

TRUCKEE MEADOWS COMMUNITY COLLEGE
PEOPLESOFT SECURITY AUDIT
Internal Audit Report
November 1, 2011 through January 10, 2013

GENERAL OVERVIEW

PeopleSoft Campus Solutions is the software system implemented across NSHE institutions as part of the iNtegrate Project to replace the 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 system before it was implemented at the remaining campuses. In mid-2010, TMCC and UNLV went live with the new system with 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 Truckee Meadows Community College (TMCC). We conducted our review between November 1, 2011 and January 10, 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, our primary focus was 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 TMCC'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.

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. TMCC defined 180 roles and 296 permission lists for use at TMCC and they have access to an additional 195 roles and 317 permission lists defined for use by any of the NSHE institutions that operate within the shared instance of the PeopleSoft Campus Solutions database. 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 as the employees involved in the original project move on to other positions.

We recommend that TMCC develop narrative descriptions for both roles and permission lists that 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

TMCC concurs with this finding. The existing documentation for roles and permission lists will become more obsolete as time passes. It is critical that we have a system in place to update the roles and permissions as operations and staff change. This will be addressed first at a system level to ensure consistency with other colleges, and then at the institutional level.

System-Level Coordinated Effort

As part of the Shared Instance, TMCC will coordinate its documentation efforts to complement the work being done by System Computing Services (SCS). SCS is developing a plan and timeline for a re-architecture of the Shared Instance security infrastructure. Chris Piekarz, Senior Security Analyst for SCS, will have this plan done by May 1, 2013. If this rebuild plan is passed by the iNtegrate Shared Instance Advisory (iSIA) group, the rebuild will go forward. This rebuild will impact how TMCC will proceed with documenting roles and permission lists.

TMCC 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:

- **For roles and permission lists that TMCC does not expect to change as a result of the Shared Instance rebuild, TMCC has begun the documentation effort. This documentation will be completed within one year from the date of this response.**

● For roles and permission lists that will be rebuilt, TMCC will create the documentation for that role / permission list within one month of its migration to production by System Computing Services.

Tommie Guy, Security Coordinator and Shanna Rahming, Business Analyst will lead and facilitate the efforts above in coordination with the functional leads from Financial Aid, Admissions, Student Records, Outreach, Student Financials and Advising

Follow-up Response:

As of October 25, 2013, TMCC understands that every role and permission list in the PeopleSoft Shared Instance rebuild will be changed. Documentation of roles and permission lists will be automated and are a part of the rebuild plan approved by the iSIA and carried out by System Computing Services analysts Chris Piekarz and Eric March. This finding is no longer in the purview of TMCC's audit response. We request that this finding be closed.

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 TMCC evaluate the design of these components and begin a process of migrating roles and permission lists toward the design philosophy noted above. Since this will have an impact across the other institutions using the shared instance, this effort will need to be coordinated amongst those institutions.

Institution Response

TMCC concurs with the auditor, “..this effort will need to be coordinated amongst those institutions [of the shared instance]”. As part of the Shared Instance, TMCC 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 is in the process of developing a re-architecture of the shared instance security infrastructure and an execution plan for that re-architecture. Chris Piekarz, Senior Security Analyst for SCS, will have this plan done by May 1, 2013. Mr. Piekarz has shared his ideas for the new design philosophy with Grant Dintiman, NSHE Internal Auditor. Mr. Dintiman is in agreement with creating a plan around this philosophy.

Since the rebuilding of the shared instance security infrastructure represents a significant commitment of resources, the plan will be reviewed by iSIA. If this rebuild plan is approved by iSIA, the rebuild effort will go forward. If iSIA does not approve the plan, all institutions of the Shared Instance will need to revisit how to comply with this audit finding.

TMCC Migration to the Shared Instance Design Philosophy

As the new roles and permission lists are developed by SCS, TMCC will assist in testing and developing narratives as described in audit item number one. This will be completed by Tommie Guy, Security Coordinator and Shanna Rahming, Business Analyst in cooperation with functional leads from Financial Aid, Admissions, Student Records, Outreach, Student Financials, and Advising.

Migration to the Shared Instance design philosophy will be accomplished as follows:

- **If it is found the new roles and permission lists meet our security needs, TMCC will replace our current security with that developed for the shared version.**

- Where it is found the shared version does not match our needs, TMCC will build new roles and permission lists that adhere to the shared instance design philosophy.

The exact time frame for this project will depend on SCS and shared instance resources and availability and is unknown at this point pending the completion of the execution plan and its review by the iSIA group. As mentioned above, Chris Piekarz, Senior Security Analyst for SCS expects to have the execution plan completed by May 1, 2013.

Follow-up Response:

As of October 25, 2013, TMCC understands that the rebuild plan was approved by iSIA. The rebuild of roles and permission lists is an ongoing project being conducted by System Computing Services. It is no longer in the purview of TMCC's audit response. We request that this finding be closed.

2. We noted 29 defined roles not assigned to any user profiles and 27 permission lists not assigned to any roles or users. 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 TMCC evaluate unassigned roles and permission lists to determine their need and eliminate any that are not necessary.

Institution Response

TMCC concurs with this recommendation. Shanna Rahming, TMCC Business Analyst, has evaluated unassigned roles and permission lists as suggested by the auditor. Mrs. Rahming has removed unassigned roles and permission lists that have no further purpose for TMCC PeopleSoft security. This review and deletion of unnecessary roles will continue every four months with the next examination taking place in August 2013 by Shanna Rahming, Business Analyst and Tommie Guy, Security Coordinator.

Follow-up Response:

As of October 25, 2013, this recommendation has been implemented and we request that this finding be closed.

SENSITIVE DATA ACCESS

We evaluated user access to 55 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, student admissions and records, student financials, academic advising and outreach. 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. We noted the following:

1. Four users had invalid roles, one user had terminated but was still active in the system and eleven users needed role changes.

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

Institution Response

TMCC concurs with this recommendation. Regular review of end-user security is a necessary step in providing efficient and strong security.

Functional Area Reports

Tommie Guy, Security Coordinator, will prepare functional area reports every four months (three times per year). These reports will be sent to the functional leads in Financial Aid, Admissions, Student Records, Outreach, Student Financials and Advising. The report will list PeopleSoft users who have access to roles and permission lists identified as belonging to their area. After review of the report by functional leads, the functional leads will make note of any changes they suggest. The list of these changes will be reviewed, edited and approved by Andrew Hughes, the TMCC Campus Solutions Service Manager and Registrar. The Security Coordinator will then make the changes. The last review by the functional leads was done in January and February 2013. The next reports will go out in April 2013 and every four months thereafter. Functional leads will have two weeks to respond. A non-response will be reported to Sharon Wurm, the TMCC Functional Project Lead for follow up.

Follow-up Response:

As of October 25, 2013, this recommendation has been implemented and we request that this finding be closed.

We also recommend that TMCC evaluate the notification process when employees change positions to ensure that the Security Coordinator is notified in a timely manner.

Institution Response

TMCC concurs with this recommendation and acknowledged the importance of timely removal of data access from individuals whose employment has been terminated or who have moved departments. As such, Tommie Guy, Security Coordinator has several processes in place to identify these individuals. Additionally, TMCC is implementing new constructs to increase shared information across departments. TMCC is also pursuing reliable and timely data on employee departures and department moves by being active in the Request for Proposal efforts for a new Human Resources System.

Identifying Terminated and Re-assigned Employees

In pursuit of timely removal of access from employees who have left employment with TMCC or moved departments, the Security Coordinator has five methods in place.

- **The Security Coordinator has lobbied for and received email reports from SCS that identify when an employee's HRS status data field is changed to a 'T' for terminated.**
- **The Security Coordinator prepares a bi-monthly report showing Peoplesoft users by department. This report is disseminated to department contacts. The department contacts are asked to review the report and relay back any information about terminations or department changes. TMCC will implement an additional step here beginning with the next report in April 2013. Any outstanding reports will be forwarded to the departmental head or their supervisor one week from the report's original date.**
- **TMCC has in place an Employee Exit Process Sign-off Checklist. The Human Resources department gives this form to departing employees. They are asked to take the form to the different departments, including Information Technology for sign-off. This process notifies us of a departure. Application access is removed for that person.**
- **Supervisors are asked to report an employee's departure/departmental move to the Security Coordinator through completion of an online Network Application for Security Access (NASA) request to remove access for that employee or through an email to the Security Coordinator.**
- **SCS provides monthly reports that are helpful to the Security Coordinator in identifying employees who are no longer employed. These are reviewed by**

the Security Coordinator monthly. Despite these five types of efforts, TMCC recognizes that employee departures sometimes go unnoticed. The reason an employee departure may not trigger a notice to the Security Coordinator is that they are kept on active status in HRS for valid reasons. And neither the supervisor nor the departing employee remembers to notify the Security Coordinator. To help address this, TMCC will:

- Ensure new HRMS system would provide timely notification of employee changes. It is the TMCC Security Coordinator's understanding that iNtegrate2, a new HRS system, may be able to provide timely information on employee departure dates. These concerns have been forwarded to Craig Scott, Director of Budget and Planning and Michele Meador, Chief Human Resources Officer. They represent TMCC's interest to Huron Consulting, the company writing the request for proposal (RFP) for iNtegrate2.**
- Implement an Employee Entrance Exit Notification system. A distribution list will be set up for all key staff involve in processing TMCC system set up for new or terminated employees. TMCC Personnel Analyst, Nicole Scollard will be setting up the notification system and protocols with staff from departments that consistently deal with the issues of new and departing employees. This group will be notified immediately by HR as employee status changes.**
- TMCC will also implement supervisor training to reinforce entrance and exit procedures for new and departing employees. This training will be conducted yearly as part of the Fall Professional Development Days, typically held in August.**

Follow-up Response:

As of October 25, 2013, Michele Meador, Chief Human Resources Officer, has been made aware of Information Security's concerns regarding the new HR software providing timely information on employee departures. Human Resources implemented an Employee Entrance Exit Notification system. Supervisor training on entrance and exit procedures is in the end stages of development and undergoing legal review for presentation on the regularly scheduled supervisor trainings. We request that this finding be closed.

We performed a more detailed review of Social Security Number (SSN) and Date of Birth (DOB) data due to their increased sensitivity. PeopleSoft provides the capability to mask the SSN and the birth year in the DOB on selected high use screens, however there are many more screens that do not mask the data. We observed the following issues.

2. Approximately 50 individuals have unintended access to SSN data through access to screens with unmasked SSN data.
3. Even though the option exists to mask the birth year on selected high use screens, that option has not been implemented.

We recommend that TMCC evaluate users with access to unmasked SSN data and ensure that they have a job related need for such access. Further, we suggest that TMCC work with other institutions in the shared instance and consider masking birth year on the high use screens.

Institution Response

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

The System Level Technology Solution

Masking of SSN is done at the system level. Currently, PeopleSoft's delivered masking mechanism is used on only two pages, RELATIONSHIPS and SCC_BIO_DEMO_PERS. Further masking of additional pages can only be accomplished by a modification. A modification is a technical term to describe programming changes at the system level. These typically require work by SCS and outside consultants. The delivered masking currently masks SSN only on the Search/Match page, with the default being to mask SSN for everyone on this page. To see an unmasked SSN, a person must be specifically provided with an additional role.

TMCC Review of Unmasked SSN Access

Tommie Guy, Security Coordinator and Shanna Rahming, Business Analyst are evaluating users with access to unmasked Social Security Number data and examining whether there is a job-related need to see this information. There are a limited number of users who have a job-related need to see unmasked SSN. These users are in the Financial Aid department. TMCC will remove access from users it finds do not have a job-related need to have such access. All removals will be completed by December 2013.

Follow-up Response:

As of October 25, 2013, the removal of roles containing unmasked SSN has begun. All removals will be completed by December 2013. We request that this finding be closed.

Masking Year in Date of Birth

Chris Piekarz, SCS Senior Security Analyst has brought the issue of using the delivered masking mechanism for birth year on high use screens to the attention of Ginger Holladay-Houston, SCS Director of Information and Application Services. Consequently, SCS has applied the mask in the test database for the year portion of date of birth (DOB) on the Search/Match page.

TMCC Review of Date of Birth Access

Tommie Guy, Security Coordinator, and Shanna Rahming, Business Analyst, will work with the TMCC user base to determine the business effect of the new masking and will also evaluate who needs to see full DOB on the Search/Match page. Within a month of SCS applying the mask in production, TMCC will restrict full DOB access from those not found to have a job-related need.

Follow-up Response:

As of October 25, 2013, this recommendation has been implemented and we request that this finding be closed.

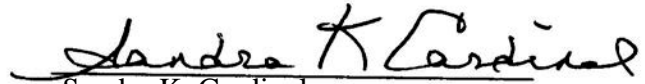
The Internal Audit Department would like to thank the Information Technology Services staff and other college employees for their cooperation and assistance during this review.

Reno, Nevada
January 25, 2013



Grant Dintiman

IT Auditor



Sandra K. Cardinal

Assistant Vice Chancellor for
Internal Audit

TMCC PeopleSoft Security Audit Update
Internal Audit Report
November 1, 2011 through January 10, 2013

#	Recommendation	Implemented	Update*	Est. Date of Completion
1	<p>Security Administration – Roles and Permissions</p> <p>We recommend that TMCC develop narrative descriptions for both roles and permission lists that 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).</p>	See update	<p>As of October 25, 2013, TMCC understands that every role and permission list in the PeopleSoft Shared Instance rebuild will be changed. Documentation of roles and permission lists will be automated and are a part of the rebuild plan approved by the iSIA and carried out by System Computing Services analysts Chris Piekarz and Eric March. This finding is no longer in the purview of TMCC’s audit response. We request that this finding be closed.</p>	Oct. 25, 2013
2	<p>Role and Permission List Usage and Design Philosophy</p> <p>We recommend that TMCC evaluate the design of these components and begin a process of migrating roles and permission lists toward the design philosophy noted above. Since this will have an impact across the other institutions using the shared instance, this effort will need to be coordinated amongst those institutions.</p> <p>We recommend that TMCC evaluate unassigned roles and permission lists to determine their need and eliminate any that are not necessary.</p>	See update	<p>As of October 25, 2013, TMCC understands that the rebuild plan was approved by iSIA. The rebuild of roles and permission lists is an ongoing project being conducted by System Computing Services. It is no longer in the purview of TMCC’s audit response. We request that this finding be closed.</p> <p>As of October 25, 2013, this recommendation has been implemented and we request that this finding be closed.</p>	<p>Oct. 25, 2013</p> <p>Oct. 25, 2013</p>

#	Recommendation	Implemented	Update*	Est. Date of Completion
3	<p data-bbox="272 279 675 531">Sensitive Data Access</p> <p data-bbox="272 352 675 531">We recommend that TMCC adjust these users as necessary and conduct regular reviews of user roles to ensure role assignments are correct.</p> <p data-bbox="272 573 675 825">We also recommend that TMCC evaluate the notification process when employees change positions to ensure that the Security Coordinator is notified in a timely manner.</p> <p data-bbox="272 1014 675 1413">We recommend that TMCC evaluate users with access to unmasked SSN data and ensure that they have a job related need for such access. Further, we suggest that TMCC work with other institutions in the shared instance and consider masking birth year on the high use screens.</p>	<p data-bbox="699 279 870 342">Yes</p> <p data-bbox="699 573 870 636">Yes</p> <p data-bbox="699 1014 870 1077">Yes</p> <p data-bbox="699 1224 870 1287">Yes</p>	<p data-bbox="894 279 1255 447">As of October 25, 2013, this recommendation has been implemented and we request that this finding be closed.</p> <p data-bbox="894 573 1255 1371">As of October 25, 2013, Michele Meador, Chief Human Resources Officer, has been made aware of Information Security's concerns regarding the new HR software providing timely information on employee departures. Human Resources implemented an Employee Entrance Exit Notification system. Supervisor training on entrance and exit procedures is in the end stages of development and undergoing legal review for presentation on the regularly scheduled supervisor trainings. We request that this finding be closed.</p> <p data-bbox="894 1413 1255 1707">As of October 25, 2013, the removal of roles containing unmasked SSN has begun. All removals will be completed by December 2013. We request that this finding be closed.</p> <p data-bbox="894 1749 1255 1877">RE: Masking birth year: As of October 25, 2013, this recommendation has been implemented and we</p>	<p data-bbox="1279 279 1429 342">Oct. 25, 2013</p> <p data-bbox="1279 615 1429 678">Oct. 25, 2013</p> <p data-bbox="1279 1455 1429 1518">Dec. 31, 2013</p> <p data-bbox="1279 1791 1429 1854">Oct. 25, 2013</p>

#	Recommendation	Implemented	Update*	Est. Date of Completion
			request that this finding be closed.	