

COLLEGE OF SOUTHERN NEVADA
PEOPLESOFT SECURITY AUDIT
Internal Audit Report
May 1, 2013 to August 1, 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. College of Southern Nevada (CSN) 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 CSN. We conducted our review between May 1, 2013 and August 1, 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 feel that CSN must make changes to user role assignments and data access levels in order to properly control access to sensitive data. In addition, 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. CSN 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 39 roles and 37 permission lists defined specifically for CSN. 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 etc.
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 CSN 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

The College of Southern Nevada concurs with this recommendation. As stated in the audit, the existing documentation for roles and permission lists developed by the implementation consultants will become increasingly obsolete as the roles of CSN staff change over time. To ensure the security administration function, it is particularly critical that we have a system in place to update the roles and permissions to coincide with operational and staff change when such occurs. This must be addressed by System Computing Services (SCS) to ensure consistency and continuity with other colleges utilizing PeopleSoft, and at the institutional level.

CSN is but one member of the shared instance of PeopleSoft. Under the shared instance structure, certain facets of software structure and/or configuration are performed by SCS. The ability to define and structure certain aspects lies with SCS and is performed by SCS in consultation with the other participants of the shared instance. Final resolution of this recommendation will be led by SCS in consultation with the members of the shared instance including CSN, NSC, GBC, WNC, and TMCC.

CSN Documentation

Narrative descriptions that define job functions for roles and permissions lists, including data accessible under these constructs and level of access, must be developed as a part of an automated method that is being developed by System

Computing Services (SCS) as part of the re-architecture of the shared instance security infrastructure. SCS's timeframe for completion is at present unknown.

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 10-20 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 CSN work with SCS and their fellow institutions 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

College of Southern Nevada concurs with this recommendation. As part of the shared instance, CSN will coordinate with System Computing Services and the

other NSHE institutions to rebuild the insufficient roles and permission lists that were prepared by the implementation consultants to strengthen the role and permission components and to ensure that they are consistent with PeopleSoft's more stringent security design philosophy.

CSN is but one member of the shared instance of PeopleSoft. Under the shared instance structure, certain facets of software structure and/or configuration are performed by SCS. The ability to define and structure certain aspects lies with SCS and is performed by SCS in consultation with the other participants of the shared instance. Final resolution of this recommendation will be led by SCS in consultation with the members of the shared instance including CSN, NSC, GBC, WNC, and TMCC.

CSN Migration to the Shared Instance Design Philosophy

As the new roles and permission lists are developed by System Computing Services, CSN will assist in testing and developing narratives as described in *Role and Permission List Usage and Design Philosophy* (#1 above.) This will be completed by CSN iNtegrate co-project leads with assistance from functional leads from college departments including Admissions, Advising, Financial Aid, Student Records and Student Financials.

Migration to the Shared Instance design philosophy will be according to the following criteria:

- If it is found that the new roles and permission lists developed by SCS meet security design philosophy described above, CSN will replace its current security with that developed for the shared version; and conversely
- Where it is found that the shared version does not match the more stringent design philosophy, CSN will build new roles and permission lists that adhere to the shared instance design philosophy.

The timeframe for completion will be determined by SCS and is under the purview of both SCS and shared instance resources. After consultation with SCS representatives, it is estimated that completion can be achieved within one year.

2. We noted 1 CSN specific role and 4 SHR roles 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 CSN 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

College of Southern Nevada concurs with this recommendation. The CSN Security Coordinator has evaluated the one unassigned role identified by the auditor and requested that System Computing Services remove it. Review of unnecessary shared instance roles will occur during the system-level re-architecture of the shared instance security infrastructure which will be led by System Computing Services.

SENSITIVE DATA ACCESS

We evaluated user access to 159 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 57 pages, student financials with 31 pages and admissions and records, academic advising and outreach with 71 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 the 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. 104 individuals were over provisioned in the financial aid area. 97 individuals were over provisioned in the student financials area. In the admissions and records area we noted substantial over provisioning and over authorization on the limited number of pages that we were able to check.

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

Institution Response

College of Southern Nevada concurs with this recommendation. iNtegrate project leads have completed adjusting security access as necessary for Student

Financials and Financial Aid areas. Efforts are in process with the functional leads from Student Records and will be completed not later than the end of February, 2014.

Within six months after the completion of the System-level security infrastructure re-architecture (which is being led by SCS), the CSN iNtegrate Security Coordinator, will work with functional leads from the areas of Academic Advising, Student Records and Admissions, Student Financials, and Financial Aid to develop a standardized set of security roles to apply to defined positions within the institution. If, during a security request, a role is requested that falls outside of the standardized set, the request will be scrutinized by the respective functional area and co-project leads and their approval must be obtained prior to security being granted. Documentation of these exceptions will be maintained by the CSN security coordinator.

We took a more detailed look at Social Security Number (SSN) due to its increased sensitivity. PeopleSoft provides the capability to mask SSN on selected high use screens, however there are many more screens that do not mask the data. We observed the following issues.

1. Approximately 341 individuals have access to SSN data through access to screens with unmasked SSN data.

We recommend that CSN evaluate users with access to unmasked SSN data and ensure that they have a job related need for such access.

Institution Response

CSN concurs with this recommendation and also values the trust placed in us by our students, faculty and staff to protect Personally Identifiable Information (PII). We honor that trust by restricting access to PII except in those cases where it is deemed absolutely necessary to serve our constituents.

iNtegrate co-project Leads have worked with functional team leads to determine which staff members have a required business need to have access to unmasked SSN. Those areas are Financial Aid, Student Financials and Student Records. For those individuals that do not have a business need to have access, only masked SSN are viewable. This recommendation has been implemented.

STUDENT ADMINISTRATION and CONTRIBUTOR RELATIONS (SACR)

SECURITY

The community and state colleges 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 CSN01 institution code, in general, they can only access CSN records and not another institution's in the database. We noted the following issues with SACR settings.

1. CSN is able to post student transactions, including refunds, at other institutions through multiple navigation paths.

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

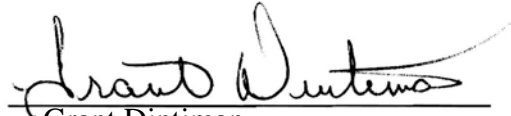
Institution Response

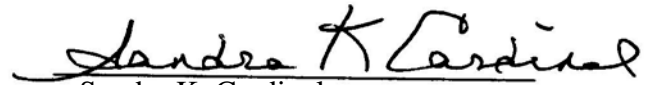
College of Southern Nevada concurs with this recommendation. This issue has been brought to the attention of System Computing Services (SCS) and CSN currently is awaiting the solution that SCS will develop for CSN's implementation.

Additional conversations have been held with SCS leadership regarding a similar circumstance within the Financial Aid Module. CSN is but one member of the shared instance of PeopleSoft. Under the shared instance structure, certain facets of software structure and/or configuration are performed by SCS. The ability to define and structure certain aspects lies with SCS and is performed by SCS in consultation with the other participants of the shared instance. Final resolution of this recommendation will be led by SCS in consultation with the members of the shared instance – CSN, NSC, GBC, WNC, and TMCC. Through conversations with SCS, an additional set of issues was identified regarding the ability of the shared instances to change financial aid information on students.

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
September 20, 2013


Grant Dintiman
IT Auditor


Sandra K. Cardinal
Assistant Vice Chancellor for
Internal Audit



Memorandum

Senior Vice President, Finance & Administration

TO: Scott Anderson, Audit Manager
NSHE

FROM: Patricia Charlton
Senior Vice President, Finance & Administration

SUBJECT: Initial Response for CSN PeopleSoft Security Audit
For the period May 1, 2013 to August 1, 2013

DATE: January 24, 2014

Attached is the initial response to the CSN's PeopleSoft Security Audit for the period from May 1, 2013 to August 1, 2013. The recommendation and status of corrective actions are provided below.

#	Recommendation	Agree	Completed
1.	<p>Security Administration – Roles and Permissions</p> <p><i>We recommend that CSN work with System Computing Services (SCS) and fellow institutions to develop narrative descriptions for both roles and permission lists to include job functions supported, data or pages that can be accessed and manner in which they are designed to access data.</i></p>	Yes	<p>Final resolution of this recommendation will be led by System Computing Services in consultation with members of the shared instance including CSN, Nevada State College, Great Basin College, Western Nevada College and Truckee Meadows Community College. This will ensure consistency and continuity with the other colleges utilizing PeopleSoft and at the institutional level. The timeframe for completion is at present unknown.</p>
2.	<p>Role and Permission List Usage and Design Philosophy (Note: Internal Audit's analysis of roles and permission lists noted that the implementation consultants did not follow the security design guidelines recommended by PeopleSoft and other authorizes in the field.)</p> <p><i>a. We recommend that CSN work with SCS and fellow institutions to evaluate the design of components and begin process of migrating roles and permission lists toward the design philosophy noted in report.</i></p>	Yes	<p>Final resolution of this recommendation will be led by System Computing Services in consultation with members of the shared instance including CSN, Nevada State College, Great Basin College, Western Nevada College and Truckee Meadows Community College. CSN will coordinate with SCS and other NSHE institutions to rebuild the insufficient roles and permission lists that were prepared by the implementation consultants. In addition as the new roles and permission lists are developed by SCS, CSN will assist in testing and developing the narratives consistent with the Role and Permission List Usage and Design Philosophy referenced by Internal Audit in the audit report. The timeframe for completion will be determined by SCS; it is estimated that completion can be achieved within one year.</p>

#	Recommendation	Agree	Completed
2.	<p>Role and Permission List Usage and Design Philosophy (continued)</p> <p><i>b. We recommend that CSN work with SCS and their fellow institutions and evaluate any unassigned roles to determine their need and eliminate any that are not necessary.</i></p>	Yes	<p>CSN's Security Coordinator evaluated the one unassigned role identified by Internal Audit and requested SCS to remove it. This has been completed.</p> <p>Review of the unnecessary shared instance roles will occur during the system-level re-architecture of the shared instance security infrastructure which will be led by System Computing Services.</p>
3.	<p>Sensitive Data Access</p> <p><i>a. We recommend that CSN adjust these users as necessary and conduct regular reviews of user roles to ensure role assignments and authorization levels are correct.</i></p> <p><i>b. We recommend that CSN evaluate users with access to unmasked SSN data and ensure that they have a job related need for such access.</i></p>	Yes	<p>CSN's iNtegrate project leads have completed adjusting security access as necessary for Student Financials and Financial Aid areas. Student Records area will be completed not later than the end of February 2014.</p> <p>Within 6 months of the completion of the System-level security infrastructure re-architecture led by SCS, CSN iNtegrate Security Coordinator will work with functional leads from Academic Advising, Student Records & Admissions, Student Financials and Financial Aid to develop standardized set of security roles to apply to defined positions within the institution.</p> <p>If a requested role falls outside of the standardized set, the request will be scrutinized and approved by the respective functional area <u>and</u> co-project leads prior to security being granted. The CSN Security Coordinator will maintain documentation of these exceptions.</p> <p>CSN values the trust placed in us by students, faculty and staff to protect Personally Identifiable Information (PII) and honor that trust by restricting access to PII except in those cases where it is deemed absolutely necessary to serve our constituents. iNtegrate project co-leads have worked with team leads in Financial Aid, Student Financials and Student Records to determine which staff members have a required business need to have access to unmasked SSN. For all others, only masked SSN are viewable. This recommendation has been completed.</p>
4.	<p>Student Administration and Contributor Relations (SACR) Security</p> <p><i>We recommend that CSN work with SCS to research and implement SACR parameters and settings to prevent cross institution data changes.</i></p>	Yes	<p>This issue has been brought to the attention of System Computing Services (SCS) and CSN is awaiting the solution that SCS will develop for CSN's implementation.</p> <p>Additional conversations have been held with SCS leadership regarding a similar circumstance</p>

#	Recommendation	Agree	Completed
4.	Student Administration and Contributor Relations (SACR) Security (cont.)		within the Financial Aid Module. Through conversations with SCS, an additional set of issues was identified regarding the ability of the shared instances to change financial aid information on students. The ability to define and structure certain aspects of the shared instance is performed by SCS in consultation with the other participants of the shared instance. Final resolution of this recommendation will be led by SCS in consultation with members of the shared instance--CSN, NSC, GVC, WNC and TMCC. .

The Audit Committee Agenda Request form is also attached. Please let me know if you have any questions regarding this information.

Thank you!

PAC:mte

- c: Michael D. Richards, President
- Dan Morris, Executive Director for Business Operations
- John Bearce, Director of Institutional Research
- Mary Kaye Bailey, Associate Vice President for Financial Services/Controller