WESTERN NEVADA COLLEGE
PEOPLESOFT SECURITY AUDIT
Internal Audit Report
September 1, 2013 to November 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. Western Nevada College (WNC) 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 WNC. We conducted our review between September 1, 2013 and November 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 WNC'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. WNC has access to 191 roles and 302 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 22 roles and 23 permission lists defined specifically for WNC. 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 WNC 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

   WNC concurs with this recommendation. The existing documentation for roles and permission lists will become more obsolete as time passes. To have a system in place to update roles and permissions as operations and staff change is critical. This must first be addressed at the system level to ensure consistency among other institutions and then at the college level.

   System Level Coordinated Effort

   As part of the Shared Instance, WNC will coordinate documentation efforts to complement the work being done by System Computing Services. The Senior Security Analyst for System Computing Services has developed a plan and timeline for a re-architecture of the Shared Instance security infrastructure. The rebuild will impact how WNC will proceed with documenting roles and permission lists.

   WNC Documentation

   Narrative descriptions defining job functions for roles and permission lists including data accessible under these constructs and level of access will be developed in the following manner:

   - **WNC will begin a documentation effort for WNC roles /permission lists that are not expected to change as a result of the Shared Instance rebuild.**

   - **WNC will create documentation for roles/permission lists that will be rebuilt after System Computing Services migrates the role/permission lists to production.**

- **The iNtegrate Project lead, in conjunction with the Module Leads from Admissions, Advising, Financial Aid, Student Records, and Student Financials will facilitate the efforts above.**

WNC expects this project to begin upon commencement of the SCS coordinated effort.

3. We noted one WNC specific role that is 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 WNC 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

   WNC concurs with this recommendation. WNC evaluated the one unassigned role as suggested by the auditor and the role has been removed by SCS. Review of unnecessary shared instance roles will occur during the system level re-architecture of the shared instance security infrastructure.

   Prevention and Monitoring

   The Security Coordinator will monitor unassigned roles for removal on a monthly basis.

<u>SENSITIVE DATA ACCESS</u>

We evaluated user access to 174 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 60 pages, student financials with 39 pages and admissions and records, academic advising and outreach with 75 pages. We compared the list of departmental employees to the list of employees with access according to our queries of the PeopleSoft system. We asked 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. Six individuals were over provisioned across the functional areas via two roles with excessive access authority.

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

   Institution Response

   WNC concurs with this recommendation. The Security & Student Records Module Leads have begun the efforts to adjust security access with a plan to have this recommendation completed by April 2014.

   - **Role adjustments have been completed for four of the six individuals.**
   - **One role requires a modification to be completed by System Computing Services. The modification will eliminate the ability to change data in other modules for two individuals that are over provisioned.**

   Prevention and Monitoring

   The Security Coordinator and Module Leads complete monthly user role audits, however, authorization levels to make changes to data had been overlooked for two roles during the implementation of PeopleSoft. The Security Coordinator and Module Leads will include a review of authorization levels in monthly audits to ensure users are not over provisioned.

   Roles and permission list assignments based upon duties will be clearly defined upon completion of the documentation and re-architecture. This will complement the monthly user role audits.

<u>OTHER</u>

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

<u>STUDENT ADMINISTRATION and CONTRIBUTOR RELATIONS (SACR) SECURITY</u>

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 WNC01 institution code, in general, they can only access WNC records and not another institution's in the database. We noted the following issues with SACR settings.

1. Various SACR parameters have not been properly set for institutions and individuals in the shared instance. These parameters affect user's ability to manipulate student records at other institutions including grades, enrollment and other student transactions.

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

Institution Response

WNC concurs with this recommendation. The Student Records Module Lead has, and will continue to, work with SCS to research and implement SACR security parameters and settings to prevent cross institution data changes.

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.

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 WNC 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

WNC concurs with this recommendation. As part of the Shared Instance, WNC will coordinate with SCS and the other institutions to implement a rebuild of security components in line with a new design philosophy.

System Level Rebuild

SCS has developed a re-architecture for the shared instance security infrastructure and an execution plan for the re-architecture. The Senior Security Analyst for SCS, has met with the NSHE Internal Auditor, and they are in agreement with the execution of a plan around this philosophy.

WNC Migration to the Shared Instance Design Philosophy

As new roles/permission lists are developed by SCS, WNC will assist in testing and developing narratives as described in the audit finding above. This will be completed by the iNtegrate Project Lead and Module Leads from Admissions, Advising, Financial Aid, Student Records, and Student Financials. Migration to the Shared Instance design philosophy will be accomplished as follows:

- **If the new roles/permission lists meet WNC security needs, WNC will replace the current security with that developed for the shared version.**

- **If the new shared version does not meet WNC security needs, WNC will build new roles/permission lists that adhere to the shared instance design philosophy.**

The exact time frame for the project will depend on SCS and shared instance resources.

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
January 10, 2014

Grant Dintiman

Grant Dintiman
IT Auditor

Scott Anderson

Scott Anderson
Director of Internal Audit

Western Nevada College

Memorandum

TO: **Scott Anderson, Director of Internal Audit, NSHE**

FROM: **Chester Burton, President**

SUBJECT: **Audit Response for Western Nevada College PeopleSoft Security Audit**
September 1, 2013 to November 30, 2013

DATE: **February 27, 2014**

Attached is the initial response to WNC PeopleSoft Security Audit for the time period of September 1, 2013 to November 30, 2013. The recommendations and status of corrective actions are provided below.

#	Recommendation	Agree	Completed
1. & 2.	We recommend that WNC work with System Computing Services and their fellow institutions to develop narrative descriptions for both roles and permission lists.	Yes	WNC will coordinate documentation efforts to complement the work being done by SCS. A plan and a timeline has been developed.
3.	We recommend that WNC work with SCS and fellow institutions and evaluate any unassigned roles to determine their need and eliminate any that are not necessary.	Yes	WNC has evaluated the one unassigned role and it has been removed.

#	Recommendation	Agree	Completed
4.	We recommend that WNC adjust these users, as necessary, and conduct regular reviews of user roles to ensure role assignments and authorization levels are correct.	Yes	WNC has begun the efforts to adjust security access. Four of the six individuals have been adjusted. The remaining two are dependent upon a modification being completed at SCS. We anticipate that this will be completed by April 2014.
5.	We recommend that WNC work with SCS to research and implement SACR parameters and settings to prevent cross institution data manipulation.	Yes	WNC staff continue to work with SCS to research and implement security parameters.
6.	We recommend that SCS work with WNC 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.	Yes	WNC will continue to coordinate with SCS and the other institutions to implement a rebuild of security components.