JACKSONVILLE UNIVERSITY

Created by: *Christian Block, Director of Information Services*
Date: *05/06/14*
Status: *Added department procedures*

Information Security Procedures

Contents

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's 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 different laws, best practices, and good judgment.

2.1 Accountability

All the information that is produced, acquired, or maintained by all employees at Jacksonville University while performing University business processes is considered University information. Users that collect, store, transfer, administer or maintain this information are held accountable for its use.

2.2 Employee Responsibilities

All University employees that interact with any kind of information that belongs to the institution are required to understand the different processes, procedures and laws that are in place to protect that information. The information is maintained by several different departments on campus, and it is the employee's responsibility to learn all of these responsibilities from their direct supervisor.

2.3 University Departments Responsibilities

There are several different departments that are part of the institution. Many of these departments are responsible for the information that is entered, processed and stored in their area. The director and chiefs that oversee these departments need to know all of the different legal requirements their departments need to enforce when working with information within the institution. Furthermore, these departments are responsible to granting access and revoking access to their information when needed. This can be done with the help of the Information Technology department or within the system if the department has the necessary access.

2.4 Information Technology Department Responsibilities

The department of Information Technology at the University is responsible for providing the means of storing, transferring and maintaining the information for all of the departments and users at the University. The information is secured according to the different legal requirements and best practices. Therefore, the department is responsible for adding the different technical layers of security for the University, such as: encryption, firewalls, monitoring, log maintenance, backup security, etc. The Information Technology department does not have the authority to grant permissions to users nor release information without the consent of the different departments on campus that maintain this information.

3. Information System Ownership

This describes the current operating procedures departments should be following when it comes to granting, revoking and sharing information within the institution or outside the institution.

3.1 ERP Module Owners

The current ERP system that is used by the University is module based. This means it is broken down into different sections of information and processing. There are several different modules currently being used by the University: Student, Core, Finance, Utilities and Human Resources. There are several departments that are considered owners of each module that houses the information. Some modules may include sub-modules within them and are many times managed by a different department than the main module. Below is a list of modules and sub-modules currently being used in the system and their respective responsible department(s):

Main Module	**Sub-Module**	**Owner**
Student	Academic	Registrar's Office
Student	Housing	Residential Life Office
Student	Financial Aid	Financial Aid Office
Student	Recruiting	Admissions Office
Student	Accounts Receivable	Controller's Office
Core		Student Life, Human Resources, Financial Aid, Admissions, Registrar, Controllers, Information Technology.
Finance		Controller'
Utilities		Information Technology
Human Resources		Human Resources

3.2 Other System Owners

There are several other systems on campus that are used by departments within the University. Many are fully managed by the department, meaning, they add/remove accounts and access. These systems can be either hosted offsite or onsite.

4. Operating Procedures – Information Access and Sharing

The operating procedures identify the general process most departments use when working with access and sharing of information in various systems.

4.1 Information Technology Procedures

The Information Technology department manages the primary user database for authentication at the University. This database is stored on a Microsoft Active Directory platform. Most of the systems currently used on our campus use this directory for authentication, therefore, when accounts are deleted or disabled within the main directory, it also revokes access to most systems on campus. However, if accounts are created or enabled, it does not necessarily provide access to any other systems on campus.

The populating of the directory is based on the procedures for each department. The Information Technology department automates the process of user creation, based on the entries from the Admissions teams for applicants and students, and the entry of employees and non-employees by the Human Resources department.

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 Controller's 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.

The university's instance of the Xitracs system is managed by the Director of Institutional 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 been given access to the system.

Xitracs

http://www.xitracs.com/

Provided by Concorde USA, Incorporated

Xitracs 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 accreditation module and anticipates continuing its use. The system is externally hosted and contains the narratives

and documentation submitted to its regional accreditor, the Southern Association of Colleges and Schools Commission on Colleges (SACS-COC).

The university's instance of the Xitracs system is managed by the Director of Institutional Effectiveness and Research. This permission was granted by the Senior Vice President for Academic Affairs and affirmed by the university president. Five university employees have been given access to the system.

Courseval

http://www.connectedu.com/course-evaluations

https://ce3.connectedu.net/etw/ets/et.asp?nxappid=0R1&nxmid=start

Provided by ConnectEDU, Incorporated

Courseval is an online system for managing online assessments that include faculty evaluation of students and student evaluation of faculty. It is evaluation component of a suite of online systems provided by the company. The university has used the evaluation module, but may terminate its use at the end of the 2013-14 academic year. The system is externally hosted and contains course, faculty, and student information/data that is updated on a daily basis.

The university's instance of the Courseval system is managed by the Director of Institutional Effectiveness and Research. This permission was granted by the Senior Vice President for Academic Affairs and affirmed by the university president.

4.2.3 University Advancement

University Advancement uses the Raisers Edge fund raising software to track alumni, donors, gifts, and related events. Employee access is given on a need to know basis. Most JU employees who are involved with fundraising can receive permission to have read-only access to the donor records, with additional permission to write notes on interactions.

Access to the RE software system is terminated when an Advancement employee leaves JU or changes out of a fund raising role. The JU HR office notifies the UA office manager when employees outside of UA are terminated. On receiving these notifications, the former employees have their Raisers Edge access revoked.

The Advancement office also uses the Lexis Nexis information database. When a user leaves JU's employment, the password will be changed.

University Advancement employees are given access to Colleague if their work requires it and it is granted by the Registrar. If UA employees change jobs within the university, the UA office manager will request that HR remove the access granted to perform UA work.

4.2.4 Residential Life

Each user is assigned a unique identity (their JU Username) and a unique password that they can personalize. There are Administrator, Power User, and RA (Student Employee) accounts. In Residential Life, Administrator access is only granted to the Director, Associate Director, and Assistant Director of Operations (Luke Morrill, David Stout, Alex Brucker respectively). IT has been granted Admin access as well.

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.