Memorandum

To: FDU University Community
From: Hania Ferrara, Vice President and Treasurer
       Neal Sturm, Vice President and Chief Information Officer
Date: July 17, 2013
Re: Personal Information Security Policy

Fairleigh Dickinson University recognizes the importance of safeguarding the confidential and personal information of its students, alumni, and employees against data breach. FDU will be undertaking the effort to formalize a University-wide Information Security plan. While this plan is a work in progress, the FDU community must implement policies and procedures, effective immediately, to safeguard personal information against data breach and to meet regulatory compliance. Neither this memo nor the policy being developed is a result of any security breach or problem that has occurred; rather, it is to ensure full regulatory compliance and to prevent the possibility of a security breach in the future.

For this purpose, “Personal information” is the term for protected information and it is defined as an individual’s:

1. Social security number
2. Driver's license number or State identification card number
3. Full date of birth in combination with a person’s name
4. Account number or credit or debit card number, or an account number or credit card number in combination with any security code, access code or password that would permit access to an individual's financial account.

To protect and safeguard personal information, and until a University-wide Information Security Plan is developed, Brian Domenick will continue to serve as the acting Information Security
Officer and is charged to review all University administrative processes for storing and for the transmission of personal information.

Effective immediately, all members of the FDU community are required to adhere to the following policy regarding personal information:

- No personal information is to be stored on any device or system, other than within Datatel, without prior explicit authorization from the Information Security Officer.
- No personal information is to be electronically transmitted (e.g., email, ftp, ...) without prior explicit authorization from the Information Security Officer.

All personal information currently stored on any system other than Datatel should either be immediately removed from the storage devices (e.g., desktops, laptops, smart phones, thumb drives, etc..) or discussed with the Information Security Officer.

If you have any questions regarding compliance to this policy, please contact Brian Domenick, brian@fdu.edu or Neal Sturm, sturm@fdu.edu.