

GREAT BASIN COLLEGE
PEOPLESFT SECURITY AUDIT
Internal Audit Report
July 2, 2013 to September 30, 2013

GENERAL OVERVIEW

PeopleSoft Campus Solutions is the software system implemented across all NSHE institutions as part of the iNtegrate Project to replace the outgoing Student Information System known as SIS. The iNtegrate Project began in 2008 and completed in late 2011. Truckee Meadows Community College (TMCC) and the University of Nevada Las Vegas (UNLV) were the institutions picked to pilot the systems before it was rolled out to the remaining campuses. In mid 2010, TMCC and UNLV went live with the new system with all students enrolled in or applying to TMCC or UNLV using the new system. Great Basin College (GBC) went live with the admission module in the fall of 2010 with all modules live by the end of 2011. PeopleSoft Campus Solutions is considered part of an Enterprise Resource Planning (ERP) system, with the Campus Solutions portion covering the major functions of student services consisting of the following five modules or functions: Recruiting and Administration; Student Records; Student Financials; Financial Aid and Academic Advising.

SCOPE OF AUDIT

The Internal Audit Department has completed a review of PeopleSoft Campus Solutions Security at GBC. We conducted our review between July 2, 2013 and September 30, 2013. Our audit included a review of policies and procedures governing PeopleSoft security administration and tests of individuals' access to sensitive data as determined by representatives of the key functional areas. In particular, we were concerned with data that would fall under the auspices of

the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standards (PCI DSS).

In our opinion, we can be reasonably assured that access to sensitive data in GBC's PeopleSoft Campus Solutions system is properly controlled and that PeopleSoft security administration is functioning in a satisfactory manner. However, we believe that implementation of the following recommendations would further improve security and simplify security administration in the future

SECURITY ADMINISTRATION – ROLES AND PERMISSIONS

User access to data within PeopleSoft is primarily controlled by assigning roles to a user. In turn, roles have permission lists assigned to them that define what pages can be accessed and how the data on the page can be accessed. Data access can vary from display only at the low end to the ability to correct data at the high end. Permission lists can access from tens to hundreds of data items. Users can have multiple roles and roles can have multiple permission lists. It is also possible to assign a permission list directly to a user. GBC has access to 186 roles and 558 permission lists defined for use by any of the NSHE institutions that operate within the shared instance of the PeopleSoft Campus Solutions database. There are another 21 roles and 13 permission lists defined specifically for GBC. The development of the roles and permission lists was driven by the implementation consultants with the help of key functional area leads at the time of the iNtegrate project. We noted the following concerns with regard to the documentation of roles and permissions that was created as a part of the iNtegrate project.

1. There are no narrative descriptions that define what job functions roles and permission lists are designed to support, what data a permission list can access and the manner of that access – display only or update and so forth.

2. The existing documentation for roles and permission lists is inadequate for an ongoing security administration function and is becoming more obsolete as time passes and the employees involved in the original project move on to other positions.

We recommend that GBC work with System Computing Services (SCS) and their fellow institutions to develop narrative descriptions for both roles and permission lists. The narratives should provide information on the job functions supported, the data or pages they can access and the manner in which they are designed to access the data (display through correction).

Institution Response

We agree with this recommendation.

Correction

GBC is in agreement with SCS's response. For the past two months, GBC has been working with SCS and our fellow institutions' Student Financials Advisory Support Group on the security rebuild project. A better narrative description of roles and permissions will be developed as we proceed.

SCS Response

SCS has developed a plan and timeline for a re-architecture of the Shared Instance security infrastructure. Completion of the project is estimated to be sometime in the fourth quarter 2014. However, the various functional areas within the project will be completed in phases throughout the course of the year. The overall design and the reporting tools for the security rebuild project have been completed. SCS Security Administrators next will work with the institution Security Coordinators and the various functional Advisory Support Groups to further define their security needs.

Prevention & Monitoring

Not developed at this time due to the status of ongoing security rebuild project.

3. We noted one GBC specific role and four shared instance roles that are not assigned to any user profiles. There were no unassigned permission lists. Unused roles and/or permission lists obfuscate the security picture because it cannot be determined that they are not used or are invalid without research.

We recommend that GBC work with SCS and their fellow institutions and evaluate any unassigned roles to determine their need and eliminate any that are not necessary.

Institution Response

We agree with this recommendation.

Correction

For the past two months, GBC has been working with SCS and our fellow institutions' Student Financials Advisory Support Group on the security rebuild project. As we proceed through this project, an evaluation of unassigned roles to determine their need and necessary elimination will be conducted.

Prevention & Monitoring

Not developed at this time due to the status of ongoing security rebuild project.

SENSITIVE DATA ACCESS

We evaluated user access to 177 different pages that were deemed to contain sensitive data across the main functional areas of the PeopleSoft Campus Solutions system. These areas deal with financial aid with 61 pages, student financials with 39 pages and admissions and records, academic advising and outreach with 77 pages. We compared the list of departmental employees to the list of employees with access according to our queries of the PeopleSoft system. We inquired to department heads to evaluate non-departmental users with access rights in their functional area. Users with access rights in excess of what they should have are considered over provisioned. We noted the following:

1. Twenty individuals were over provisioned across the functional areas, with another three currently under review.

We recommend that GBC adjust these users, as necessary, and conduct regular reviews of user roles to ensure role assignments and authorization levels are correct.

Institution Response

We agree with this recommendation.

Correction

Beginning in November 2013, GBC reviewed the twenty-three individuals who appeared over provisioned across the functional areas and made adjustments accordingly. The adjustments were completed in December 2013.

Prevention & Monitoring

The Security Coordinator will continue to monitor user roles to ensure assignments and authorization levels are correct as they are created.

STUDENT ADMINISTRATION and CONTRIBUTOR RELATIONS (SACR) SECURITY

The colleges, community college and state college utilize a single shared database for their implementation of PeopleSoft Campus Solutions. Each institution needs to maintain some separation of their data from the other institutions and this is partially done with a host of parameters that are defined through SACR security tables and settings. SACR parameters are defined for an individual and thus restrict data on some pages by user and not by the user's assigned roles. For example, institution is one SACR parameter, so if an individual is assigned the GBC01 institution code, in general, they can only access GBC records and not another institution's in the database. We noted the following issues with SACR settings.

1. SACR parameters have not been properly set for approximately 49 users at GBC. These users have the ability to manipulate student records at other institutions including grades, enrollment and other student transactions.

We recommend that GBC work with SCS to research and implement SACR parameters and settings to prevent cross institution data manipulation.

Institution Response

We agree with this recommendation.

Correction

Beginning in November 2013, personnel from GBC and SCS worked together to review and adjust SACR parameters that had not been properly set. The adjustments were completed in December 2013.

Prevention & Monitoring

The Security Coordinator and SACR Coordinator will continue to monitor SACR security to prevent any future cross institution data manipulation.

OTHER

The following issues were noted during this review; however, they are the responsibility of the System Computing Services.

ROLE AND PERMISSION LIST USAGE AND DESIGN PHILOSOPHY

Security design is an important part of the implementation of any system. Since this is a new system that will likely be in use for the foreseeable future, the design foundation is critical to long term ease of use, maintenance and proper security functioning. There are competing objectives in the design of roles and permission lists with the tradeoffs being in scalability, flexibility and system performance. We evaluated role and permission list design against PeopleSoft's own recommendations on design and against published design criteria from authorities in the field. Design criteria from these sources indicate that, in general, roles should not overlap in their use of system features and similarly, permission lists should be mutually exclusive in their assignment of system pages. Further, the average user should have between 10 to 20 permission lists for optimal system performance. With these in mind, we noted the following concerns.

1. Our analysis of roles and permission lists noted that the implementation consultants did not follow the security design guidelines identified above. We found overlapping

permission lists and roles as well as many users with substantially more permission lists than the guideline indicates.

We recommend that SCS work with GBC and their fellow institutions in the shared instance to evaluate the design of these components and begin a process of migrating roles and permission lists toward the design philosophy noted above.

Institution Response

We agree with this recommendation.

Correction

GBC will work with SCS and our fellow institutions on the security rebuild project to better define roles and permissions. We will strive to achieve the proper balance in roles and permissions to ensure that employees are able to complete their job assignments keeping in mind that many roles and duties overlap.

SCS Response - SCS has developed a plan and timeline for a re-architecture of the Shared Instance security infrastructure. Completion of the project is estimated to be sometime in the fourth quarter 2014. However, the various functional areas within the project will be completed in phases throughout the course of the year. The overall design and the reporting tools for the security rebuild project have been completed. SCS Security Administrators next will work with the institution Security Coordinators and the various functional Advisory Support Groups to further define their security needs.

Prevention & Monitoring

Not developed at this time due to the status of ongoing security rebuild project.

SCS Response

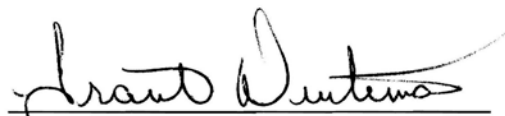
As was noted, the community colleges and state college share a single database for the implementation of PeopleSoft Campus Solutions. Not having been involved in the decisions or implementation of the PeopleSoft Campus Solutions software in this shared environment, SCS reviewed, in great detail, the documentation surrounding the shared instance implementation. From this research, it is clear that the implementation of this function of the shared instance is currently operating precisely as it was designed in that the data constituted "System" records and that they could be viewable and actionable from the various institutions of the shared database. Indeed, System legal counsel specifically reviewed and addressed the matter prior to implementation from the perspective of a single database that collectively constituted the records of the Nevada System of Higher Education as the owner entity.

SCS subsequently contacted the University of Nebraska System, which implemented the PeopleSoft Campus Solutions software around the same time. They operate in a similar manner to NSHE within a shared database environment. In other words, the staff managing the data were employees of the System, and the students submitting the data were students of the System. In this particular module of Campus Solutions, the software operates in a single database and does not provide the capability to limit access to such data by institution, through security controls. Indeed, the University of Nebraska System had attempted to build such security controls. They early-on discovered numerous unintended consequences. The resulting institutional data silos were largely unworkable and the exceptions required and cost of maintenance were extraordinarily high. Moreover, such capabilities would likely preclude such activities as those currently under discussion among some of the NSHE institutions of the shared instance to operate combined back-office services.

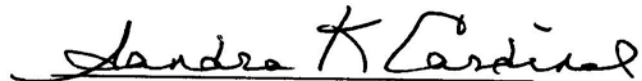
Security has many purposes and can be viewed from various perspectives. Security is maintained through many levels of control. The first line of defense in any system is to limit access to components of the system to only those who require access to specific data and hence have appropriate authorization. That level of control through authorization is necessarily at the campus level.

The Internal Audit Department would like to thank the Information Technology Services staff and other college employees for their cooperation and assistance during this review.

Reno, Nevada
November 6, 2013



Grant Dintiman
IT Auditor



Sandra K. Cardinal
Assistant Vice Chancellor for Internal Audit



MEMORANDUM

Vice President for Business Affairs

TO: Scott Anderson, Interim Director of Internal Audit

FROM: Sonja Sibert, Vice President for Business Affairs

SUBJECT: Audit Response for Great Basin College PeopleSoft Security Audit
July 2, 2013 to September 30, 2013

DATE: April 18, 2014

Nbr	Finding	Agree	Implemented	Est Date of Completion
1	Security Administration – Roles and Permissions Develop narrative descriptions for both roles and permission lists.	Yes	No	12/31/2014
2	Evaluate any unassigned roles to determine their need and eliminate any that are not necessary.	Yes	No	12/31/2014
3	Sensitive Data Access Conduct regular reviews of user roles to ensure role assignments and authorization levels are correct.	Yes	Yes	
4	Student Administration and Contributor Relations (SACR) Security Research and implement SACR parameters and settings to prevent cross institution data manipulation.	Yes	Yes	
5	Role and Permission List Usage and Design Philosophy Evaluate the design of components and begin a process of migrating roles and permission lists.	Yes	No	12/31/2014