

UNIVERSITY OF NEVADA, LAS VEGAS  
PEOPLESOFT SECURITY AUDIT  
Internal Audit Report  
March 2015 to June 2015

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. 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 UNLV. We conducted our review between March 1, 2015 and June 30, 2015. 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 UNLV'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. UNLV has access to 507 roles and 601 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 UNLV Office of Information Technology 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 UNLV develop narrative descriptions for both roles and permission lists. The narratives should provide high level 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.**

- **What will be done to avoid the identified problems and issues in the future.**  
The roles description text will be used to contain the appropriate documentation of what is assigned by a role. This will include the type of access (view, update or correction) granted by the role by noting the permission lists that should be assigned. This will allow for a one-to-one match of description details to actual assignments which can be verified periodically.

Permission list names and brief descriptions will be updated to describe the appropriate function of the permission list. As noted above the permission lists used in role creation will be included in the documentation procedures for roles.

- **How compliance and future good management and practice will be measured, monitored, and assured.**  
Lists will be generated based on the update datetime stamps of roles and permission lists. Samples from the list will be identified for a verification to the adherence of the documentation procedures for roles and accuracy of the permission lists naming and documentation procedures.
- **Who will be responsible and may be held accountable in the future if repeat or similar problems arise.**  
The Software Engineering Services Manager has oversight of the PeopleSoft security administration.
- **When the measures will be taken and on what schedule compliance and good practice will be secured.**  
The new role and permission list description procedures have been instituted as of October 2, 2015. The process of bringing existing roles and permission lists into compliance is slated for completion by January 29, 2016.
- **How compliance and performance will be documented for future audit, management and performance review.**  
Security administration procedures provide documentation of user access and profile review and are available for audit review.

3. We noted 130 UNLV specific roles that are not assigned to any user profiles and 33 unassigned permission lists. Unused roles and/or permission lists obfuscate the security picture because it cannot be determined whether they are unused or are invalid without research.

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

### **Institution Response**

**We agree with this recommendation.**

- **What will be done to avoid the identified problems and issues in the future.**  
A review existing roles and permission lists assignments will be performed to produce a list of the roles and permission lists that are not assigned. That list will be reviewed and any role or permission list identified as no longer needed will be removed.
- **How compliance and future good management and practice will be measured, monitored, and assured.**  
The list of roles and permission lists not assigned will be produced. Samples from the list will be identified for a verification that the review process had been performed and appropriately documented.
- **Who will be responsible and may be held accountable in the future if repeat or similar problems arise.**  
The Software Engineering Services Manager has oversight of the PeopleSoft security administration.
- **When the measures will be taken and on what schedule compliance and good practice will be secured.**  
The review of roles and permission lists not assigned was completed in October, 2015. We plan on performing this review twice annually in the future.
- **How compliance and performance will be documented for future audit, management and performance review.**  
Security administration procedures provide documentation of user access and profile review and are available for audit review.

## SENSITIVE DATA ACCESS

We evaluated user access to 195 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 70 pages, student financials with 41 pages and admissions and records, academic advising and outreach with 84 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 numerous individuals with update access to functional area data who were not functional area employees. In some cases this was due to individuals leaving employment at UNLV who were not removed from PeopleSoft, or individuals that changed positions at the university whose access rights were not updated.

We recommend that UNLV 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.**

- **What will be done to avoid the identified problems and issues in the future.**  
The security administration team will create a report at the start of Fall and Spring terms that will be sent to departments for review and sign-off.
- **How compliance and future good management and practice will be measured, monitored, and assured.**  
Reports and their sign-off will be tracked and used as evidence of compliance.
- **Who will be responsible and may be held accountable in the future if repeat or similar problems arise.**  
The Software Engineering Services Manager has oversight of the PeopleSoft security administration.

- **When the measures will be taken and on what schedule compliance and good practice will be secured.**  
This process will be completed the first time by January 29, 2016. After completion of this first review, we plan on continuing to perform the review twice annually.
- **How compliance and performance will be documented for future audit, management and performance review.**  
Security administration procedures provide documentation of user access and profile review and are available for audit review.

## OTHER

The following issues were noted during this review; however, they are the responsibility of 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, some evidence of overlapping permission lists and roles was noted.

We recommend that UNLV evaluate roles and permission lists to minimize overlap in their design where possible.

### **Institution Response**

**We agree with this recommendation.**

**Many of the documents published by PeopleSoft and other authorities are indeed recommendations. UNLV reviewed a number of documents to arrive at our security design. While we acknowledge that it is overdue for closer review, the overall structure is sound and working as needed. No performance or processing issues have been reported and no inappropriate security has been granted through the design or its application to a user accounts.**

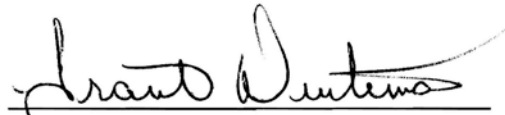
**Reviews of roles and permission lists currently occur as needed. At times new ones are created for the need of a business area. If an account owner is someone with duties multiple areas, like Admissions and Student Records, overlap assignment can occur. While this is discouraged it not restricted.**

**UNLV is currently planning to upgrade to 9.2 Campus Solutions. We foresee this as an opportunity to not only review but to streamline security design. It is our current plan to engage a consultant that is proficient with PeopleSoft security to assist in this process.**

**We respectfully request that this item be closed.**

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

Reno, Nevada  
August 26, 2015



Grant Dintiman  
IT Auditor



Scott Anderson  
Internal Audit Manager



Joe Sunbury  
Chief Internal Auditor





**AUDIT:** PeopleSoft Security

**AUDIT PERIOD:** March – June 2015

**NUMBER OF FINDINGS:** 4

**NUMBER OF RECOMMENDATIONS IMPLEMENTED:** 2

Nbr	Finding	Agree	Implemented	Est Date of Completion
1	No narrative descriptions, and existing documentation is inadequate	Yes	No	01/29/2016
2	Evaluate unassigned roles and permission lists and eliminate unnecessary ones	Yes	Yes	
3	Many employees have update access who are not functional area employees	Yes	No	01/29/2016
4	Evaluate roles and permission lists to minimize overlap in design	Yes	Yes	