1. Purpose

The purpose of this document is to help limit information access to authorized users, protect information against unauthorized users and establish the different responsibilities each department at the university has when it comes to information security. This document is not limited to a specific information system and will be applied to any system that houses or interacts with the University information.

2. Departmental and Personal Responsibilities / Legal Requirements

In order to operate, the University collects, transmits, stores, reports and interacts with information from individuals associated with the institution or that are doing business with the institution. All of this information is accessible and stored in many different forms, such as: paper, desktops, laptops, servers, portable media, mobile devices, backup systems, etc. Most this information is managed by users within the individual departments at the University. Therefore, each individual staff and faculty member must protect and manage this information in accordance to the

The Information Technology department does not decide what access to provide or what accounts to disable/delete, unless it is for users under the Information Technology department. All access additions and removals are managed with requests from the directors or chiefs within each department. These requests are tracked by using a work order system that is web accessible to every user on campus. Requests that come from non-directors or non-chiefs are routed to the appropriate information owners for approval. Without the appropriate approvals, the Information Technology does not act on any information access requests.

4.2 Other Department Procedures

4.2.1 Office

For access to Web Advisor budget information:
The My Budget Access form is available on Web Advisor. The form requires the department to specify the unit(s) an employee needs to access. The form is the sent to the Budget Director for approval. Once approved the form is forwarded to the Controller's Department where the access will be set up in Colleague. For some positions the access is granted to a range of units, this allows the employee to automatically be given access to new units set up within that range.

Access to Ellucian screens for Controller's Office employees is based upon the job functions. When a new employee is hired, they are given access based upon the job description. If new duties are assigned to the position and additional access is needed we review the employee's access to ensure we have proper controls and segregation of duties in place. When an employee leaves the department their access to the Finance and/or Student modules is deactivated.

4.2.2 Institutional Effectiveness and Research

TracDat Online Planning-Assessment System

http://www.nuventive.com/

http://www.nuventive.com/products/tracdat/

Provided by Nuventive, Incorporated

TracDat is an online system for planning, assessment, and documenting accreditation compliance. It is part of a suite of online systems provided by the company. The university has used the TracDat module and anticipates continuing its use. The system is externally hosted and contains plan narratives and documentation maintained and utilized by the university.

Effectiveness and Research. This permission was granted by the Senior Vice President for Academic Affairs and affirmed by the university president. Many university employees have be-3(d)1es are manaPr(m)1

The Administrator has full access to all information and settings and assign other access/creates new accounts. Admin users create profiles for every new user and update the active users. They are also the ones responsible for contacting StarRez with any issues and system concerns.
Power Users are other professional staff members on campus and office workers. The Power Users are able to have normal access to the system to create bookings and work with student profiles.
RA users is only read only access. This is used for students to log in and submit Incident Reports. The only reports they can see are the ones that they themselves have submitted. RAs only have access to the Web Portal of StarRez and are only displayed minimal student information (Name, Birthdate, Room Location, Photo).

StarRez also tracks all changes made to an account by logging date, time, System User, and System Computer that made the change. Access to the program is only through direct install on approved computers by going through he //wall server and there is also myroom.ju.edu/starrezweb for online access. Part of each employee contract is a confidentiality agreement that pertains to all student information that is found from StarRez.

5. Information Management Committees and Groups

There are three different groups on campus currently responsible for managing the different aspects information, systems and technology projects on campus. These groups allow for better communication of the procedures currently used in each department when it comes to technology and information security.

5.1 Users Group Advisory Committee

The UGAC (Users Group Advisory Committee) is a committee headed by the Information Technology department and is gathering of the directors and data managers from all of the key departments on campus. This committee is responsible for prioritizing all high level technology projects on campus and also discussing any changes to technology that might have an impact on the University. More information on the UGAC can be found on the UGAC web site located on http://www.ju.edu .

5.2 Student Group

The Student Group is currently headed by the Registrar. It is a gathering of all key users that work with student information in the various systems, but particularly the ERP system. This group was formed to communicate changes and track them when it pertains to student information and processes.

5.3 Ellucian Data Integrity Committee

This committee is headed by the Institutional Research department and is a gathering of all the users from every different department on campus, including those that do not interact with the Ellucian ERP system. Although the name includes the company name of Ellucian, the main focus of this committee is to discuss the data that is in the various systems on campus. Topics such as the understanding of information, releasing of information, department procedures are discussed. Any issues or new projects related to the data within our systems are brought to this committee.