office of Information Technology
Related Policies	Data Protection Policy for Administrative Applications User Accounts and Strong Passwords Policy
Related Procedures	(Other related enterprise procedures both within or external to this manual.)
Storage Location	\\cats\ITDocs\Audit and Compliance\Policies
Effective Date	September 15, 1996
Next Review Date	September 15, 2015

Purpose

Fort Valley State University ("FVSU") recognizes the importance of protecting [the privacy of] Personally Identifiable Information ("PII") about entities – recruits, applicants, students, graduates, faculty, staff and third parties – with data in our Banner Student Information System ("users"). What follows is an overview of the FVSU policy on Protecting Personally Identifiable Information ("PII").

Scope

This Protecting Personally Identifiable Information (PII) Policy refers to a person's name, address, email address, username and password, phone numbers, credit/debit card information, SSN and/or UserID (ID) in the Banner Student Information System and the PeopleSoft Financials/HR Self-Service System. The name of prior schools attended or workplace history, date of birth, personal interests, and grade information is also considered personally identifiable information when used and/or combined with PII. These systems are licensed for use by the Board of Regents (BOR) of the University System of Georgia (USG) and by Fort Valley State University (FVSU) as a USG institution. Specifically, it covers:

- All students attending the University, their parents and/or guardians associated with FVSU
- All employees, clients or other third parties that access FVSU non-public information systems
- All contractors and third parties that perform work on behalf of FVSU
- All financial information for FVSU, its employees, clients or other third parties.

Policy

1. PII may be used by, but is not limited to, FVSU to facilitate the following: (1) admission acceptance; (2) registration; (3) grades processing; (4) financial aid processing; (5) fee and other bill payments; (6) graduation processing; (7) transcripts processing; (8) network and computer systems access rights and validation after login; (9) personalizing the end user experience; and (10) helping us to improve our educational services and products. *Note: PII will be treated as confidential by Fort Valley State University.*

2. At FVSU, it is our policy ***not*** to share PII with third parties without consent except as is stated expressly in this policy. However, FVSU reserves the right to share PII with any or all FVSU affiliated third parties for the purpose of supporting the enterprise applications in use at the University or in support of the administrative or educational experience of our constituents. *Note: any PII voluntarily posted to a public area of a University application (includes posts to a blog, bulletin board or chat room) might be collected and used by others. FVSU cannot prevent such uses.*

Procedures

Procedure 1

Configure administrative systems to completely or partially mask confidential and sensitive data appearing in desktop and web-based applications:

- Where possible, data masking should be used for all confidential data displayed to users.
- Data masking solutions should be centrally managed by security personnel.

Procedure 2

All transmission or viewing of personally identifiable information must be handled in such a manner as to ensure the protection of the data that's being stored, viewed or transmitted:

- Use software functions to protect confidential data from persons or exposure that would jeopardize the confidentiality and/or integrity of the data.
- Use encryption functions to protect confidential data when transmitting electronically.

Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- A minor breach will result in written reprimand.
- Multiple minor breaches or a major breach will result in suspension.
- Multiple major breaches will result in termination.

Revision History

Version	Change	Author	Date of Change
1.1	To include reference to "User Accounts and Strong Passwords Policy" and to update Policy Approver with new CIO, Gary Miller	V. Clark	6/10/2013