AUDIT & MANAGEMENT
AMAS
ADVISORY SERVICES

Internal Audit Report

Information Management of Sensitive Data - User Awareness

Report No. SC-18-01
December 2017

James Dougherty
Auditor in Charge - Principal Auditor

Steve Architzel
Assisting - Principal Auditor

Approved
Barry Long, Director
Audit & Management Advisory Services

UC SANTA CRUZ

Table of Contents

I. EXECUTIVE SUMMARY

Audit & Management Advisory Services (AMAS) has completed an audit of information management of sensitive data – user awareness to determine the level of awareness for marking, transmitting and storing manual and electronic data containing various levels of sensitivity, and to evaluate the controls in place to help ensure sensitive information is secured in compliance with relevant policies and regulations.

Overall, the awareness on campus of information sensitivity levels and an understanding on how to treat sensitive information varied. Based on our survey and review of available campus guidance, controls were in place to provide a reasonable but less than optimum level of assurance that sensitive information was secure and in compliance with relevant policies and procedures. Opportunities for improvement are identified below.

We surveyed the campus with questions that covered such topics as adequacy of training; awareness of where sensitive information is; how access to sensitive information is restricted; how sensitive information is protected when stored or shared; the use of virtual private networks; control of physical access to computers and hard copy records; how computers are technically secured; secure access to information in the cloud; protecting sensitive information in transit and on mobile devices; whether or not approval is required to transmit sensitive information offsite; whether or not sensitive information is securely disposed of when no longer needed; and whether or not documented policies and procedures for protecting sensitive information are available. *See Appendix B for survey results*

Opportunities were identified for enhancing access and improved guidance on how to identify and distinguish types of sensitive information; expanding encryption goals to academic divisions; and placing limits of security of vendor-supplied cloud services.

The following observations requiring management corrective action were identified:

A. Awareness of Sensitive Information
Our survey indicated a wide range of confidence levels of users ability to identify and distinguish between restricted and confidential information, from none to high confidence; and a lack of consistency in available guidance and where to access.

B. Protection of Sensitive Information - Encryption
Academic divisions were not taking full advantage of Information Technology Services (ITS) encryption services.

C. Protecting Sensitive Information – Google Drive
Although UC guidance prohibits the use of Google Drive or Dropbox to store restricted information without first encrypting it, these apps are commonly used to store sensitive information.

Management agreed to all corrective actions recommended to address risks identified in these areas. Observations and related management corrective actions are described in greater detail in section III of this report.

II. INTRODUCTION

Purpose

The purpose of the audit was to determine the level of awareness for marking, transmitting and storing manual and electronic data containing various levels of sensitivity, and to evaluate the controls in place to help ensure sensitive information is secured in compliance with relevant policies and regulations.

Background

Sensitive data or information is a general term that pertains to information that requires some level of protection. At UCSC this includes both confidential and restricted information. UC BFB IS-3 Electronic Information Security Policy (IS-3) defines restricted information as:

> *Any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit.*

IS-3 does not define confidential information. However, UCSC Information Technology Services (ITS) describes it:

> *The term confidential information applies broadly to information for which access or disclosure may be assigned some degree of sensitivity, and therefore, for which some degree of protection or access restriction may be warranted. Unauthorized access to or disclosure of information in this category could result in a serious adverse effect, cause financial loss, cause damage to the University's reputation and loss of confidence or public standing, constitute an unwarranted invasion of privacy, or adversely affect a partner, e.g., a business or agency working with the University.*

UCOP is planning to revise IS-3 for various reasons with a planned release date of November 2017, and has a different information classification:

> *UC's electronic information now has four protection levels. The first level, P1, is public information. Here UC's concerns relate to integrity and availability. The next level is P2, where we find information that UC does not intend to be public. At P2 we start to become concerned with confidentiality, ensuring only those who are intended to access the information can do so. At P3, we are very concerned with confidentiality. P3 information includes student educational records and staff records. At P4, the highest level, UC has a statutory or contractual obligation to protect the data with the highest level of care.*

Although these descriptions of sensitive information come from IT sources, sensitive information also includes paper records that also require protection. Further, there are federal and state laws, as well as UC policy related to personal privacy and access to University records. Consequently, all University employees are responsible to manage, protect and use University records accordingly. *See Appendix C*

There are various methods employed for protecting sensitive information including the deployment of technical, physical and administrative controls.

Technical controls include user authentication (login) and logical access controls to the network and systems, an Active Directory network, encryption of data at rest and in transit, remote access through a virtual private network, printers that only print when a password is entered, etc. Most of the people we

surveyed kept their sensitive data in Active Directory files or in the UCSC Data Warehouse. There were PIs we contacted that kept sensitive data in computers within their labs, not connected to any network including the Internet, and only accessed by themselves or authorized lab personnel.

Physical controls include door locks to offices and office suites or labs, lockable file cabinets, secluded printers and fax machines, cable locks on computers, etc.

Administrative controls include policies and procedures, training, background checks, having employees sign the *Access to Information Statement,* sanctions, etc.

Scope

We reviewed UC policies and procedures, federal regulations, surveys of campus units, and conducted discussions with campus unit management. Specifically, we

- Reviewed the following related laws, UC policies and federal standard:
  - The Privacy Act of 1974 and the Information Practices Act of 1977
  - UC Business Finance Bulletin (BFB) IS-3 Electronic Information Security and the last draft of the proposed new IS-3
  - UC BFB RMP-1 University Records Management Program and RMP-7 Privacy and Access to Information Responsibilities
  - NIST Special Publication 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
- Reviewed the ITS and Privacy websites for guidance and requirements for identifying and protecting sensitive information
- Reviewed relevant training on the UC Learning Center, namely UC Cyber Security Awareness Training and FERPA Training
- Conferred with ITS Information Security and the Privacy and Information Practices directors
- Surveyed a sample of campus data stewards, academic divisional liaisons, and principal investigators on their awareness and protection of sensitive data. *See Appendix B*
- Reviewed SC-17-58 Data Use and Release Processes within the Campus Admissions and Financial Aid and Scholarship Offices

One of the observations surfacing from our review was the complexity and overlapping criteria and governance over management of sensitive information and its use, and the various stages of maturity of policies in this area. We chose to emphasize the data protection aspect of information management of sensitive data, as electronic data is proliferating and we had an opportunity to help introduce the campus to changes in information security policy. Consequently, there was legitimate discussion raised about coverage from the Privacy and Information Practices perspective as it relates to the appropriate use of sensitive information, which did not become the focus of this audit. For more discussion, refer to Appendix C - Privacy and Information Practices Comments and related observations.

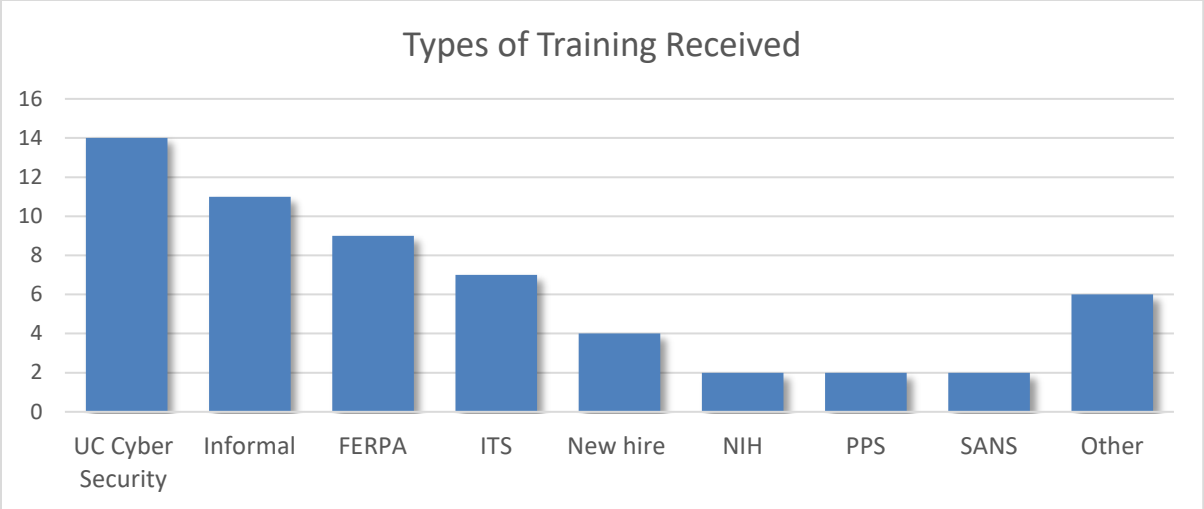
III. OBSERVATIONS REQUIRING MANAGEMENT CORRECTIVE ACTION

A.	Awareness of Sensitive Information	
Our survey indicated a wide range of confidence levels of users' ability to identify and distinguish between restricted and confidential information, from none to high confidence; and a lack of consistency in available guidance and where to access it.		
Risk Statement/Effect		
Without sufficient awareness that correctly distinguishes the different levels of sensitive information, there is the risk that inadequate protection could be applied to ensure the security of that information.		
Agreement		
A.1	Information Technology Services will review and streamline guidance on their website for the identification and protection of various types of data in a format that is complete, up to date, and with simple navigation. This will include coordination with the UCSC Privacy officer and reference as needed to relevant elements contained on the UCSC Privacy website and related to information use, such as employees' responsibility for protecting the privacy of individuals when they use and share sensitive information.	Implementation Date July 2, 2018 Responsible Manager Director, Information Security

A. Awareness of Sensitive Information – Detailed Discussion

In our survey, we asked survey respondents open-ended questions as to what training they received to identify and protect restricted and confidential information; and whether they could confidently distinguish between those two types of sensitive information, and knew how to protect it as a result of that training.

Table 1- Types of Training Received



The most frequent mechanisms survey responders indicated receiving training was through UC Cyber Security, Informal, FERPA and ITS. A few comments on the types of training survey respondent indicated as having received:

- UC Cyber Security training does not provide instruction on how to identify sensitive information.
- FERPA training adequately addresses student records, but not other forms of sensitive information.
- The ITS Information Security website has three different sites that address working with different types of data. All three are listed under the topic of In-Depth Computer Security Topics for UCSC on the Security Awareness Training site linked from the Information Security home site. There is duplicate information on these three sites that could be combined, which would ease navigation to this guidance. Further, this information will have to be updated when the new version of IS-3 is adopted.
- New hire training on this topic only consists of signing the *Access to Information Statement.*
- NIH training is adequate for PIs working on human subjects research projects. PIs also have agreements with sources of private information that they are required to comply with, and a review by the UCSC Institutional Review Board.
- PPS training is provided to those with approved access to PPS based on their payroll/personnel related job duties. Training includes accountability through the *Access to Information Statement.* Information in PPS is divided into two types: 1) non-disclose information, which is personally identifiable information, such as sex, ethnicity, birth date, and social security number related to an individual through his or her name; and 2) public information. *Compare these two types with the three or four types identified in Electronic Information Security policy.*
- SANS or System Administration, Networking, and Security Institute provides training for IT professionals. This training was referenced by an ITS divisional liaison.
- There are units that provide their own training. This is especially the case when units have specific requirements for protecting sensitive information.

While the majority of survey responders were confident that they could distinguish between confidential and restricted information, and know how to protect it, some said there were times when they were not so confident and that others in their divisions probably were not able to make these distinctions. Some responders said they could not make these distinctions and some said they simply regarded all university information as confidential.

As different levels of sensitive information require different controls to protect them, those who regard all university information or all sensitive information the same might use inappropriate or inefficient methods.

A director of an outreach unit believed that training was needed to increase the level of awareness of sensitive information, as well as its types and ways to appropriately protect it. She believed this training should be reoccurring, such as every two years, and included in other required training, such as the UC Cyber Security Training. UC Cyber Security Training is managed by UCOP and currently does not address the identification and appropriate protection of sensitive information.

While we do not have direct control over the UC Cyber Security Training, we have an opportunity to improve the guidance provided by ITS and periodically notify the campus how to access it.

There is a further aspect of training that needs to be addressed having to do with how information is being used. Information management and privacy principals address the employees' responsibility for protecting the privacy

of individuals when they use and communicate information related to individuals. Only the minimum amount of private information should be obtained or communicated to achieve a business purpose. The Registrar told us that this is not always happening. Information management and privacy principals require a person working with information that contains private information related to an individual as having the responsibility to redact the nonessential information prior to forwarding this information on. Training in this responsibility could mitigate the unnecessary proliferation of private information.

B.	Protection of Sensitive Information - Encryption	
Academic divisions were not taking full advantage of ITS encryption services.		
Risk Statement/Effect		
When unencrypted computers are stolen, sensitive information on those computers can be accessed by thieves in violation of the public trust and privacy regulations, which involve hard and soft costs to the University.		
Agreement		
B.1	Information Technology Services will work with academic divisions to accelerate efforts to encrypt as many supported devices as possible within a realistic period.	Implementation Date July 2, 2018 Responsible Manager Vice Chancellor, Information Technology Services

B. Protection of Sensitive Information – Encryption – Detailed Discussion

ITS's Client Services & Support unit manages approximately 3,500 computers through Desktop Support; most are administration computers, but some belong to faculty. This unit plans to encrypt all these computers in two phases by the end of 2018. The first phase is encrypting all computers with new operating systems, e.g., Mac OS X and Windows 10 (approximately 1,200 computers). As of August 18, forty-nine percent of first phase computers have been encrypted. The second phase will encrypt computers with older operating systems. As of December 2016, all new computers Desktop Support manages are set up with the Standard Desktop Services image and are encrypted via this service.

The ITS encryption service encrypts both Macs and Windows computers. It also stores recovery keys centrally to ensure access to encrypted information. ITS provides this service free of charge and by request.

Not all Campus computers are managed by ITS; academic divisions manage their computers locally as do PIs who purchase computers with grant funds.

The ITS academic divisional liaisons (DLs) we heard from and the Baskin School of Engineering (BSOE) website referenced a level of encryption service provided to these divisions.

We learned:

- Encryption service is not uniform. PBSci and BSOE provide encryption through Standard Desktop Services, but not for all computers; SocSci uses JAMF for Macs, and manual encryption for Windows boxes – this does not provide key escrow service like JAMF does; Humanities was waiting for the new Apple file system, APFS, coming this fall, before it starts encrypting computers.
- Encryption is offered on request and without any timelines by which all supported academic computers will be encrypted.

- Computers purchased by PIs with grant funds are not supported by DLs unless PIs request it.

If the goal is to get as many academics' computers encrypted as possible, then DLs would need to decide on adequate encryption methods that include a key escrow service, and ITS would probably have to conduct an email campaign, which could also be reinforced by support from divisional senior management.

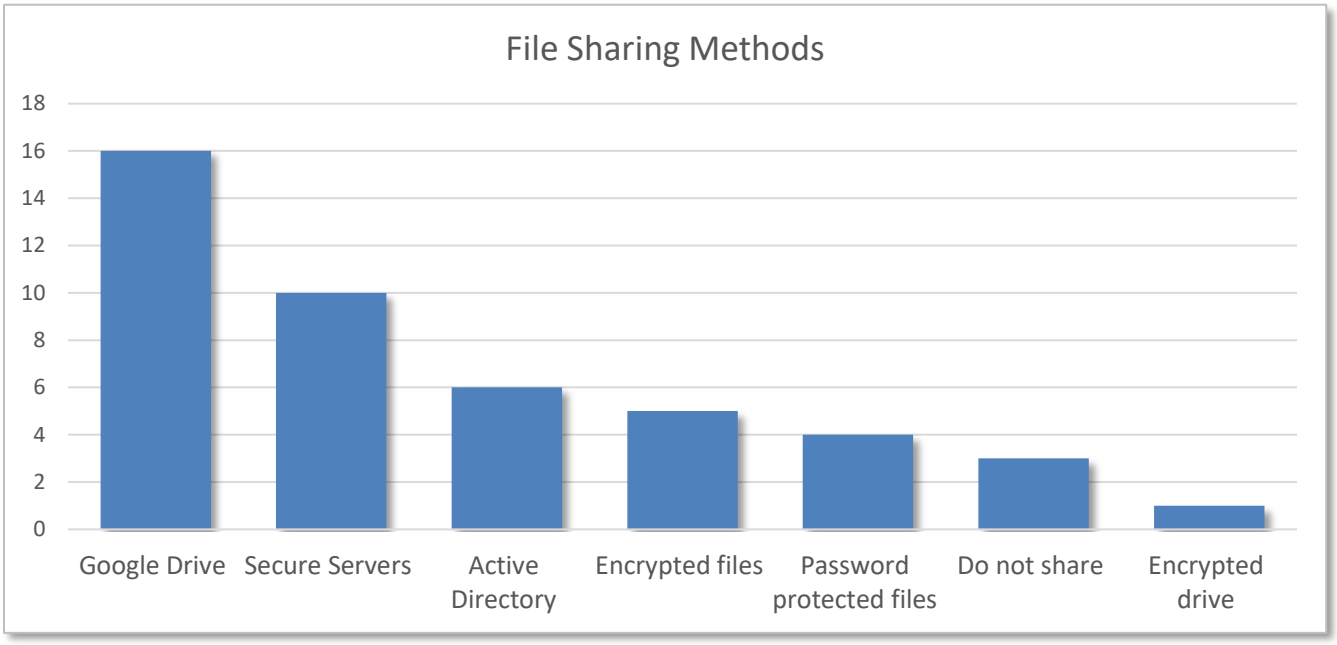
As the theft of faculty computers does occur, we recommend the goal of getting all supported computers encrypted.

C.	Protecting Sensitive Information – Google Drive	
Although UC guidance prohibits the use of Google Drive or Dropbox to store restricted information without first encrypting it, these apps are commonly used to store sensitive information.		
Risk Statement/Effect		
Without agreements with vendors who provide cloud services to UC, all the liability falls on the University if the security of vendor services is breached.		
Recommendation/Agreement		
C.1	Information Technology Services will include guidance on the secure use of Google Apps and other file hosting services on working with different types of data.	Implementation Date July 2, 2018 Responsible Manager Director, Information Security
C.2	Information Technology Services will identify potential solutions for reducing the risk of unencrypted data stored in cloud storage providers and communicate recommended actions to campus leadership.	Implementation Date September 30, 2018 Responsible Manager Director, Information Security

C. Protecting Sensitive Information – Google Drive – Detailed Discussion

In our survey, we asked how shared files with sensitive information are protected from unauthorized access. The majority of responses were with Google Drive. See the table below.

Table 2 – File Sharing Methods



UCOP provides guidance when using Google Apps, which includes Google Drive:

> *Google Drive is not acceptable for PCI-DSS data, export controlled data, and ePHI. UCOP recommends consulting with data proprietors and appropriate UC location authorities for other confidential information.*

UCOP references ITS as the UCSC authority. ITS provides the following guidance:

> *Keep restricted data out of Google. Don't use Google to send or store highly sensitive information such as PII or other restricted data. If you must, encrypt it first.*

We could not identify the type of sensitive information that our survey responders kept in Google Drive, but given the difficulties encountered with distinguishing between restricted and confidential information, we believe it is likely that units are keeping some restricted information there.

ITS could include guidance on the secure use of Google Apps in its guidance on working with different types of data, at least as a link.

Further, as the use of Google Apps, such as Google Drive, is increasing, the University could discuss with Google how an agreement might be reached to provide further assurances regarding the security of highly sensitive information on such systems as Google Drive. UC already has a contract with Google that provides a level of assurances regarding the security and privacy of customer information stored on Google's systems. If the level of assurance were increased, UC could store restricted information on those systems.

As UC has no contract with Dropbox, UC sensitive information should not be stored on that system. ITS could inform the campus of this.

APPENDIX A - Summary of Work Performed and Results

Preliminary Survey and Risk Analysis	
Work Performed	**Results**
• We conducted a preliminary survey to identify the objective of relevant campus offices concerning user awareness and protection of sensitive information. • We surveyed data stewards, divisional liaisons and principal investigators with 14 open-ended questions on how they are aware of and protect sensitive information	• There are UC policies and guidance for the identification and use of sensitive information, covering paper records as well as electronic format. • UC plans to replace the current IS-3 Electronic Information Security Policy. The last draft we reviewed requires a finer discrimination of types of information from three types in the current IS-3 to four types. • UCSC ITS provides guidance for working with types of data. There are three websites with guidance that we believe can be combined into one website and made easier to navigate to. • We sent the survey to 60 individuals and requested them to forward the survey as appropriate. We received responses from 36 individuals. See Appendix B • Based on the responses to our survey we did additional work reflected below.

Survey of units/departments on security of faxed and printed information	
Work Performed	**Results**
We surveyed 13 campus units/departments to find out how they protected hard copies/paper records of sensitive information, including fax machines and printers where potentially sensitive information could be received.	We received eight responses (another was implied). These did not indicate a weakness in the management of sensitive paper records at rest or incoming through printers or fax machines. • One unit did not keep paper records • Faxes and printers were sequestered or Pharos printers were used, which require a password before they print

Encryption	
Work Performed	**Results**
1. Contact ITS Client Services and Support and learn what the plan and current status is for encrypting hard drives.	1. The first phase of this encryption service was to encrypt computers with Window 10 and Mac OS X operating systems, which number 1,200. The total encrypted computers so far represent 50% of those computers with newer operating systems. • ITS plans to have all 3,500 computers that it services encrypted by the end of FY2018 • As of December 2016, all new computers it sets up are encrypted • By Friday, August 18, 2017, Total Encrypted Computers: 589 • Total Managed Computers: 3,479; Percent encrypted 16.93%
2. Contact ITS Academic Divisional Computing and learn what plans academic divisions have to encrypt hard drives.	2. Academic divisions are also going in this direction, but there are no timelines to encrypt divisions because encryption is provided only upon request. PI's who purchase computers with grant money would have to request this service, as ITS divisional liaisons do not know of these computers unless they are informed of them. Further, DLs in different divisions are using different methods of encryption; some do not provide encryption key escrow.
3. Contact ITS Security and find out if there are recommended practices for encrypting transmissions of sensitive information.	3. While users/clients may have individual methods to encrypt transmitted messages, such as HIPAA units, the campus is rolling out an application, UCSC Filelocker, which provides this service. Through these methods, the campus will be able to satisfy its responsibilities for encrypting restricted information at rest and when transmitted - currently there is no requirement to do so; it is only a recommended practice. In the future, it may become a requirement. While these are technical solutions to secure sensitive information, they will still require users to implement them conscientiously, as user errors can still defeat these controls. Further, full disk encryption is only as strong as its weakest link, viz. computer password strength and avoiding giving passwords away due to social engineering scams, such as phishing attacks.

Interview a sample of data stewards	
Work Performed	**Results**
We interviewed three data stewards: 1. Educational Partnership Center Director 2. UCSC Registrar 3. Employee & Labor Relations Manager	1. EPC Director • Supported periodic training on identifying sensitive information and the appropriate ways to protect it • Supported more guidance in the appropriate use of tools for sharing and sending sensitive information, e.g., the use of Google Drive and Filelocker • Plans on getting all its computers encrypted 2. The Registrar The Registrar's Office is taking action to ensure that sensitive information is secure at rest, in transit and when used. Interesting actions are acquiring an app to scan workstations for SSNs; using Filelocker to encrypt email messages and destroy them when no longer needed; moving student records from a Student Affairs' server to the AD domain; and keeps paper records in a secure room within a secure suite of offices. They reported receiving restricted information, such as SSNs from campus offices and from other UC campuses. Sometimes this is necessary, but there are cases when this is not necessary and indicates a problem with awareness of how to protect sensitive information. The Registrar's Office redacts unnecessary private information and instructs its senders to not send it. Further, the Office has provided face-to-face instruction to student advisors on how to send only information needed by the Registrar. 3. Employee & Labor Relations (ELR) In general, Staff HR has sensitive information, such as PII, including SSNs, PHI, background checks, including criminal records, Title IX information, and disciplinary information. It has recently moved to the Scotts Valley Center. • ELR was working to further restrict access to its folder on the Staff HR AD domain • ELR laptops were not encrypted • Paper records are up to date with disposition schedule and securely stored • ELR personnel are instructed to not keep files on their computers

APPENDIX B – Results of Survey of Sensitive Data – User Awareness

Audit Objective and Methodology

Purpose

- The purpose of this review is to determine the level of awareness for identifying, storing and transmitting manual and electronic data containing various levels of sensitivity.
- This audit was included on the campus FY18 Internal Audit Plan.

Methodology

- We identified data stewards and likely organizations where sensitive information, such as personally identifiable information (PII) and FERPA information is generated, stored and transmitted.
- We sent a brief questionnaire to campus academic and staff personnel in organizations likely to generate, store and transmit sensitive information and compiled the results.
- Based on responses received, we interviewed additional individuals to gain a better understanding of the extent of user awareness of policy and practices designed to prevent the inappropriate or unintended release of the most sensitive information.

DRAFT - CONFIDENTIAL - DO NOT DISTRIBUTE - 9-12-2017

Data Stewards

- We initially identified data stewards using a Draft August 2015 Data Stewardship Designee Document (see right).
- We then used Division Organization Charts and the Campus Directory to specifically identify individuals whom were designated as a Data Domain Stewards.

UCSC Data Stewardship - Administrative

Steward or Resource Proprietor	Administrative Data Domain	Related Designee
Campus Provost and Executive Vice Chancellor	Faculty (Teaching, Research and other Academic Staff)	Divisions and Assistant Vice Chancellor, Academic Personnel
	Bio-demographic Data	Divisions and Assistant Vice Chancellor, Academic Personnel
	SMG Bio-demographic data	
	Student Medical and Mental Health	Executive Director, Student Health Services
	Disability, student accommodation, diagnoses	Director, Disability Resource Ctr
	Student Conduct Records	Assistant Dean of Students, Campus Life
	Student Wellbeing, medical	CARE Coordinator
	HS student personal info, release of liability	Director of SOMeCA
	Alumni and student employment	Director, Career Center
	Athletics, emergency family, bio-narrative, insurance, medical documentation, bank info	Director - OPERS
Vice Chancellor, Business and Administrative Services	General Ledger, Payroll, Time Reporting	Assistant Vice Chancellor, Financial Affairs
	Staff Bio-demographic data, Benefits	Assistant Vice Chancellor, Staff Human Resources
	Facilities Management	Director Physical Plant
	Non-person entitites (vendors, governmental agencies, corporations)	Assistant Vice Chancellor, Financial Affairs
	Physical Planning/ Construction Documents	Assistant Vice Chancellor, Phycial Planning and Construction
	Environmental Health and Safety	Assistant Vice Chancellor, Risk and Safety Services

DRAFT - CONFIDENTIAL - DO NOT DISTRIBUTE - 9-12-2017

Survey Results

Who we Sent Survey to

- We sent the survey to the data stewards identified in the previous charts.
- We sent the survey to divisional liaisons and some PIs
- Additionally we solicited Division Leadership to forward the survey to their staff as they deemed appropriate.
- In total we sent survey to 60 individuals:
  - 45 administrators and
  - 15 academic researchers (PIs).

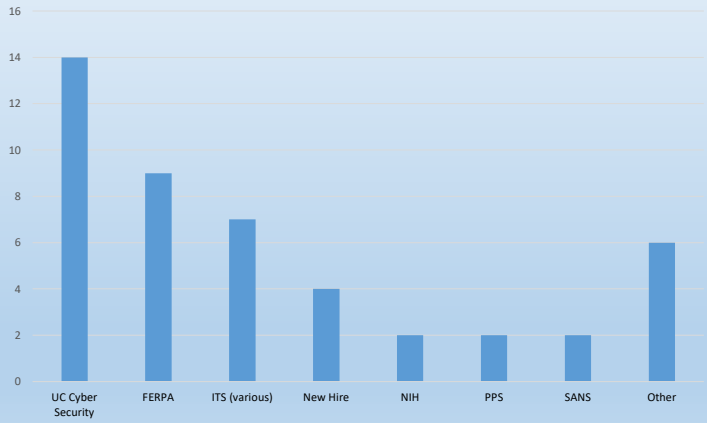
Who Responded

- We received responses from 37 individuals (62% response rate):
  - 31 administrators (either original contacts, their staff, or new requests) and
  - 6 academic researchers (PIs).

DRAFT - CONFIDENTIAL - DO NOT DISTRIBUTE - 9-12-2017

Survey Results

1.a. What training do workforce members in your organization receive to identify and protect restricted or confidential (sensitive) information?

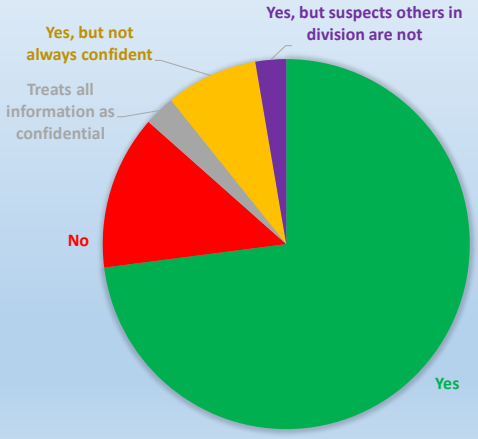


DRAFT - CONFIDENTIAL - DO NOT DISTRIBUTE - 9-12-2017

6

Survey Results

1.b. As a result of the training received, can you confidently distinguish between restricted and confidential information and how to protect this information?



Yes	27
No	5
Treats all information as confidential	1
Yes, but not always confident	3
Yes, but suspects others in division are not	1

DRAFT - CONFIDENTIAL - DO NOT DISTRIBUTE - 9-12-2017 7

Survey Results

2. Are you aware of where your organization keeps sensitive information, both paper and electronic files?

No	3
Yes	34

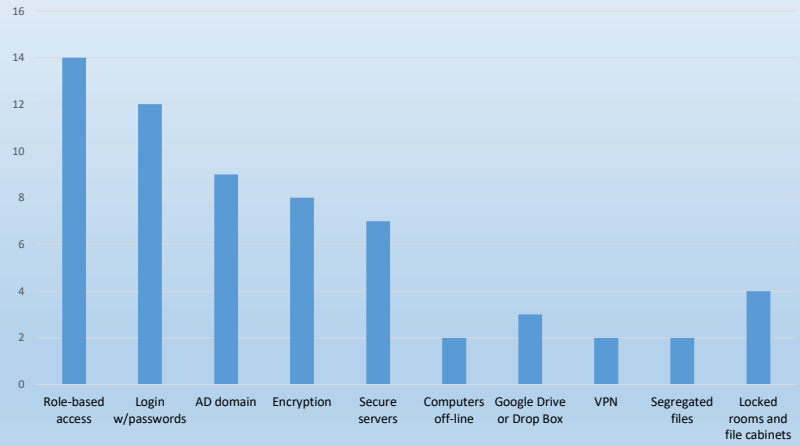
Note:

- Two of three "No" responses were divisional liaisons which could not speak for the entire division.

DRAFT - CONFIDENTIAL - DO NOT DISTRIBUTE - 9-12-2017

Survey Results

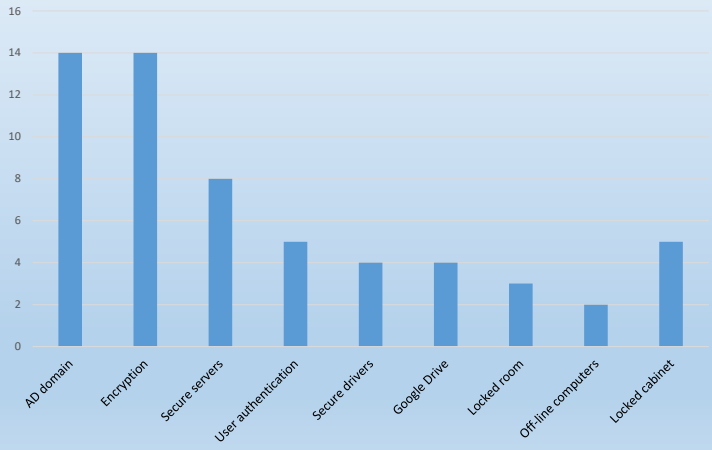
3. How does your organization restrict access to electronic systems with sensitive information?



DRAFT - CONFIDENTIAL - DO NOT DISTRIBUTE - 9-12-2017

Survey Results

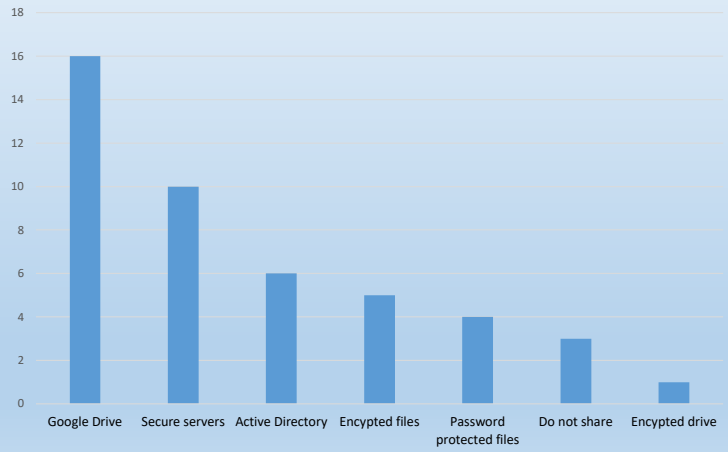
4. How is sensitive information stored to protect it from unauthorized access?



DRAFT - CONFIDENTIAL - DO NOT DISTRIBUTE - 9-12-2017

Survey Results

5. How are shared files with sensitive information protected from unauthorized access?



DRAFT - CONFIDENTIAL - DO NOT DISTRIBUTE - 9-12-2017

Survey Results

7. How does your organization control physical access to computers and hard copies of sensitive information?

DRAFT - CONFIDENTIAL - DO NOT DISTRIBUTE - 9-12-2017

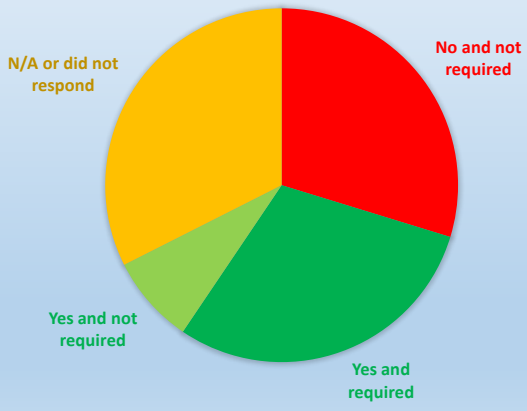
Survey Results

8. How does your organization technically secure work computers?

DRAFT - CONFIDENTIAL - DO NOT DISTRIBUTE - 9-12-2017

Survey Results

9. When workforce members access sensitive information directly from the cloud, do they only use secure devices?

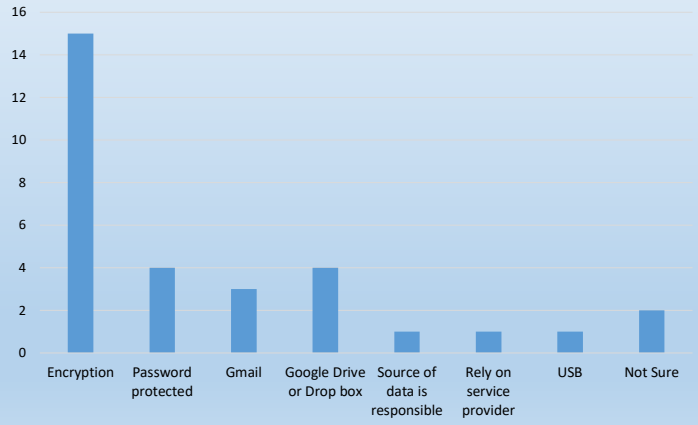


No and not required	11
Yes and required	11
Yes and not required	3
N/A or did not respond	12

DRAFT - CONFIDENTIAL - DO NOT DISTRIBUTE - 9-12-2017

Survey Results

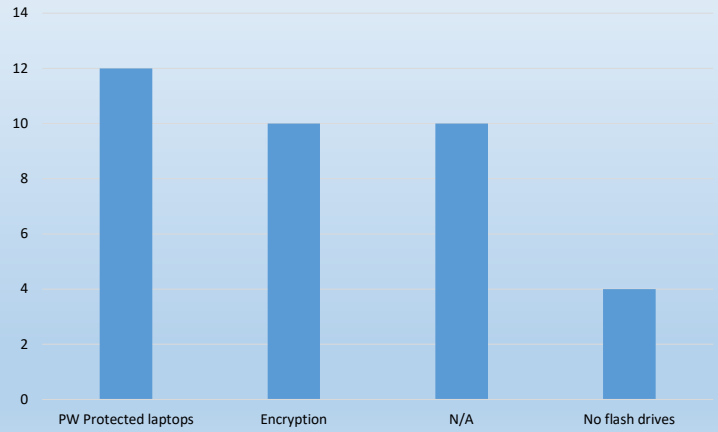
10. When workforce members transmit sensitive information, how do they protect it from unauthorized access?



DRAFT - CONFIDENTIAL - DO NOT DISTRIBUTE - 9-12-2017

Survey Results

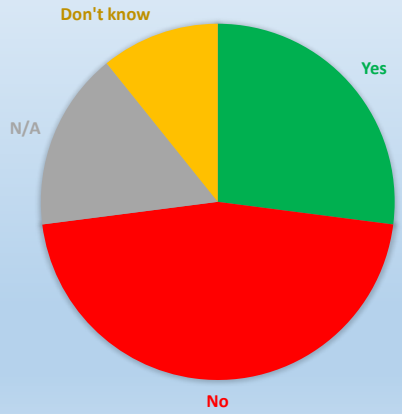
11. How do workforce members protect sensitive information when it is on a mobile device, such as a laptop or USB flash drive?



DRAFT - CONFIDENTIAL - DO NOT DISTRIBUTE - 9-12-2017

Survey Results

12. Is approval required to take or transmit sensitive information off-site?

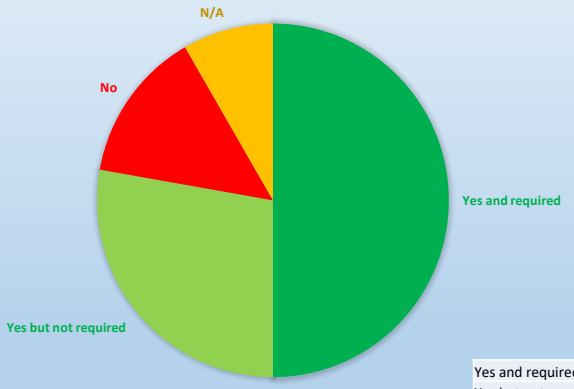


Yes	10
No	17
N/A	6
Don't know	4

DRAFT - CONFIDENTIAL - DO NOT DISTRIBUTE - 9-12-2017

Survey Results

13. Do workforce members delete sensitive information from their computers or flash drives when no longer needed?

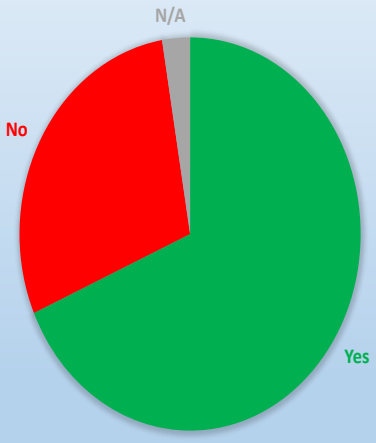


Yes and required	18
Yes but not required	10
No	5
N/A	3

DRAFT - CONFIDENTIAL - DO NOT DISTRIBUTE - 9-12-2017

Survey Results

14. Does your organization have documented policies and procedures for protecting sensitive information?



Yes	26
No	11
N/A	1

Note:

- The Yes's include ITS and UCOP policies, and IRB and data source requirements.
- The No's refer to unit, department or lab policies

DRAFT - CONFIDENTIAL - DO NOT DISTRIBUTE - 9-12-2017

APPENDIX C – Privacy and Information Practices Comments

We asked the director of UCSC Privacy and Information Practices, who is also the campus privacy official (Director) to review and comment on our draft report on Information Management of Sensitive Data - User Awareness. The Director shared with us that the report's focus did not address points raised during initial audit scoping meetings relating to how sensitive information was being used.

The Director is the local coordinator of information practices with responsibilities established by RMP-7, Privacy of and Access to Information Responsibilities (1985). These responsibilities were assigned by that policy to help ensure that the University complied with federal and state laws that address an individual's civil right to privacy, such as the California Information Practices Act of 1977 (IPA).

The Director observed that this review focused on security of sensitive information and could also have included:

- Maintaining information that is pertinent and necessary to accomplish the purpose for which it was intended or authorized by law
- Assure compliance with records privacy and access
- Understand legal requirements, including differences between confidential, personal and non-personal information
- Ensure files are maintained with accuracy, relevance, timeliness, and completeness

The Director's perspective was supported by a definition in and certain requirements of the IPA, such as:

- "personal information" means any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual. *The IPA did not define confidential information.*
- Each agency shall maintain in its records only personal information that is relevant and necessary to accomplish a purpose of the agency required or authorized by the California Constitution or statute or mandated by the federal government.
- Each agency shall maintain all records, to the maximum extent possible, with accuracy, relevance, timeliness, and completeness.
- Each agency shall establish rules of conduct for persons involved in the design, development, operation, disclosure, or maintenance of records containing personal information and instruct each such person with respect to such rules and the requirements of this chapter, including any other rules and procedures adopted pursuant to this chapter and the remedies and penalties for noncompliance.
- Each agency shall establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance with the provisions of this chapter, to ensure the security and confidentiality of records, and to protect against anticipated threats or hazards to their security or integrity, which could result in any injury.

The University had established the policy RMP-8: Requirements on Privacy of and Access to Information to help address those requirements, but this policy was rescinded on 11/13/2015, as it mainly restated federal and state requirements, and was replaced by a UCOP policy website. The director alerted us to a document on that website,

Rules of Conduct for University Employees Involved with Information Regarding Individuals, which was an attachment to RMP-8. This document has seven rules that help ensure compliance with the IPA.

The University has different policies to address different privacy requirements, whether in the civil liberties sense or in the data protection and system security sense. In 2010, UC President, Mark Yudof (2008-2013), established a UC Privacy and Information Security Initiative. The purpose of the Initiative was to "review existing privacy and information security policies; develop a new overarching policy framework to address privacy and information security in the modern legal, technology, and social context; and provide clear updated guidance to assist the University community in meeting legal obligations to safeguard "protected" data while at the same time abiding by deeply held principles of privacy." The last meeting for the Initiative was in April 2012. We did not see a new overarching policy framework document to emerge from this effort.

One of the observations surfacing from our review was the complexity and overlapping criteria and governance over management of sensitive information and its use; and the various stages of maturity of policies in this area. We elected to pursue our review with an emphasis on the data protection sense of information management of sensitive data, as electronic data is proliferating and we had an opportunity to help introduce the campus to changes in information security policy.

Nevertheless, our review addressed some of the concerns expressed by the Director, such as:

- Personally identifiable information (PII) is identified as confidential information in Electronic Information Security Policy (IS-3) and is defined like personal information in the IPA.
- Access to sensitive information, including PII, is restricted by job responsibilities. This is called role-based access.
- The Admissions Office provides training to its employees to ensure they comply with the IAP.
- The Admissions Office relies on a UCOP website for student applications to the University.
- The Financial Aid and Scholarship Office complies with NIST 800-171, which requires training to carry out employee assigned information security-related duties and responsibilities.
- Personnel we spoke to told us their standard practice is to redact sensitive information they receive that they do not need to accomplish their business purpose.
- Personnel who access student information on enterprise systems, such as AIS, are required to take FERPA training before getting access to those systems.
- The Registrar's Office has provided face-to-face training to student advisors on restricting the sensitive information advisors send to the Registrar.
- Offices we spoke to follow a disposition schedule. For example, Employee and Labor Relations destroyed records following their disposition schedule before moving to the Scotts Valley Center.
- Our survey showed that Campus units had administrative, technical and physical practices to secure their sensitive information.
- We observed room for improvement of training in the identification and protection of sensitive data. We will request ITS to reference the UCSC Privacy website when they update their training.