UCPath Security

Introduction

The UCPath system at UCOP is based on Oracle|PeopleSoft's Human Capital Management platform.. While accommodations to individual locations were considered, UCPath Security is universally deployed based on strict guidelines and best practices in higher education systems.

The security control environment governs the process related to provision of access and use of the system.

UCPath Security Principles

UCPath Security design objectives were aimed at allowing users to process transactions in UCPath efficiently, accurately, and completely, while maintaining data integrity and control on the process and system levels. The objectives satisfy UC's ability to provide UCPath reporting assurance to internal and external stakeholders.

Some of the key objectives are:

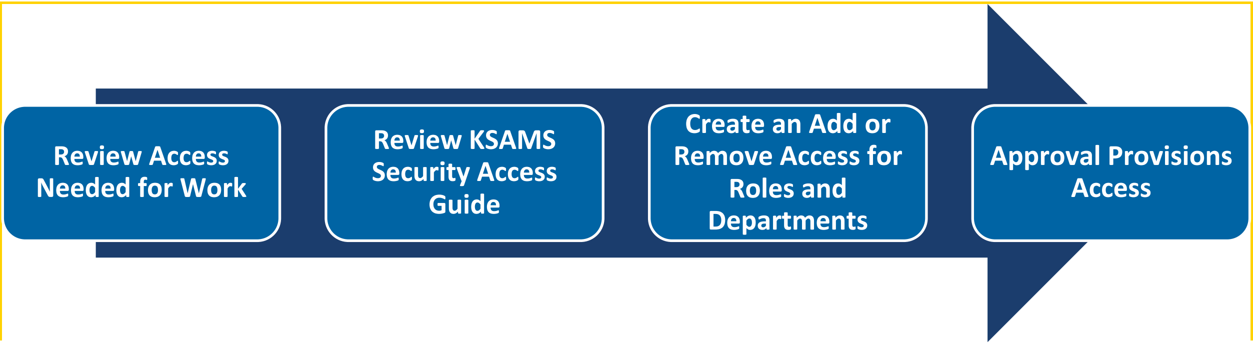
- Allow necessary access to let the user complete the activity in the business process
- Prevent user from gaining more access then is needed for performing their tasks
- Prevent user from getting access to transactions or reports for which the user is not responsible
- Maintain strict control on compensation-related information
- Maintain strict control on employee and contingent worker personal information
- Maintain strict control on pay related information
- Maintain segregation of duties in role assignment on user level so that one user cannot process a transaction end to end without checks

KSAMS process for UCPath Security

At UCI, the system of record for UCPath Security access requests and approval is KSAMS.

KSAMS is a university-wide "system of security record". The process in KSAMS is simplified for easy use and requires minimal training.

UCPath Security Access Management is a four-step process:


Review Access Needed for Work
Review KSAMS Security Access Guide
Create an Add or Remove Access for Roles and Departments
Approval Provisions Access

01 UCPath Roles Wiki is the primary resource to help understand what security roles the user needs to request. Roles Wiki provides an in-depth understanding of each KSAMS role.

02 KSAMS Security Access Guide for UCPath Access

03 Utilizing KSAMS, users create an access request to add or for removing existing access of a user. Note: There are two types of roles needed for a new user - Role security and Row Level security.

04

- KSAMS notification email is sent to user when role is provisioned
- User is able to navigate to pages in UCPath that Roles Wiki indicated they would have acces to
- User is able to bring up the people online in depts. they are approved to process

DSA Roles & Responsibilities

Department Security Administrators play a pivotal role in granting or revoking access for users in their respective departments, divisions, schools and colleges.

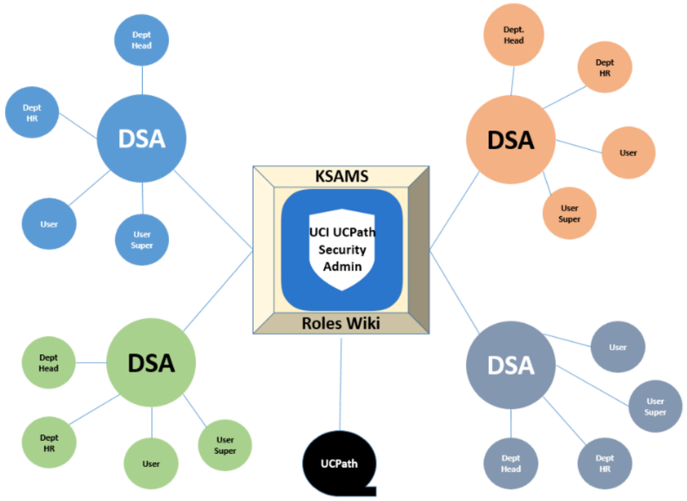


Figure 1 DSA in hub and spoke relationship

For UCPath Security Administration, DSA's are first level approvers. They work as facilitators in provisioning their department-user's security access to UCPath online system.

DSAs assist in determining appropriate access for user.

On an organization level, DSAs serve as delegates for the UCPath Security Administrators, on one hand, and as a point of contact for UCPath security questions and support, on the other, for their departments.

DSA POC

As a UCPath Security Point-of-Contact (POC), the DSA's interface internally with:

- Users
- Departmental Head
- User's supervisors
- Departments HR and Payroll staff

The DSAs also interface with UCPath Security Administration

DSAs periodically run reports off of KSAMS to review if users of the department should continue with current UCPath access.

The DSAs are responsible for the following:

1. When the Roles Wiki lists training modules as pre-requisites for a role, the DSA needs to verify all of the required training has been successfully completed by the user (who is requesting the role).
2. The DSA must review that the role(s) being requested are appropriate for the user's job and departmental responsibilities.
3. The DSA must check whether the user has previously assigned rolls that do not match responsibilities of their current job. For example, a user may have just transferred into the department and their previous roles were not removed.
4. The DSA must confirm that the population of employees the user can see in UCPath is appropriate and correct.

5. DSAs must keep a record of the user’s employment changes within the department and remove the user’s access after events such as transfers, job change, or separations.
6. DSA’s need to assist in validating and certifying a user’s security in periodic statements to UCPath Support group.

A DSA’s active and diligent participation in management of the UCPath security program is vital for the department’s assurance that their UCPath data is correct, complete and has integrity.

Conclusion

Virtually every employee and contingent worker has some level of access in the UCPath system and is therefore impacted by UCPath security. As UCPath is a system of record of an employee’s records and payroll, UCPath is critical for financial management of UCI. UCPath security has far reaching risk impacts that need to be managed collectively to ensure system integrity and operational control.