Title/Subject: **SAP SECURITY - AUTHORITY, RIGHTS & RESPONSIBILITIES**

Applies to: ☒ faculty ☒ staff ☐ students ☒ student employees ☐ visitors ☒ contractors

Effective Date of This Revision: March 2011

Contact for More Information: OIT/Office Of The Controller

☐ Board Policy ☒ Administrative Policy ☐ Procedure ☐ Guideline

---

BACKGROUND:

It is the responsibility of the SAP Security Administrator(s) to ensure that any and all access to the University's SAP system and related SAP solutions is given to the appropriate persons through the necessary authorization levels, approvals and documentation.

PURPOSE:

This policy is intended to provide insight for establishing proper authorizations, rights and responsibilities related to the various modules of the SAP Enterprise information system.

DEFINITIONS:

SAP Enterprise: Integrated information system housing university financial, employment and student business and academic data.

FI: SAP Finance module, including sub-modules for financial accounting, controlling, funds management, accounts payable, cash management, grant accounting, plant maintenance, materials management and asset management.

HR: SAP Human Resource module, including sub modules for payroll, time management, benefits, personnel, training and event management, organizational management, travel management, and manager's desktop.

SLCM: SAP Student Life Cycle Management, including student administration, admissions, student accounting, academic structure, registration and event planning.

Data Ownership: Security Administrators need to seek approval from data owners (Directors of departments related to modules) prior to giving non-standard access to users external to the data owner's department. For example: access to student data is not to be given to a non-student administrative department without authorization from the Registrar.

Process	Sub Module	Owner
Data / Transaction Request	SLCM – Student Administration	Registrar
Data / Transaction Request	SLCM – Admissions	Admissions Director
Data / Transaction Request	SLCM – Student Receivables	Receivables Director
Data / Transaction Request	FI	Asst. Controller Financial Reporting
Data / Transaction Request	MM & Logistics	Purchasing Director

---

Authority: George E. Ross, President
History: None
Indexed as: SAP Security – Authority, Rights & Responsibilities; Security – SAP Enterprise Information System; Enterprise Information System.

Title/Subject: **SAP SECURITY - AUTHORITY, RIGHTS & RESPONSIBILITIES**

Data / Transaction Request	HR	Employment Director
Data/Transaction Request	Benefits/HIPAA Data	Benefits Director
Data / Transaction Request	Payroll/Time	Asst. Controller Financial Services

POLICY:

Levels of access are broken down into six areas:

1. **Standard** - Access to DISPLAY basic University information, primarily public financial information. This access level is generally granted to any non-student university employee that requests it.

2. **Department level and/or position based** – This level of access is defined in collaboration between the Security Administrator and the Department Manager/Director, and applies to the specific duties/functions and responsibilities of the user/job.

   When a new position based role is created, it is defined in collaboration with the necessary supervisor and if needed, data owner. Once established, future occupants (employees) of that job will inherit the position based security associated with that job with only their supervisor approval on the SAP User Account Request form.

   Over time a position may change, and may need a different level of position based access. Responsibility for this type of change lies with the supervisor. The supervisor must again collaborate with the SAP Security Administrator on any and all necessary changes to the employee's position based security.

3. **Custom** – This is generally a level of access when job functions require data access outside of their work department. For example, some users in the SAC may have limited HR access to verify employment and/or family relationships for membership signup.

4. **Legal** – This level of access pertains specifically to data that is considered to have a policy owner and legal ramifications. This level of access is highly limited and is defined with the three following policy/owners:

   - **HIPAA** – HIPAA POLICY OFFICER
   - **FERPA** – FERPA POLICY OFFICER
   - **Social Security Number** – HR/Registrar

5. **Basis Access –** Basis is the Business Application Software Integrated Solution. The Basis team administers the Netweaver layer, operating system and database on which the SAP Enterprise Application runs. The Basis team is responsible for configuring the SAP environment, landscape, application servers and installing/activating core SAP modules and enhancements. There is a very high level of access with the SAP Basis security role. It should be limited to users that need this full level of high access. Users needing only specific parts of this access should be given just the specific parts that they need to perform their job.

6. **Conflicts of Interest / Internal Control Issues –** This level of access should be avoided if at all possible. Questions/concerns pertaining to this should be directed to the Assistant Controller Financial Services or Assistant Controller Financial Reporting.