UCLA AUDIT & ADVISORY SERVICES

Edwin D. Pierce, CPA, CFE
Director

10920 Wilshire Boulevard, Suite 700
Los Angeles, California 90024-1366
310 • 794-6110
Fax: 310 • 794-8536

September 4, 2015

SENIOR VICE PRESIDENT/CHIEF COMPLIANCE AND AUDIT OFFICER SHERYL VACCA
EXECUTIVE VICE CHANCELLOR & PROVOST SCOTT WAUGH:

Re: Housing & Hospitality Services – Access Controls Audit Report #15-2230

Enclosed is the audit report covering our review of Housing & Hospitality Services' (H&HS) Access Controls unit. The primary purpose of the audit was to ensure that Access Control's organizational structure and controls are conducive to accomplishing its business objectives.

The scope of the audit included:

- Electronic Key Cards
- KeyWatcher System

Based on the results of the work performed within the scope of the audit, the organizational structure and control procedures regarding Access Controls' activities are generally conducive to accomplishing the unit's business objectives.

However, management could further strengthen controls by securing emergency master key cards, emergency sub-master key cards, and KeyWatcher override keys, with tamper-evident locks that are under camera review.

The corrective actions implemented by management satisfactorily address the audit concerns and recommendations contained in the report. In accordance with our follow-up policy, a review to assess the implementation of our recommendations will be conducted approximately four months from the date of this letter.

Please feel free to contact us if we can be of further assistance.

Edwin D. Pierce, CPA, CFE
Director

Enclosure

cc: S. Olsen

150904-5

HOUSING & HOSPITALITY SERVICES

ACCESS CONTROLS AUDIT

AUDIT REPORT #15-2230

Audit & Advisory Services

September 2015

HOUSING & HOSPITALITY SERVICES
ACCESS CONTROLS AUDIT
AUDIT REPORT #15-2230

Background

In accordance with the UCLA Administration fiscal year 2014-15 audit plan, Audit & Advisory Services (A&AS) has conducted an audit of Housing & Hospitality Services' (H&HS) Access Controls unit.

Access Controls serves the following On-Campus Housing (OCH) residential areas:

High Rise Residence Halls

- Dykstra Hall
- Hedrick Hall
- Rieber Hall
- Sproul Hall

Residential Suites

- Hitch Suites
- Saxon Suites (under construction)

Residential Plazas

- De Neve Plaza:
  - Acacia and Birch
  - Cedar and Dogwood
  - Evergreen and Fir
  - Gardenia Way & Holly Ridge
- Hedrick Summit
- Rieber Vista & Rieber Terrace
- Sunset Village:
  - Canyon Point
  - Courtside
  - Delta Terrace

The external doors to OCH residential buildings are locked 24 hours a day, seven days a week. Residents and staff must swipe their BruinCard to enter residential buildings and elevators up to the living areas. Access to residents' rooms, bathrooms, and study spaces is controlled by a separate electronic key card system called Onity. Residents must swipe their Onity key card and enter a Personal Identification Number (PIN) to access their rooms. For privacy, protection, and Family Educational Rights and Privacy Act (FERPA) compliance, Onity key cards only bear a manufacturer's card number, and no other identifiers.

The management of Onity key cards is performed by Access Control, a unit within OCH. Key cards and access privileges are issued and granted based on housing assignment or staff responsibilities. Encoding of electronic key cards for staff, master key cards, and sub-master key cards is restricted to Administrators. Encoding of electronic key cards to residential rooms is performed by Front Desk Attendants. There are four Front Desks that serve the OCH residential buildings:

- Rieber Hall Front Desk: Rieber Hall, Rieber Vista and Rieber Terrace.
- Sproul Hall Front Desk: Sproul Hall and Sunset Village.
- Hedrick Hall Front Desk: Hedrick Hall, Hedrick Summit and Hitch Suites.
- Acacia Building Front Desk: All De Neve Plaza buildings.

Purpose and Scope

The purpose of the review was to ensure that Access Control's organizational structure and controls are conducive to accomplishing its business objectives.

The scope of the audit focused on the following activities:

- Electronic Key Cards
- KeyWatcher System

The review was conducted in conformance with the *Internal Standards for the Professional Practice of Internal Auditing* and included tests of records, interviews with key personnel, and other auditing procedures considered necessary to achieve the audit purpose.

Summary Opinion

Based on the results of the work performed within the scope of the audit, the organizational structure and control procedures regarding Access Controls' activities are generally conducive to accomplishing the unit's business objectives.

However, management could further strengthen controls by securing emergency master key cards, emergency sub-master key cards, and KeyWatcher override keys, with tamper-evident locks that are under camera review.

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

Audit Results and Recommendations

Electronic Key Cards

General Building and Room Access Controls

Exterior building doors to OCH residential buildings are locked 24 hours a day, seven days a week, and residents must swipe their BruinCard to gain entry. All residents' rooms and bathrooms are equipped with an Onity key card system. Residents must insert their Onity key card and unique four digit PIN to enter their rooms. A&AS staff conducted a tour of a judgmental sample of two OCH residential buildings to verify the general building and room access controls in place.

A judgmental sample of access to ten residents' doors from ten different OCH residential buildings were reviewed, noting that only the assigned residents and appropriate staff were granted access. In addition, access for residents is set to expire on the last day of each school year, which is when they need to move out.

Also, based on discussions with Access Controls management, A&AS staff determined that Access Monitors are strategically stationed in certain OCH residential buildings overnight to ensure that only authorized guests and residents enter the buildings.

There were no significant control weaknesses noted in this area.

Master, Sub-Master, and Emergency Key Cards

Master key cards provide access to all Onity locks within a building. Sub-master key cards can be programmed for sections or floors of buildings or types of rooms (e.g. restrooms).

Emergency key cards for the fire department are secured in Knox Boxes outside the entrances to the OCH residential buildings. Access to the Knox Boxes is limited to the fire department and UCLA fire marshal.

Resident Assistants (RAs) live in the halls and buildings, and are responsible for student welfare and programming. A sub-master key card, which opens all rooms under their responsibility, is secured in tamper evident key boxes, in each of the RAs' rooms.

A&AS staff determined if master, sub-master, and emergency key cards are adequately secured by conducting a tour of a judgmental sample of two OCH buildings. The majority of master and sub-master key cards are stored in KeyWatcher cabinets, which require valid fingerprint authentication to open and users are only able to retrieve the master and sub-master key cards they have been granted access to.

However, the following concern was noted:

A. <u>Master and Sub-master Key Cards Storage</u>

Accountability over emergency master and sub-master key cards in Hedrick Hall warrant improvement. There are 36 master and sub-master keys stored in an unlocked wall cabinet in the back office area. Although access to the back office area is restricted to front desk staff, if a key card were missing, it would be difficult to hold any one person accountable.

<u>Recommendation:</u> In order to ensure that accountability over master and sub-master key cards are maintained, management should consider storing these key cards in containers with tamper-evident locks. Also, these tamper-evident containers should be stored in areas covered under security camera surveillance.

Response: Access Control concurs. Management will purchase boxes with tamper-evident locks to store these keys, which will be placed under security camera surveillance.

Onity Security and User Access Controls

A unique user ID and password is required to access the Onity electronic key card system to perform all key card access administration and encoding. A security hierarchy has been defined that restricts the ability to administer access only for certain buildings, doors, and users. At the top of hierarchy are Onity system administrators, who can grant access to all doors for all OCH buildings, for all types of key card users including residents and staff, and they have full access to load and use the Extended Portable Programmers (XPPs).

System administrator access was reviewed, noting that access is limited to four Access Control personnel, who are responsible for Onity system administration, or are backups. Area managers only have access to the group of OCH residential buildings they are responsible for. Residence Hall and Assistant Residence Hall Managers only have access to the doors, residents, and staff for the courts they are responsible for. Front desk workers only have access to residents' doors, not staff. We reviewed Onity access granted for a judgmental sample of six different levels of OCH staff, noting that access is granted based upon job responsibilities.

There were no significant control weaknesses noted in this area.

Extended Portable Programmers

XPP is a portable hand-held device that is used to program, update, and, in emergency cases, open the Onity door locks. There are ten XPPs: one for each of the four Front Desk areas, four for OCH Maintenance, and two for Access Control. Access to XPPs was reviewed to ensure the devices are secured and restricted to authorized users, noting that XPPs are secured in the KeyWatcher cabinets or safes at each of the front desks. In order to use an XPP, a valid four digit PIN must be entered and the doors that need to be accessed must be loaded onto the XPP. The ability to load door access files onto the XPPs is restricted to authorized users. XPPs are set to time-out after one minute of inactivity.

There were no significant control weaknesses noted in this area.

KeyWatcher

OCH uses the KeyWatcher Touch cabinets and system to secure and control access to master and sub-master key cards, hard keys, vehicle keys, and XPPs. The KeyWatcher Touch cabinets are bolted to the walls and fingerprint authentication is required to access the items stored inside. Users can only retrieve keys that they have been granted access to based on their assigned security group.

There are nine KeyWatcher Touch cabinets located throughout OCH. There is one at each of the four OCH front desks, two in the OCH maintenance area, one at UCLA Catering, one for the UCLA meeting rooms, and one for the Athletics' tutoring program.

Physical access controls for the KeyWatcher Touch cabinets were reviewed by observing the location of a judgmental sample of two cabinets and how they are secured. The KeyWatcher Touch cabinets reviewed are located in restricted areas that are covered by security camera surveillance, and are locked requiring fingerprint authentication to open and remove items from the cabinets. The KeyWatcher System Administrator indicated the other seven KeyWatcher Touch cabinets are secured in the same manner.

Access to the key rings stored inside the KeyWatcher Touch cabinets was reviewed to ensure that only appropriate staff have access to remove keys based on their job responsibilities. Ten key rings from the Covel and Hedrick Hall KeyWatchers were judgmentally selected and reviewed, noting that staff had been granted access only to the key rings they need based on their job responsibilities. Also, A&AS staff reviewed and verified that system administrator level access to the KeyWatcher system is restricted to authorized Access Control personnel. Further, A&AS determined that the KeyWatcher system tracks the removal of all keys and a daily report that identifies all keys that have not been returned is reviewed by management.

Remote access to KeyWatcher Touch cabinets is available for technical support purposes. We discussed how remote access is secured with the KeyWatcher System Administrator, noting there are multiple layers of security in place. In order to connect remotely, a user would need to authenticate with a valid password to the remote access application, know the IP address of the KeyWatcher Touch cabinet, and then authenticate to the KeyWatcher system with a valid PIN.

Emergency override keys are available to manually open the KeyWatcher Touch cabinets in the event of a technical issue and the cabinets cannot be opened electronically. A&AS staff observed where the override keys are stored at Covel to ensure that they are adequately secured and there is accountability when the keys are used.

Based on audit review, the following concern was noted:

A. KeyWatcher Override Keys

While areas where the four override keys for the KeyWatcher Touch cabinets are stored are restricted by card key access to staff and covered by security camera surveillance, accountability over the use of three of these keys could be strengthened.

Accountability is maintained over the override key stored in the Covel KeyWatcher, as fingerprint authentication is required to access it. However, the other three override keys are stored in the following areas in Covel:

- Two override keys are stored in the KeyWatcher System Administrator's unlocked desk drawer.

- One override key is stored in an unlocked wall mounted box.

Under current business practices, if a key were missing, it would be difficult to hold any one person accountable.

Recommendation: Management should consider storing override keys to the KeyWatcher Touch cabinets in tamper-evident containers to better enable identification of when these keys are used. Management should also evaluate if there is a need for four emergency override keys, or if the number of keys can be reduced.

Response: Access Control concurs. Management will continue to store one override key in the KeyWatcher Touch cabinets. An additional key will be stored in the wall-mounted box, which will be retrofitted with a tamper-evident lock. The remaining keys will be destroyed.