

UNIVERSITY OF NEVADA, RENO
PEOPLESOFT SECURITY AUDIT
Internal Audit Report
December 1, 2013 to April 30, 2014

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 was 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. The University of Nevada, Reno (UNR) 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 UNR. We conducted our review between December 1, 2013 and April 30, 2014. 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 UNR'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. UNR has access to 273 roles and 665 permission lists defined solely for their use. The development of the roles and permission lists was driven by key users involved in the project from the UNR Information Technology Department and the user areas. 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 for example.

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 UNR 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

UNR agrees with the audit finding and recommendation.

- **How compliance was achieved.**

Narrative descriptions are being developed that define job functions, roles, and permission lists for the undocumented roles and permissions lists. The narrative descriptions include what the permission lists can access and the manner of that access. This will be accomplished December 31, 2014 with annual reviews.

- **What will be done to avoid the identified problems and issues in the future.**

As new roles and permissions lists are created, concise narrative descriptions are being added.

- **How compliance and future good management and practice will be measured, monitored and assured.**

Roles and permission lists are reviewed annually. Updates are performed to the narrative descriptions as needed.

- **Who will be responsible and may be held accountable in the future if repeat or similar problems arise.**

Admissions and Records, Financial Aid and Student Financials Security Administrators in coordination with Campus Security Coordinator will be held accountable in the future if repeat or similar problems arise.

- **When the measures will be taken and on what schedule compliance and good practice will be secured.**

All measures are in progress and will be completed by December 31, 2014.

- **How compliance and performance will be documented for future audit, management and performance review.**

Annual reviews of narrative descriptions of roles and permission lists are being documented.

Follow-Up Response

This item has been completed as of April 20, 2015.

3. We noted 61 UNR specific roles that are not assigned to any user profiles and 84 unassigned permission lists. Unused roles and/or permission lists obfuscate the security picture because it cannot be determined whether they are not used or are invalid without research.

We recommend that UNR evaluate any unassigned roles and permission lists to determine their need and eliminate any that are not necessary.

Institution Response

UNR agrees with the audit finding and recommendation.

- **How compliance was achieved.**

Unused roles and permission lists are in the process of review.

- **What will be done to avoid the identified problems and issues in the future.**

We will audit unused roles and permissions lists and remove those which are no longer needed.

- **How compliance and future good management and practice will be measured, monitored and assured.**

A yearly review of unused roles and permission lists will be completed and those that are no longer needed will be removed.

- **Who will be responsible and may be held accountable in the future if repeat or similar problems arise.**

Admissions and Records, Financial Aid and Student Financials Security Administrators in coordination with Campus Security Coordinator will be held accountable in the future if repeat or similar problems arise.

- **When the measures will be taken and on what schedule compliance and good practice will be secured.**

All measures are in progress and will be completed by December 31, 2014.

Follow-Up Response

This item has been completed as of April 20, 2015.

SENSITIVE DATA ACCESS

We evaluated user access to 202 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 66 pages, student financials with 47 pages and admissions and records, academic advising and outreach with 90 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.

During this review, we noted 33 individuals were over provisioned across the functional areas with excessive access authority.

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

Institution Response

UNR agrees with the audit finding and recommendation

- **How compliance was achieved.**

UNR reviewed the over-provisioning of user rights and the specific individuals have been adjusted accordingly.

- **What will be done to avoid the identified problems and issues in the future.**

IT and Security Administrators are developing a written plan for quarterly review of user access that can modify student data in the system. Quarterly calendar reminders will trigger the review process.

- **How compliance and future good management and practice will be measured, monitored and assured.**

In addition to the process noted previously, Student Services is working on making more expedited notifications of department changes and/or terminations to ensure those individuals are not retaining their access past their contractual end.

- **Who will be responsible and may be held accountable in the future if repeat or similar problems arise.**

Admissions and Records, Financial Aid and Student Financials Security Administrators in coordination with Campus Security Coordinator will be held accountable in the future if repeat or similar problems arise.

- **When the measures will be taken and on what schedule compliance and good practice will be secured.**

All measures are in progress and will be completed by November 30, 2014.

- **How compliance and performance will be documented for future audit, management and performance review.**

The security plan review will be implemented on a quarterly basis for those with modifying access to the system.

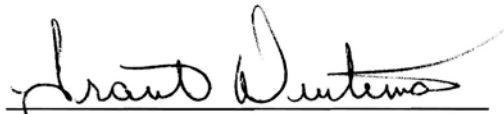
Follow-Up Response

This item has been completed as of April 20, 2015. All Users have been adjusted and access has been changed in accordance with their duties. The initial cleanup was completed in November 2014. Going forward, security access will be reviewed on a quarterly basis with the dates being the first of the following months: February, May, August and November. The review will involve the PeopleSoft Security Administrator notifying each team of users who have access to their respective areas in PeopleSoft. The functional teams will review the access and then notify the PeopleSoft Security Administrator of changes that need to be made due to personnel leaving or changing duties. The Security Administrator will then take that list and

make the appropriate changes in PeopleSoft. As mentioned, this will be done on a quarterly basis.

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

Reno, Nevada
September 23, 2014

A handwritten signature in black ink, appearing to read "Grant Dintiman", written over a horizontal line.

Grant Dintiman
IT Auditor

A handwritten signature in black ink, appearing to read "Scott Anderson", written over a horizontal line.

Scott Anderson
Director of Internal Audit

Memorandum

To: Scott Anderson, Director Internal Audit, Nevada System of Higher Education

From: Tom Judy

Date: April 29, 2015

Subject: PeopleSoft Security audit response

The purpose of this memorandum is to transmit the follow-up response from the Enrollment Services Department to the PeopleSoft Security audit for the period December 1, 2013 through April 30, 2014.

I have reviewed and concur with all responses.

cc: Marc Johnson, President
Ronald Zurek, Vice President, Administration and Finance
Kathlin Ray, Chief Information Officer
Melisa Choroszy, Associate Vice President, Enrollment Services



AUDIT

PeopleSoft Security

AUDIT PERIOD

December 1, 2013 through April 30, 2014

NUMBER OF RECOMMENDATIONS

3

#	Recommendation	Implemented	Est. Date of Completion
---	----------------	-------------	-------------------------

Security Administration - Roles and Permissions

1	We recommend that UNR 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).	Yes	
---	--	-----	--

2	We recommend that UNR evaluate any unassigned roles and permission lists to	Yes	
---	---	-----	--

Sensitive Data Access

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