

## **Information Technology – Rod Tosten, Vice President of IT**

**Effective Date:** July 24, 2013

**Title:** PeopleSoft Application Access Request Policy

**Applicable with restrictions:** Support Staff, Administrators, Faculty, and members of the Campus Community.

**Summary:** The PeopleSoft applications by Oracle are utilized and supported across all divisions of the college. There are currently three production PeopleSoft application baselines that include Campus Solutions, Human Capital Management, and Financials. This policy explains how to request access to these PeopleSoft applications.

**Contacts:** The point of contact for this policy is the Director of IT Data Systems at phone extension 6984.

### **Policy Scope:**

This policy applies to both employees and non-employees of the college who require access to the PeopleSoft software applications including PeopleTools. This policy covers employees including administrators, faculty and support staff personnel in addition to other campus community members who are not employees of the college such as contractors, volunteers, and consultants.

### **Policy Statement:**

Access will be granted to PeopleSoft under the following conditions:

The user has a Gettysburg College Network Account

The Department Director or Functional Analyst for the specific area in PeopleSoft has approved a detailed written request including the following information:

- a) Name of employee who is requesting access, department, job title, phone extension, and location.
- b) Name of person for whom access is being requested, department if an employee or company name if a non-employee, job title, phone number, location and other pertinent information.
- c) Definition of the role or service that is being performed by the person for which security access is being requested and the business reason for which the access is needed.
- d) Duration for which the access is required including start and end dates.
- e) Detailed information that identifies the specific PeopleSoft application access that is being requested. Examples include roles, permission lists, query access, specific application modules, menu navigation, business functions, process scheduler processing, page access, page data element inquiry and update (add/change/delete) rights, and reporting. Two-tier access to the Application Designer and Query access are other considerations.
- f) Other software and reporting tools that are required by the individual including Crystal, Query, nVision, SQL or other client software. This information is needed so that IT technical personnel can load the proper software on the computer.

- g) Other security access that may be needed for example access to Outlook, specific read/write access to file share(s) and other file types.

Contractors and consultants are not to be granted unmonitored access to production environments and commonly they work in the test development environments. Contractors and consultants who require access to production environments or servers are provided access via a GoToMeeting which is to be closely monitored by an employee of the college.

For non-employees of the college, additional information is required by the HR Office before access to the college network is granted. This information includes the Personal Data Collection Sheet and a signed copy of the IT computer network use policy agreement.

Training is to be provided by the department director, the designated Functional Analyst, or others in the division once security access has been granted to the PeopleSoft applications to ensure proper and consistent use of the application.

Note: This policy has been in effect since January 15, 2003 with the current revision on July 24, 2013. The policy is to remain in effect until superseded by IT leadership in writing.