Introduction

The University of California is committed to high standards of excellence for the protection of its confidential information and information technology that support the University. The implementation of appropriate controls and security measures plays a critical role in assuring information retains its integrity, availability, and where appropriate their confidentiality. Security measures also protect information technology from damage or compromise and assure the University's operations will continue without interruption.

Security and information security is the condition of information being protected from or not exposed to unintended access, loss of availability or corruption. In addition, security also includes the methods, processes and techniques necessary to ensure the availability, correct operation of systems, and protection of data from unauthorized access. The magnitude of security controls should be commensurate with the magnitude of the potential loss or seriousness in the event controls fail. Although the type of security controls may vary, the proper security of information is important, regardless of the medium in which the information is stored.

To assure compliance with the standards expected, the UCSB Chief Information Security Officer has developed this plan to document the existing controls and to document plans for the coming year to improve security. While the scope of the information security applies to all University of California Santa Barbara (UCSB) departments, members of the university community (faculty, staff, and students), contractors, consultants, and organizations or individuals, this plan focuses on applications containing confidential or restricted information. Restricted information is defined by UC Policy BFB IS-2.

The information security program plan consists two major parts. The first part of the security plan is focused on individual applications that contain confidential and restricted information. Each of these applications will be evaluated for threats and risks. The existing controls for each application will be considered and where needed, additional controls will be implemented. The second part of this plan reports the ongoing and planned security processes and initiatives. These campus wide initiatives either meet a need of many departments or are the response to specific legal and regulatory requirements.

1. Application Level Information Security Program

The security program includes cost-effective processes, projects and strategies that are consistent with the organizational goals. The processes include controls that are specific to an individual application in addition to processes that are central and apply to all applications. To insure the security plan is cost-effective, the first step is to review and perform a risk assessment.

a. Risk Assessment, Asset Inventory and Classification

The risk assessment starts by determining the type of information that is most subject to risk. In recent years, the University of California's greatest costs associated with security failures are those caused by the unauthorized disclosure of information. This has resulted in required notifications to millions of individuals system wide. While the University does not release data related to the costs for all of these breaches, anecdotal evidence suggests that this is one of the greatest and most expensive information security risks to the University.

As a result, the current plan focuses on information that would require notification in the event of a breach of security. Within the University's classification system (BFB IS-2) this data is classified as Restricted. This data includes personal information including social security numbers, driver licenses, health information and health insurance information. For the purposes of the current plan, only data requiring a notification in event of a breach will be within the scope.

The each division maintains an inventory of restricted applications. For each application in the inventory, the CISO will assist the owner of the application to assess the risks using the guidance provided in policy IS-3. This assessment will evaluate existing controls and where needed develop specific plans and processes for their applications.

During the current fiscal year a new inventory mechanism will be introduced and potentially outdated information will be purged providing a more accurate picture of UCSB's applications and the types of sensitive data they process and store.

b. Goals of Security Assessment and Plans: Confidentiality, Integrity, and Availability

As stated above, the primary focus of this plan is to assure the controls, that maintain the confidentiality of the information, are working effectively. A secondary, but still important focus of the plan is the integrity and availability of the application and data. As part of the evaluation of each application, the owner will consider the threats, potential damages and existing controls.

Following IS-3 guidance, this evaluation will include the administrative workforce controls, operational and technical controls and physical and environmental controls.

2. Security Plans, Projects and Processes – Central

Because security is a continuing process, many of the security related processes and projects started in prior years are either established or are ongoing. These projects and processes were started based upon risks and needs identified in the past and provide support for many departments or applications. It is intended that these security processes provide leverage of limited security resources available and enabling the owner of the application to improve the security of their application. The security projects and processes that have a centralized component will be discussed below. The central processes are intended to assist, not replace, the actions of the application owners.

This list below of central security processes, services, procedures and controls should not be considered comprehensive. There are many other programs, processes and procedures that also contribute to good information security.

a. Incident Management Response Implementation Plan

During fiscal year 2015-2016 there was one reportable incidents on the UCSB campus. While the campus experiences security breaches and other problems on a regular basis, only one of these breaches leaked restricted information that required notification.

Current Status:

UCSB has adopted the system wide incident response plan for the campus. Key individuals on campus, including the CISO, have access to the Ethics Point system for uniform reporting of incidents.

The response plan was exercised in fiscal year 2014-2015 for a breached that occurred in the prior fiscal year. A review of the incident response found that the plan worked well.

Plans: Technical response capability on campus is limited and distributed. Current plan is to identify skilled resources from across campus that can be brought together to respond to incidents outside of the normal capabilities of the SOC and department IT resources.

b. Critical Positions

Some positions with job responsibilities directly related to the applications containing restricted information are deemed to be Critical Positions. (The term "Critical Positions" is used here as defined in University Personnel policies, and is not to be confused with the use of the term "critical" as used with respect to information resources.) It is important that the hiring process include appropriate background checks to assure the honesty and reliability of these individuals.

Current Practice:

- UCSB hiring procedures ensure that candidates requiring access to restricted data undergo applicable background checks as part of the hiring process.
- For staff requiring access to restricted or essential resources, procedures have been established to immediately restrict, suspend or terminate access in the event of disciplinary action or termination.
- During an investigatory leave, access privileges are revoked or restricted, as appropriate.

When a job posting is requested, HR works with the department to determine if the position is deemed a Critical Position. If the position is deemed Critical, then an HR specialist will order the background check on the individual. The results are shared with the department when the background check is completed. The official record of the background checks is maintained by HR.

Plans: This practice is considered to be working well, and the plan is to continue the current practices.

c. Identity Management Systems

The management of the identity is fundamental to the access controls of a system. The IT departments at UCSB continue to support central identity management.

The access control measures to an application should include secure and accountable means of *authorization* and *authentication*.

- **Authorization** is the process of determining whether or not an identified individual or class has been granted access rights to an information resource, and determining what type of access is allowed, e.g., read-only, create, delete, and/or modify.

- **Authentication** is the process of confirming that a known individual is correctly associated with a given electronic credential, for example, by use of passwords to confirm correct association with a user or account name.

Current Status Authentication is managed through the campus LDAP directory for most applications and via Microsoft Active Directory (AD) that is synchronized with the LDAP directory in Student Affairs (SA) and Administrative and Residential IT (ARIT). A campus wide single sign-on solution was made available in 2016.

UCSB does support authentication federation suing Shibboleth. This federated authentication is leveraged by multiple service providers and for services obtained through other UC campuses.

The principal authorization mechanisms used are Microsoft Active Directory and an internal system called Allin02. As noted above, SA and ARIT make extensive use of AD. Allin02 is used to control access to multiple line-of-business applications.

A nascent capability involves group management within the identity and access management system.

Plans: A project is underway to create a campus wide AD synchronized with Microsoft's Azure AD. The first use of this capability will be to support centralized cloud services such as application hosting. A collaborative effort will be initiated to develop an integrated AD infrastructure to meet the needs of campus. Group management capability as a foundational element for role-based access control (RBAC) will be expanded. Nascent use of 2-factor authentication will be expanded.

d. Network Security

Network security is important to maintaining a secure working environment.

Current Status:
Network security and operations is managed centrally by Enterprise Technology Services (ETS). The tools used to protect the networks include access control lists and intrusion detection/prevention systems (IDS/IPS) deployed at the campus border. An authenticated virtual private network (VPN) capability grants campus access to authentication users from untrusted networks allowing secure remote access to campus resources.

At UCSB, many departments implement firewalls at demarcation points for their networks and some isolate their operational networks with network address translation (NAT).

VLANs are extensively used to provide layer 2 network segregation and to meet the needs of departments that operate across 2 or more physical locations.

Network security includes basic security related network capabilities such as the capture and logging of net flow data and the ability to capture packets when required.

Plans: Advanced UTM will replace end-of-life IPS capability at the border. Selective deployment of firewall and UTM will be deployed within the data center and other critical locations.

\

e. Security services and capabilities

ETS provides the campus with a wide variety of security services that supplement basic network security controls to enhance the overall ability to protect the network and systems running on it and to detect and respond to events and incidents. Among these are:

- Centralized logging of security events coming from network devices
- Vulnerability scanning from within the campus network and from outside of it
- On demand web application vulnerability scanning
- Advanced malware detection
- SSL/TLS certificates
- Security information and event monitoring system (SIEM)

Together with these and other services a Security Operations Center (SOC) monitors the state of security throughout the network, examines events, and manages routine incidents like vulnerability detection and compromised credentials. The SOC is instrumental in supporting the forensic and investigatory demands of significant incidents such as those where restricted information or critical resources are compromised.

Plans: During the current fiscal year the SIEM and centralized logging capabilities will be expanded. There will be other enhancements to services to increase effectiveness. A centrally managed log processing capability using Splunk is being introduced.

f. Security Awareness Training Project

UCSB has implemented the SANS Security the Human (STH) awareness training. In-person training is available to groups on campus in lieu of the CBT. Ten IT staff from across campus have attended bootcamp style training leading to Security+ certification.

Plans: UCSB will continue to sponsor qualified IT staff for training toward Security+ certification. Application developer CBT is under evaluation. An application security training approach will be implemented. Advanced training will be available on a case-by-case basis to meet business needs and employee development.

g. Payment Card Industry (PCI) data security standards

The UCSB campus must comply with the PCI data security standards for all entities that process credit cards (merchants). Matt Coy is responsible for managing the PCI compliance program for the UCSB campus.

UCSB is a Tier IV merchant with a relatively low number of payment card transactions each year. All on-campus merchants complete self assessment questionnaires (SAQ) each year as required by payment card brands and merchant banks. The campus has contracted with a qualified system assessor (QSA) and an authorized scanning vendor (ASV) to provide consultative services and external vulnerability scanning respectively.

FY 2016 introduced a significant effort to replace all POS terminals on campus with terminals capable of end-to-end encryption. This significantly reduces compliance requirements.

Plan: CISO and operational security and network staff will continue to provide technical advice as needed. Replacement of POS terminals will continue.

h. Secure Compute Research Environment (SCRE)

ETS introduced a service designed to meet the needs of researchers that use restricted data sets provided from state and federal sources. These data sets usually include personally identifiable information (PII) or personal health information (PHI). Many sources of these data sets require strict security controls.

ETS developed a service that facilitates full life cycle use of restricted data sets. A virtualized environment with tight security controls and access restrictions provides a set of security controls that have been accepted by many data set providers in lieu of their regular requirements. The service even provides secure storage of the original source media while the data sets are in use so they can be returned at the end of the research project. Two-factor authentication and a virtual private network provide researchers the ability to access their work from anywhere.

Plan: The service will be expanded and security controls introduced to implement those control from the FISMA set required for sensitive but unclassified information. This will allow the environment to be used for certain federally sponsored research projects.

i. Disposition of Equipment

Procedures should ensure implementation of controls to address the re-assignment or final disposition of hardware and electronic media, including requirements that ensure complete removal of restricted or other sensitive information as appropriate, such as by shredding, overwriting a disk, or employing professional data destruction services as commensurate with risk. Sufficiently strong disk encryption may be used as an alternative mitigation.

Current practice:
Secure removal of sensitive and restricted information may be achieved by overwriting media or physical destruction. The medium most associated with sensitive data is the disk drive. Secure disposal of disks from systems being retired has been difficult and time consuming. To address this concern ETS has introduced a secure disk drive disposal mechanism using NSA approved degaussing and physical destruction by mechanical crushing of the device. Forensic chain-of-custody practices are a part of the service allowing documentation of the destruction where required for research projects and PII. This has been widely accepted by campus.

In FY2016 the drive disposal process and tools were enhanced to include tape media.

Plan: This practice appears adequate and there are no plans for change.

j. Health Records / HIPAA Controls

UCSB has a number of departments that create and handle personal health information. This health information is regulated by both state and federal law. The plan is for departments managing health records to assess risks and identify risk mitigation plans. Because of the nature of the regulation of the health information, the risk mitigation strategies will incorporate the practices and procedures recommended by the Federal department of Health and Human services and the Federal Department of Education.

Plan: To continue to assess risks, evaluate controls and consider additional controls. An evaluation of departments with HIPAA data will be conducted on a rotating basis.

k. Managed anti-malware

Historically departments have adopted their own choice of anti-malware for endpoints and servers. Many departments have chosen to implement unmanaged solutions. This precludes gaining a full understanding of the incidents of malware on campus and the effectiveness of protective controls.

Plan: In the current fiscal year a managed anti-malware service will be deployed first targeting end-points and later servers. Information will be incorporated into SOC practices and reporting.

l. Potential Future Projects with Merit

As part of developing the current plan, potential projects were identified that would improve the security of information on the campus. While these projects have not been started, as people, technology and resources become available these projects will be evaluated and may move from a planned to active status. These projects include:

- Encrypted Email
- Secure File transfer (using encryption)
- Forensic equipment and training

m. Policy and Standards

The UC system and UCSB operate under a collection of policy documents generally referred to as the Business and Finance Bulletin Information Systems Series. To better align with industry standards and to update controls to meet currently accepted best practices, a new policy framework is being developed that will replace the central document, IS-3 and several others. The new policy document will be follow the format of ISO 27001 and 27002. Supporting standards and implementation guidelines will be created and used to supplement the high-level controls of the policy

Plan: Participate in the creation of the new IS-3 and evaluate current services for compliance with the new policy. Provide support to IT organizations across campus as they move toward compliance with the revised policy.

Appendix A. References

Statement of Ethical Values and Standards of Ethical Conduct
Electronic Communications Policy
Policy on Reporting and Investigating Allegations of Suspected Improper Governmental Activities (the "Whistleblower Policy")
IS-2, Inventory, Classification, and Release of University Electronic Information
IS-7, Guidelines for Maintenance of the University Payroll System
IS-10, Systems and Development Standards
IS-11, Identity and Access Management
IS-12, Continuity Planning and Disaster Recovery
PPSM: Personnel Policy for Staff Members, Section 21 Employment
RMP-2, Records Retention and Disposition: Principles, Processes, and Guidelines
Security at the University of California
Management Guide for Information Security
UC Privacy and Data Security Incident Response Plan
Information Security Resources at UCSB