UC RIVERSIDE: AUDIT & ADVISORY SERVICES

July 28, 2014

To: Jadie Lee
Associate Vice Chancellor, Human Resources

Subject: Privacy and Confidentiality

Ref: R2014-11

We have completed our Privacy and Confidentiality audit in accordance with the University of California, Riverside Audit Plan. Our report is attached for your consideration. We will perform audit follow-up procedures in the future to review the status of management action. This follow-up may take the form of a discussion or perhaps a limited review. Audit R2014-11 will remain open until we have evaluated the actions taken.

We appreciate the cooperation and assistance provided by campus personnel contacted to complete this audit. Should anyone have any questions concerning the report, please do not hesitate to contact me.

Gregory Moore
Director

xc: UCR Audit Committee Members
Executive Director & Chief Technology Officer Grant
Director, Computing Infrastructure & Security Harvey

UNIVERSITY OF CALIFORNIA AT RIVERSIDE

AUDIT & ADVISORY SERVICES

MEMBER OF ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

REPORT R2014-11

PRIVACY AND CONFIDENTIALITY

JULY 2014

Approved by:

_____	_____
Robin A. Maras	Rodolfo Jeturian
Principal Auditor	Assistant Director

_____

Gregory Moore
Director

UC RIVERSIDE
PRIVACY AND CONFIDENTIALITY
AUDIT REPORT R2014-11
JULY 2014

I. MANAGEMENT SUMMARY

Based upon the results of work performed within the scope of the Privacy and Confidentiality audit, it is our opinion that, overall, the system of internal controls established to protect the privacy and confidentiality of information retained by the University of California, Riverside (UCR) campus is operating effectively in compliance with applicable policies and procedures.

Positive observations included:

- Computing and Communications (C&C) has established regular, automated internal scans of the UCR campus network in an effort to identify and block network security intrusions.

- All 20 personnel file custodians (from 12 UCR departments) interviewed regarding personnel files properly maintained their medical information/documentation in a manner consistent with policy.

However, during a review of the security and management of internal controls over a sample of UCR staff personnel files (213 files from 12 departments), we observed several areas that need enhancement to strengthen controls and/or effect compliance with best practices and University policy:

- Documentation – Required documentation (including Performance Appraisals, State Oath of Allegiance, Patent Agreements, etc.) was not included in all personnel files in one department. (Observation III.A)

- Access – Access to personnel files was not sufficiently restricted in accordance with UC Policy PPSM-80: Staff Personnel Records in two departments. (Observation III.B)

- Training – Five of 12 personnel file custodians have been inadequately trained in the area of personnel file maintenance. (Observation III.C)

- I-9 Documentation – I-9 forms and documentation were not properly managed by most personnel file custodians. (Observation III.D)

II. INTRODUCTION

A. PURPOSE

UCR Audit & Advisory Services (A&AS), as part of its annual Audit Plan, conducted an audit regarding privacy and confidentiality to evaluate

compliance with University policies and procedures, effectiveness of selected operations, and adequacy of internal controls.

B. BACKGROUND

UCR is the owner of the confidential information it collects; therefore, the University has several policies concerning privacy and confidentiality in an effort to educate information users of their rights and responsibilities regarding confidential data. UCR reserves the right to deny access to those who fail to use such data in accordance with the policies, as well as all applicable laws such as the Health Insurance Portability and Accountability Act (HIPAA) and Family Educational Rights and Privacy Act (FERPA).

UCR is committed to protecting the privacy of its students, alumni, parents, faculty, and staff. This protection extends to electronic data and information technology resources, as well as confidential print data including employment contracts, personnel files, etc. University employees and students working in campus offices, who have access to non-public information about others, must not disclose such information. If a security breach of electronic or print data is found to have occurred, UCR must give notice of such breach to the affected persons in the most expedient time possible.

While every department at UCR deals with aspects of privacy and confidentiality, there are two departments whose fundamental responsibilities involve protecting the campus from unauthorized privacy disclosures: Human Resources (Labor Relations) and C&C. Human Resources (Labor Relations) is responsible for private and confidential activities such as managing disciplinary actions, dismissals, layoffs, and employee disputes. C&C is responsible for activities such as protecting campus networks from security breaches and helping to ensure that private data remains safe from intrusion. Employees from both of these departments were interviewed for this audit.

C. SCOPE

A&AS conducted interviews with 20 personnel file custodians from 12 UCR departments, as well as reviewed a sample of 213 personnel files.

Additionally, A&AS interviewed the Chief Information Officer, Chief Technology Officer, Senior Director for Technology Operations, Computing Infrastructure and Security Director, and Services Enterprises Director regarding UCR network security, as well as reviewed process documentation for UCR network scanning activities.

Our substantive audit procedures were performed from August to October 2013. Accordingly, this report is based on our knowledge as of that time and should be read with that understanding.

III. OBSERVATIONS, RECOMMENDATIONS, AND MANAGEMENT RESPONSES

A. Documentation

Required documentation (including Performance Appraisals, State Oath of Allegiance, Patent Agreements, etc.) was not always included in all personnel files.

COMMENTS

Per the document *"Best Practices for Maintaining Personnel Files"* disseminated by UCR Human Resources on September 3, 2013, there are certain documents that must be maintained in every staff employee's personnel file. These documents include such items as the employee application, resume, State Oath of Allegiance, patent agreement, W-4 form, performance appraisals, etc. Additionally, per UC Policy PPSM-80: Staff Personnel Records, Section III.A*., "An employee's personnel records shall contain only material which is necessary and relevant to the administration of the staff personnel program."*

Based on our review, one department was missing required documentation in 14 of 24 (58%) personnel files.

RECOMMENDATION

A directive should be conveyed from Human Resources requiring all UCR personnel file custodians to conduct a review of their staff personnel files, determine if the files are complete based on the information in *"Best Practices for Maintaining Personnel Files,"* and obtain any missing documents from applicable employees.

MANAGEMENT RESPONSE

The referenced document was initially created in 2002, but was most recently revised and disseminated in July 2014. It reflects the provisions of PPSM 80: Staff Personnel Records which was issued in 2001, and is readily available on the campus HR and Payroll websites.

HR has communicated electronically and through presentations to the Financial & Human Resources Officers Group (FHROG) in July 2014 and the Payroll/Personnel System (PPS) User's Group (with a refresher scheduled for August 2014) regarding this issue. This item will be implemented by October 1, 2014.

B. **Access**

Access to personnel files was not sufficiently restricted.

COMMENTS

Personnel files should be secured in areas or cabinets with restricted access. These areas or cabinets should be locked and only those employees directly involved with maintenance of the files should possess keys. Per UC Policy PPSM-80: Staff Personnel Records, Section III.A, *"…appropriate and reasonable safeguards shall be established by the location to ensure security and confidentiality."*

While all departments reviewed maintained the staff personnel files in locked areas or cabinets, one of 12 (8%) departments had multiple workers with access to keys to the secured personnel files. This observation was corrected during the audit period and does not require follow-up.

RECOMMENDATION

A directive should be conveyed from Human Resources requiring all UCR personnel file custodians to determine which employees are essential to the function of maintaining personnel files and the keys to the locking areas or cabinets should be limited to such employees. Any keys held by non-essential employees should be collected and secured.

MANAGEMENT RESPONSE

HR has reminded UCR personnel file custodians of the importance of key control with respect to personnel files. Additionally the information contained in *"Best Practices for Maintaining Personnel Files"* has been expanded to clarify this expectation, and to provide for regular review of access to keys.

C. **Training**

Personnel file custodians have been inadequately trained in the area of personnel file maintenance.

COMMENTS

In our interviews with personnel file custodians from 12 UCR departments, five of 12 (42%) stated that they felt inadequately trained in the area of personnel file maintenance. These custodians commented that their knowledge about personnel files was taught to them by previous custodians in their respective departments, rather than from official training courses. Additionally, training on I-9 documentation and management was offered by the UCR International Scholar Center three times during 2013. However, five of 12 (42%) of the department

personnel file custodians did not attend the course and therefore, were not current with the essentials of I-9 management.

RECOMMENDATION

UCR Human Resources should consider providing training courses for all UCR personnel file custodians on personnel file maintenance and I-9 management, possibly through the UC Learning Center.

MANAGEMENT RESPONSE

Training has historically been provided in person to the PPS User's Group, and the associated PowerPoint presentation has been available on the HR and Payroll website since its creation. HR is also adding this information to the Learning Management System (LMS) as a training course so that a record of completion can be maintained. As indicated, in-person campus training on the I-9 process is currently provided by the International Scholar Center (ISC) and HR coordinates on content with the ISC to ensure that it is consistent with policy. Furthermore, systemwide I-9 training resources are currently being developed by a systemwide workgroup, and will be shared with the campus when available. This item has an estimated implementation date of February 1, 2015. However, this estimated date is contingent upon the completion of the I-9 training resources by the systemwide work group. If the I-9 training resources are not completed by February 1, 2015, we will reevaluate the progress and revise the implementation date.

D. **I-9 Documentation**

I-9 forms and documentation were not properly managed by most personnel file custodians.

COMMENTS

I-9 forms and documentation were not effectively managed by most personnel file custodians in the following ways:

- Per I-9 training given by the UCR International Scholar Center in 2013, the I-9 forms retained by a department should not be kept in the personnel files but should be maintained in separate folders. If UCR was subjected to an audit by U.S. Citizenship and Immigration Services (USCIS) or the U.S. Department of Labor (DOL), the expectation is to provide all I-9 forms to the officials within three business days, which may be problematic for larger departments if the I-9s are not filed separately. Seven of 12 (58%) departments were found to have I-9 forms in the personnel files.

- Per I-9 training given by the UCR International Scholar Center in 2013, as well as the USCIS OMB No. 1615-0047 (Form I-9 Instructions), while photocopies of I-9 support documentation are not required, if a department chooses to retain copies of the supporting documentation, the department must be consistent and retain copies for all new hires and reverifications. Four of 12 (33%) departments were not consistent in retaining I-9 support documentation for their employees.

- Copies of employee personal identification documents, including drivers' licenses, passports, social security cards, birth certificates, Resident Alien cards, U.S. Visas, etc., were located in the personnel files for 11 of 12 (92%) departments. While these personal documents were copied during the process of I-9 verification, the USCIS Form I-9 "Instructions for Employment Eligibility Verification", Page 3 of 9 states: *"Employers may, but are not required to, photocopy the document(s) presented."* Additionally, per UC Policy PPSM-80: Staff Personnel Records, Section III.A*., "An employee's personnel records shall contain only material which is necessary and relevant to the administration of the staff personnel program."*

Due to the highly personal nature of the identification documents reviewed for I-9 forms, as well as the risk of identity theft, best practice suggests that access should be highly restricted to I-9 information and copies of an employee's personal identification should not be retained. Personal identification documents are not required to be copied by the USCIS when completing an I-9 form and therefore, should be highly protected.

RECOMMENDATION

Human Resources should address the risk of identity theft by evaluating the possibility of removing sensitive personal identification documents from personnel files. Contingent upon management's determination, A&AS recommends personal documents be shredded and copies of employee personal identification documents not be retained at the department level. If there is any need for I-9 supporting documentation to be retained, the documents should be securely stored in the Human Resources office.

MANAGEMENT RESPONSE

The Department of Homeland Security website provides information on storing I-9 forms and includes the following statement, "You should store completed Forms I-9 and any copies of documents in a manner that fits your business needs." The current campus practice is consistent with this guidance.

We recognize the concerns that led to this recommendation and there is currently a systemwide workgroup examining the issue of I-9 processing. The workgroup will develop guidelines and standards, including best practice business processes, for I-9 completion at UC. The group includes representatives from Human Resources, Academic Personnel, Financial Management, Information Technology Services, and UC Path in consultation with the Office of General Counsel.

As part of this effort, a Request for Proposal is being submitted to several vendors to provide a proposal and pricing for an automated solution (including document storage) for I-9 integration at all locations. Additionally, an online resource guide is being developed by the systemwide work group. When the guide is completed, HR will again review campus procedures and training materials and update as appropriate. This item has an estimated implementation date of February 1, 2015. However, this estimated date is contingent upon the completion of the guide by the systemwide work group. If the guide is not completed by February 1, 2015, we will reevaluate the progress and revise the implementation date.