HOUSING & HOSPITALITY SERVICES

INFORMATION TECHNOLOGY

AUDIT REPORT #16-2222

# Audit & Advisory Service August 2016

HOUSING & HOSPITALITY SERVICES

INFORMATION TECHNOLOGY

AUDIT REPORT #16-2222

# Background

In accordance with the UCLA Administration fiscal year 2015-16 audit plan, Audit & Advisory Services (A&AS) conducted an audit of information technology (IT) controls within Housing and Hospitality Services (H&HS).

H&HS provides on and off-campus housing to approximately 17,000 students and faculty. It hosts visitors, campus departments, and alumni families through its conference and catering programs, the UCLA Guest House, the Lake Arrowhead Conference Center (LACC), and the Bruin Woods Family Resort.

H&HS IT provides technical support for financial and non-financial applications used by H&HS operational units. The technical support includes server administration, user administration, data back-up, and project planning. H&HS operational units employ system administrators who provide limited IT technical support. H&HS IT acts as a centralized control for the operational units.

The H&HS IT group consists of 20 career employees and 6 Full Time Equivalent (FTE) positions (comprised of 18 student workers). The H&HS IT Director oversees the operation, and reports to the Assistant Vice Chancellor for H&HS.

Purpose and Scope

The purpose of the audit was to evaluate the information systems control environment for business applications supported by H&HS IT. Where applicable, compliance with University policies and procedures was also evaluated.

The audit’s scope included interviews with H&HS IT and administrative personnel who work with the sampled business applications and focused on the following activities:

* Technical Controls
* User Access Administration
* Disaster Recovery and Business Continuity
* Back-up and Recovery
* Physical Controls

Audit work was conducted for selected H&HS IT administered applications and processes. As part of the testing, in addition to the H&HS network, five H&HS applications were selected for review. They include:

|  |  |
| --- | --- |
| **Application/System** | **Purpose** |
| Micros POS | Point of Sale system used throughout H&HS, including dining services. |
| Opera | A property management system which provides a variety of hospitality services. |
| ServicePro Help Desk (ServicePro) | H&HS IT service management system used to request and manage service requests. |
| StarRez | Residential management application used to manage student housing arrangements and payments. |
| Virtual Desktop | H&HS user desktop computer system. |

The audit was conducted in conformance with *the International Standards for the Professional Practice of Internal Auditing* and included tests of records, interviews, and other procedures considered necessary to achieve the audit purpose. Interviews were conducted with H&HS IT management and staff, and supporting documentation was also examined.

Summary Opinion

Based on the results of the work performed within the scope of the audit, the H&HS IT organizational structure and controls are generally conducive to accomplishing its business objectives surrounding IT controls. However, controls can be strengthened in areas outlined below.

Technical Controls

* Superuser activity for critical systems should be logged for Micros POS and ServicePro, where feasible. Also, superuser activity should be monitored periodically by an independent person for Micros POS, Opera, StarRez, ServicePro, and Virtual Desktop.
* Users should be suspended after successive invalid sign-on attempts for Micros POS. Also, for Opera and Micros POS, invalid sign-on attempts should be logged and monitored.

User Access Administration

* H&HS IT should ensure that separated and transferred employee access is disabled/adjusted in a timely manner.
* For Micros POS, management should consider implementing a process to ensure that a unique identifier, such as a University ID, is maintained for each user.

Disaster Recovery and Business Continuity

* H&HS IT should conduct a business impact analysis and update the current disaster recovery/business continuity plan.

The audit results and recommendations are detailed in the following section of the report.

# Audit Results and Recommendations

Technical Controls

Technical IT controls reviewed included those related to password security and system logon controls, change management, cybersecurity, operating system and database security, and patch management. The following were noted:

1. Superuser Access Review

Controls surrounding superuser activity can be strengthened. Superusers with privileged access to critical systems have access to modify applications, maintain/authorize access, and other vital administrative functions.

* Superuser activity for Micros POS and ServicePro is not logged.
* Superuser activity for Micros POS, ServicePro, and Virtual Desktop is not monitored.
* While superuser activity is logged for the Opera system, their activity is monitored by two Opera superusers. Also, for StarRez, one superuser is the same individual who approves any changes to the database.  As a result, because an independent person without superuser access does not monitor and approve changes, there is a lack of separation of function.

See table below for summary:

|  |  |  |  |
| --- | --- | --- | --- |
| **Application/System:** | **Number of Superusers:** | **Superuser activity is logged?** | **Superuser activity is monitored?** |
| Micros POS | 3 | No | No |
| Opera | 6 | Yes | Yes |
| ServicePro (Non-Critical System) | 4 | No | No |
| Virtual Desktop | 7 | Yes | No |
| StarRez | 5 | Yes | Yes |

According to guidance on privileged users stated in UC Business and Finance Bulletin IS-3, section III.C.2.b.iii, "activities performed using a privileged account should be logged, where feasible, and the logs should be reviewed on a regular basis by an independent and knowledgeable person."  Additionally, "use of privileged accounts should be monitored periodically to ensure they are being used for authorized purposes."

Recommendation: H&HS IT management should consider the feasibility of logging superuser activity for Micros POS and ServicePro. Also, superuser activity for Micros POS, Opera, StarRez, ServicePro, and Virtual Desktop should be periodically monitored by an independent and knowledgeable individual.

Response: Agreed.

* Superuser activity for Micros POS is logged and will be reviewed monthly by the Assistant Director of Operations. A report of the review and all findings will be provided to the Director on a monthly basis. The review will be documented in a service desk request. The first report will be completed on July 31, 2016.
* Service Pro does not provide logging functionality and is not a critical system. H&HS IT management is implementing a new service desk system, KACE, with greater functionality and features. The requirements for logging and review of Superuser activity will be addressed with this implementation. The KACE system will be implemented by October 31, 2016.
* All Virtual Desktop maintenance activities require that a Change Control form be reviewed and approved by the H&HS IT Director prior to implementation. This serves as a control for logging and monitoring Superuser activity. H&HS IT has a Change Control process which has been in effect for approximately the last two years.
* The StarRez system is managed by the H&HS Housing Services department. H&HS IT and will work with Housing Services to ensure that the appropriate separation of duties is established as well as determining any recommended process improvements.

1. Invalid Sign-on Logging and Monitoring

Based on audit review, the following regarding system login controls were noted:

* The Micros POS system does not suspend a user ID after successive invalid sign-on attempts.
* Micros POS and Opera do not log invalid sign-on attempts.  H&HS IT management indicated that an upcoming upgrade to Micros POS would include an update to include the functionality to such attempts.

It is best practice to suspend a user ID after successive invalid sign-on attempts and, to log and monitor invalid sign-on attempts to help deter unauthorized access to systems.

Recommendation: Management should consider the feasibility of suspending a user ID after successive invalid sign-on attempts to the Micros POS system. Also, logging of unsuccessful user logon attempts for Micros POS and Opera should be considered.  These logs should be periodically monitored and unusual activity should be appropriately investigated.

Response: Agreed.

* Opera currently locks out a user after 3 invalid logon attempts.
* H&HS IT management will work with the Micros POS vendor to implement controls for invalid log-on attempts including processes to log and monitor invalid sign-on attempts to help deter unauthorized access to systems. This will be completed by August 31, 2016.

User Access Administration

Audit review included interviews and reviewing a judgmentally selected sample of 25 users on the H&HS network, Opera, Micros POS, ServicePro, and StarRez applications. Testing included verification that the users had been granted access by an individual with proper authority and that access was appropriate for their job responsibilities. Also, a Campus Database Warehouse (CDW) report of separated and transferred employees between January 1, 2015, and February 18, 2016, was reviewed, and a sample of 10 individuals was selected for further analysis to verify that separated and transferred employee access was deleted and/or adjusted in a timely manner. Further, related user listings were reviewed to ensure that only active employees have proper systems’ access.

*Access Policies & Procedures*

H&HS IT has adequate polices and procedures in place for granting user access to the H&HS network and sampled systems.  Users are granted a minimum amount of access required to successfully fulfill their job requirements.  H&HS IT is responsible for administering and monitoring user access to the H&HS IT Network and for several systems/applications used by business units.  To grant a user access, the business unit submits a Service Request (SR) through the ServicePro Help Desk. The SR is maintained by H&HS IT to track users' access.  H&HS IT grants network access levels based on users' roles and responsibilities.  H&HS IT uses a daily hire/termination/transfer listing from Human Resources (HR) to help that ensure access is only given to appropriate users and to remove access when needed.

1. Separated/Transferred Employees

The following was noted for the judgmental sample of 10 separated/transferred

employees selected for review.

* One employee was transferred to another department on October 11, 2015, but was an active user on the Micros POS user listing as of January 20, 2016. In this instance, H&HS IT management indicated that the Micros POS team within H&HS IT did not receive the HR new hire/transfer/termination listing.
* One employee separated from the University on April 30, 2015, but their systems access was not disabled until June 2015. H&HS IT management explained that this occurred because a staff member who was responsible for disabling access was on extended leave. Since this occurrence, H&HS IT management has developed new written procedures to ensure that there is back-up in the event staff members are on extended leave.

Recommendation: Management should ensure that separated and transferred employee access is disabled/adjusted in a timely manner to help deter unauthorized access to systems and applications.

Response: Agreed. The H&HS New Hires/Terminations list is now reviewed daily and the network accounts are disabled upon separation. The Senior Administrative Analyst confirms the network account has been disabled. The Assistant Director of Operations then reviews these activities on a monthly basis.

The Micros POS database administrator receives the H&HS New Hires/Terminations list daily and accounts are disabled upon separation. The Assistant Director of Operations will perform a sample review of disabled Micros POS accounts on a monthly basis with a report of accounts reviewed and findings submitted to the Director beginning on August 31, 2016. All activities including accounts disabled and accounts reviewed will be logged in a service desk requests.

1. User Access – Micros POS

Based on user access testing, for 2 out of 25 employees, A&AS could not verify that the individuals' Micros POS access was commensurate with their job description.  These two individuals had common names and their University ID (UID) could not be determined based on the information provided. Micros POS is not connected to Active Directory, which H&HS IT uses as the repository for all H&HS network user information, such as individuals’ UID. As a result, A&AS could not validate the two individuals’ employment status and title via OASIS.

Recommendation: H&HS IT management should consider maintaining a record of UID, or other unique personal identifier, for all Micros POS users. The UID provides a unique identifier to validate user identification when granting, managing, and removing access.

Response: Agreed. The UID for the user will be entered into Micros POS as a part of the account creation process.

Disaster Recovery and Business Continuity

Based on audit review, H&HS IT does not have an up-to-date disaster recovery/business continuity plan. The disaster recovery/business continuity plan was last tested in March 2013. However, the test was not formally documented. Also, the last Business Impact Analysis was prepared in 2008.

A disaster recovery/business continuity plan helps outline the actions needed for short-term and long-term recovery of resources and mission-critical functions. Continuous updates to the disaster recovery/business continuity plan are needed to ensure that H&HS IT addresses emerging and changing risks. Also, plans should be tested periodically to ensure that they are effective in reducing risk and minimizing disruption to H&HS activity in the event of an emergency or disaster.

According to the UC Business and Finance Bulletin IS-12: Continuity Planning and Disaster Recovery, disaster recover plans should be tested on a periodic basis and plans should be updated to reflect changing environments, processes, technology, or other impacts as appropriate.

Recommendation: Management should update the current disaster recovery/business continuity plan.  Also, a business impact analysis should be conducted in order to reflect current processes and to aid in disaster recovery/business continuity planning.  The disaster recovery/business continuity plan should be tested periodically and the test should be documented.

Response: Agreed. H&HS IT management will be working with other H&HS departments and the Business Continuity Planner from Insurance and Risk Management to develop a disaster recovery and business continuity plan. Requirements for periodic testing of the plan as well as quarterly reviews will be incorporated into the plan. The completion date to develop the scope of work and activities timeline is December 31, 2016.

Back-up and Recovery

H&HS IT personnel perform the back-up functions for all H&HS IT systems and the systems are regularly backed up. Also, database files, operating system files, and other files necessary for recovery of the server in the event of a disaster are regularly backed up. The primary backup for all mission critical data is performed daily to a near-line backup storage system on the DataDomain appliance (located at the Campus Data Center). Additionally, backup is performed daily to Microsoft Azure Cloud Solutions, a cloud computing platform.

Data from back-up media are periodically restored, which occurs at least three to six times per year. H&HS IT routinely restores and reconfigures test servers and systems that validate the recovery processes. An inventory of back-up media is managed by the CommVault backup system.

No significant control issues were found in this area.

Physical Controls

The servers for H&HS systems are in two areas. The Campus Data Center (CDC) in the Math Science building houses 80% of H&HS’ servers, while 20% of H&HS’ servers are located in Covel L-21. The CDC is managed by UCLA Information Technology Services (IT Services) and was not included in the scope of the audit review.

The Covel L-21 Server Room has adequate physical controls and is located away from any potential hazards. The server room is outfitted with fire suppression systems and raised floors, ISO-Based Seismic Isolation Platforms to protect servers in the event of an earthquake, primary and back-up cooling systems, exhaust vents, and heat, smoke and moisture alarms.

Also, physical access to the Covel L-21 server room is controlled by an Onity lock on the door and only authorized personnel are granted access to the server room. Authorized personnel access the room using the individual's Bruincard. Permission for access is granted by the H&HS IT Director or Assistant Director. A&AS reviewed the listing of all personnel with access to the server room and verified that access was appropriately restricted to authorized individuals

No significant control issues were found in this area.

160511-2  
REP