Information Technology Resources Guidelines

College of Agricultural & Environmental Sciences

Table of Contents

1. Purpose

This document is intended to provide specific guidance for compliance with University of California Policy BFB-IS-3[1] in a cost-effective and risk-based manner while maintaining a safe and reliable computing environment that supports the needs of faculty, students, and staff. Guidance described in the UC Davis Location Information Management Security Program (ISMP) may supersede requirements described in this document.

2. Background

IS-3 follows both a standards- and risk-based approach to information security to ensure that UC meets industry, government and regulatory requirements while also properly scoping controls and making appropriate investment decisions.

The policy establishes a framework to achieve six goals:

- Preserve academic freedom and research collaboration
- Protect privacy
- Follow a risk-based approach
- Maintain confidentiality
- Protect integrity
- Ensure availability

The policy incorporates a subset of controls from the international standards ISO 27001 and ISO 27002 that align with and support UC's mission of research, teaching and public service. IS-3 also addresses legal requirements associated with HIPAA, the Payment Card Industry (PCI) and other state and federal regulations and includes requirements needed to qualify for certain grants that are essential to UC research funding (NIST 800-171). Additionally, IS-3's risk-based approach guides the allocation of resources by evaluating risk and assessing the cost and benefit of risk management.

3. Scope

These guidelines apply to all of the following[2]:

- All Workforce Members, Service Providers and other authorized users of Institutional Information and IT Resources.[3]
- All use of Institutional Information, independent of the location (physical or cloud) or ownership of any device or account that is used to store, access, process, transmit, or control Institutional Information.
- All devices, independent of their location or ownership, when connected to a UC network or cloud service by Workforce Members, Service Providers, and authorized

[1] https://policy.ucop.edu/doc/7000543/BFB-IS-3
[2] Page 3, Scope for https://security.ucop.edu/files/documents/policies/minimum-security-standard.pdf
[3] See https://security.ucop.edu/policies/quick-start-guides-by-role/index.html for particular guidelines by role

users, which may include Suppliers providing Workforce Members, used to store or process Institutional Information.
- Research projects performed at any Location, and UC-sponsored work performed by any Location.

The Standard (and these Guidelines) do not apply to the following:
- End-user devices used and owned by students for the purposes of attending the University and completing projects.
- Students who are not Workforce Members.[4]

Workforce Members must signify their understanding and acceptance of these Information Technology Resources Guidelines via electronic signature.

4. Glossary

For the purposes of this document, the following terms and definitions given in the University of California BFB-IS-3 apply.

CISO: A role responsible for security functions throughout a Location, including assisting in the interpretation and application of this policy.

Institutional Information: A term that broadly describes all data and information created, received and/or collected by UC.

IT Resources: A term that broadly describes IT infrastructure, software and/or hardware with computing and networking capability. These include, but are not limited to: personal and mobile computing systems and devices, mobile phones, printers, network devices, industrial control systems (SCADA[5], etc.), access control systems, digital video monitoring systems, data storage systems, data processing systems, backup systems, electronic and physical media, biometric and access tokens and other devices that connect to any UC network. This includes both UC-owned and personally owned devices while they store Institutional Information, are connected to UC systems, are connected to UC Networks or used for UC business.

Information Management Security Program: A minimum set of information security requirements, providing Locations with the following four methods of identifying applicable security controls to manage cyber security risk:

- Conduct a Risk Assessment – see Part III, § 6 of BFB-IS-3.
- Use a Risk Treatment Plan – see Part III, § 6.1.2 of BFB-IS-3.
- Use this policy and related standards to identify applicable controls.

[4] See question 10 on https://security.ucop.edu/files/documents/policies/is-3-faq.pdf
[5] https://en.wikipedia.org/wiki/SCADA

- Some combination of the above.

Location: A discrete organization or entity governed by the Regents of the University of California. Locations include, but are not limited to: campuses, laboratories, medical centers and health systems, as well as satellite offices, affiliates or other offices in the United States controlled by the Regents of the University of California.

Service Provider: A UC internal organization that offers IT services to Units. Service Providers typically assume most of the security responsibility and help Units understand Unit responsibilities with respect to cyber security.

Supplier: An external, third-party entity that provides goods or services to UC. BFB-IS-3 Part III § 15 describes what Suppliers must do. UC has specific contract terms that clarify the responsibilities of Suppliers and protect UC.

UC: University of California.

Unit: A point of accountability and responsibility that results from creating/collecting or managing/possessing Institutional Information or installing/managing IT Resources. A Unit is typically a defined organization, such as the school of engineering, or a set of departments, such as student affairs. Because UC is a highly decentralized and independent federation of organizational units, the policy provides Units with the flexibility and responsibility to manage cyber risk.

Unit Head: A generic term for dean, vice chancellor or person in a similarly senior role who has the authority to allocate budget and is responsible for Unit performance. At a particular Location or in a specific situation, the following senior roles may also be Unit Heads: department chairs, assistant/associate vice chancellor (AVC), principal investigators, directors or senior managers. Unit heads have important responsibilities to ensure effective management of cyber risk.

Unit Information Security Lead: A term for the Workforce Member(s) assigned responsibility for tactical execution of information security activities including, but not limited to, implementing security controls; reviewing and updating Risk Assessment and Risk Treatment plans; devising procedures for the proper handling, storage and disposal of electronic media within the Unit; and reviewing access rights.

Workforce Member: An employee, faculty, staff, volunteer, contractor, researcher, student worker, student supporting/performing research, medical center staff/personnel, clinician, student intern, student volunteer or person working for UC in any capacity or through any other augmentation to UC staffing levels.

5. Data Classification

Protection and Availability Levels are used to help assess risk and select security controls required by this guideline.[6]

Protection (P) Levels	
P4	***Statutory, regulatory and contract obligations are major drivers for this risk level***. Other drivers include, but are not limited to, the risk of significant harm or impairment
P3	***Unauthorized disclosure or modification could result in small to moderate fines, penalties or civil actions***. Could result in moderate damage to UC, its students, patients, research subjects, employees, community and/or reputation; could have a moderate impact on the privacy of a group; could result in moderate financial loss
P2	May ***not be specifically protected*** by statute, regulations or other contractual obligations or mandates, but are generally ***not intended for public*** use or access
P1	Public information or information intended to be readily obtainable by the public, but whose integrity is important and for which unauthorized modification is the primary protection concern. IT Resources where the application of minimum security requirements is sufficient
Availability (A) Levels	
A4	***Loss of availability would result in major impairment to the overall operation*** of the Location and/or essential services, and/or cause significant financial losses
A3	Loss of availability would result in moderate financial losses and/or reduced customer service
A2	Loss of availability may cause minor losses or inefficiencies
A1	Loss of availability poses minimal impact or financial losses

[6] https://security.ucop.edu/policies/institutional-information-and-it-resource-classification.html

6. Guidelines

6.1. CAES Information Security Program Management

Information security and risk management decisions will be made consistent with this guideline. The Unit Head is responsible for the CA&ES Information Security Program. The Unit Information Security Leads are responsible for the tactical execution of this guideline. All Workforce Members are responsible for ensuring the protection of Institutional Information and IT Resources.

6.2. Risk Management

The risk management process will involve:

- Identifying and classifying assets
- Protecting assets and assessing risks based on the requirements described in this guideline
- Monitoring risks on an ongoing basis

6.2.1. Risk Assessment

A Risk Assessment program shall be established in collaboration with the CISO by the Unit Information Security Leads that requires performing routine risk assessment of CA&ES Units. At a minimum, this assessment should include the Protection Level and Availability Level[7], and the Service Provider or Supplier for all IT Resources in use by the Unit.

6.2.2. Risk Treatment

A Risk Treatment Plan, reviewed and/or updated annually, shall be completed by the Unit Information Security Leads, and signed off on by the Unit head.

6.3. Exceptions Management

This guideline describes a risk-based approach to managing information security within the college. Exceptions to these guidelines are approved by the Unit Head, who assumes the risk.[8] If required by the UC Davis ISMP, exceptions must be registered and approved by the CISO. For each exception registered with the CISO, a Risk Assessment and Risk Treatment Plan shall also be filed.

6.4. Device Management

Devices include workstations, laptops, mobile phones, and tablets. The College shall establish a Device Support Policy (Appendix A) consistent with business needs and protection of Institutional Information. Items that must be addressed include the allowable number of Devices per Workforce Member, and support of personally-owned devices containing

[7] https://security.ucop.edu/policies/institutional-information-and-it-resource-classification.html
[8] See questions 4, 5, and 6 on https://security.ucop.edu/files/documents/policies/is-3-faq.pdf

Institutional Information. In addition, each device must be configured according to Appendix B: Minimum Security Standards.

6.4.1. Procuring Devices

Where possible, supported devices should be procured via agreements in Aggie Buy[9] using standards such as Aggie Desktop[10] to take advantage of UC pricing and economies of scale.

6.4.2. Operating systems

Supported devices must run a currently maintained and patched version of Android, iOS, Linux, MacOS, or Windows.

6.4.3. Malware Protection

Supported devices must run malware protection software as detailed in Appendix B: Minimum Security Standards.

6.4.4. Warranty and Inventory

All supported devices must be warrantied and inventoried. The CA&ES standard for inventory management software is PEAKS (People, Equipment, Access, Keys, and Space)[11]. The Warranty and Replacement schedule is given in Appendix C. Replaced devices shall be retired via Aggie Surplus[12] in accordance with UC Davis policy[13].

6.4.5. Accountability

In order to provide updated inventorial accountability, every Workforce Member issued a supported device must positively affirm receipt, relinquishment, or retirement of that device in PEAKS or a similar system.

6.5. Access Management

To use IT Resources, each Workforce Member must be assigned one or more accounts of the following types:[14]

- User accounts, such as the campus login, are under the control of a specific individual and used to access systems such as Office 365, Aggie Budget, etc. Campus directive requires the use of Duo 2-factor authentication for all campus accounts, which must not be accessible to others.
- Functional or shared accounts may be accessed by multiple individuals to accomplish a shared purpose or appear as a single entity (e.g. CA&ES Advising).

[9] https://aggiebuy.ucdavis.edu
[10] https://aggiedesktop.ucdavis.edu
[11] https://peaks.ucdavis.edu/Home/
[12] https://supplychain.ucdavis.edu/procure-contract/stores/aggie-surplus
[13] https://ucdavispolicy.ellucid.com/documents/view/505
[14] https://security.ucop.edu/files/documents/policies/account-and-authentication-management-standard.pdf

Commented [j1]: *We cannot effectively manage risk for hardware, software, or services we do not know exist and we will want to proactively make sure no one orders something that we cannot get in compliance with relevant policies. In that context I think we should include a statement here that "The local IT department must review requests for IT systems prior to purchase to make sure they can be secured and that they will be properly configured and tracked once in use."*

Reference: IS-3 Mandated Security Controls document states "Make sure devices can be secured before making a purchasing decision. Make sure IT Resources and Institutional Information are appropriately recorded in Location inventory. Consult your Location IT department or online resources to determine whether a device requires approval and recording in inventory. Many security breaches can be prevented or their impact minimized if your IT department is aware of your device and what's stored on it." https://security.ucop.edu/policies/security-controls-everyone-all-devices.html

Commented [j2]: We have many computers off-network connected to lab equipment running various older operating systems. Recommend consideration for re-wording this to "Supported **network** devices must…"

Reference: Page 29 IS-3 Policy section 12.6
"Units must protect IT Resources that cannot be patched to current standards with compensating controls approved through the exception process **or remove the IT Resource from network access."**

Commented [RK3]: Chrome OS :)

Commented [j4]: We have many computers off-network connected to lab equipment without updated anti-malware. Recommend consideration for re-wording to "Supported **network** devices must…"

Commented [j5]: We have many computers operating outside of warranty and this requirement would not work for our unit at all. Recommend change this to "should be warrantied where feasible and must be inventoried."

Commented [RK6]: Still not sure this is adequate language for departments who may save extend the life of computers beyond the warranty.

- Privileged accounts are used in the administration of IT Resources. They must be separate from and unable to access regular user account systems (such as email), must be used only when required, and access must be relinquished as soon as the functions of the privileged account are no longer necessary. See Appendix D: Privileged Account Policies for further details.

UC Davis accounts should not be used or affiliated with personal accounts (e.g. Facebook). Outside vendor accounts such as Amazon, which may use UC Davis email by default, should be separated into personal and business accounts.[15]

Commented [RK7]: Except that social media is part of some of our jobs.

Commented [RK8]: I assume this means UCOP expects us to untangle decades of using our UC address for personal accounts?

6.6. Software Management

Software on supported devices should have an explicit business purpose. Unless otherwise required (e.g. for compatibility with equipment/software or due to licensing restrictions), the most recent version should be used. Refer to Appendix E, Supported Software Standard.

6.6.1. Supplier Software Licensing

All software obtained from a Supplier must have a license that conforms with the business agreement between UC and the Supplier. Software Licenses are often audited by the Supplier, and non-compliance may expose UC to significant financial penalties. Installation of Supplier Software should be done by automated means to ensure compliance. The standard for automated software deployment and removal is listed in Appendix E.

Commented [RK9]: We might want to spell out that software, and clould software agreements must be reviewed by campus purchasing?

6.6.2. Open Source

Use of Open-source software[16] should conform with the guidelines for using Copyright-Protected Materials.[17]

6.6.3. Incidental Personal Use

Software for incidental personal use is allowed as long as it does not interfere with Supported Software. Software that does interfere with Supported Software will be removed.

Commented [j10]: We do not install any personal software for users in my unit and I am concerned this wording will open up the door for a ton of wasteful requests we cannot support. Recommend consideration for rewording this using the current campus "incidental personal use" wording, which helps us to say no to things like “use university resources to have your staff install turbotax (or “harmless” video game that de-stresses me during breaks)” requests.

Software for incidental personal use is allowed as long as it does not interfere with Supported Software and its use does not directly or indirectly interfere with the University's operation of resources, does not interfere with the user's employment or other obligations to the University; does not burden the
University with noticeable incremental costs; and does not violate the law or University policy. Software that does interfere with Supported Software or university operations will be removed.

Reference:
https://ucdavispolicy.ellucid.com/documents/view/357

6.7. Data Management

Electronically stored information must not be unintentionally released or accessed by unauthorized parties. Security standards in Appendix B address this goal.

[15] See §4.5 of https://security.ucop.edu/files/documents/policies/account-and-authentication-management-standard.pdf
[16] https://en.wikipedia.org/wiki/Open-source_software
[17] https://research.ucdavis.edu/industry/ia/researchers/copyright/copyright-protected/

6.7.1. Encryption[18]

All laptops, mobile devices, and portable storage (e.g. USB keys) must be encrypted to ensure that easily lost physical media is default protected in accordance with state and federal law. Encryption keys shall be stored in a central repository accessible to the Service Provider. In most cases, knowledge of the encryption key is not required by the Workforce Member to access electronically stored information. Provision of an encryption key to a Workforce Member (e.g. for remote recovery of corrupted systems) requires that the device be re-encrypted with a different key as soon as practical. See Appendix F for further details.

6.7.2. Backups

All laptops and mobile devices shall be backed up to ensure that loss or hardware failure of the device does not cause loss of Institutional Information.[19] See Appendix G: Backup Standards for further details.

6.7.3. UC Email and Calendar

All UC business done by email shall be transacted with a UC email account (Office 365 or DavisMail). The standard for email and calendar is listed in Appendix E.

6.7.4. Institutional Information documents

All Institutional Information documents shall be stored in Box[20], unless classified as HIPAA[21] or PCI[22] information. HIPAA or PCI data shall be stored in a secure filesystem. See Appendix H: Data Storage, Retention, and Disposal Standards, and the Data Sensitivity Guide[23] for further details.

Commented [j11]: Recommend consideration for rewording this to make it clear there are other data types prohibited or would require further approvals before being stored on Box "All Institutional Information documents shall be stored in Box21 unless classified as HIPAA22, PCI23 information **or otherwise restricted as noted in Appendix H**. HIPAA, PCI, **or other restricted data noted in Appendix H** shall be stored in a secure filesystem. See Appendix H:Data Storage, Retention, and Disposal Standards, and the Data Sensitivity Guide24 for further details."

Commented [RK12]: I think this should say Approved Cloud storage or local storage.

6.7.5. Personal devices

Institutional Information must not be stored on personal devices unless the personal device is managed by the Service Provider.[24] Access to UC IT Resources must be mediated by a secured system that is configured to protect Institutional Information appropriately. The standard for access by personal devices is listed in Appendix E.

6.8. Incident Management

The CA&ES Information Security Incident Response Plan meets the minimum standards described in the UC Information Security Incident Response Standard[25] and/or the UC Davis

[18] https://security.ucop.edu/files/documents/policies/encryption-key-and-certificate-management-standard.pdf
[19] See question 2 in https://security.ucop.edu/files/documents/policies/is-3-implementation-faq.pdf
[20] https://box.ucdavis.edu
[21] https://www.ucop.edu/ethics-compliance-audit-services/compliance/hipaa/
[22] https://cashier.ucdavis.edu/banking-services
[23] https://cloud.ucdavis.edu/services/box-davis
[24] https://security.ucop.edu/policies/security-controls-everyone-all-devices.html
[25] https://security.ucop.edu/files/documents/policies/incident-response-standard.pdf

Information Security Management Plan (ISMP). Details may be found in Appendix I: Information Security Incident Response Plan Requirements.

6.9. Physical Security

Devices and Institutional Information must be physically secured. Institutional Information residing in the Cloud must have appropriate physical restrictions on the location of datacenters.

Commented [RK13]: Cloud vendors must be approved by campus purchasing so as to comply with UC policy.

6.10. Procurement

Research, teaching, and administrative service require systems that are purchased, leased, open sourced, developed in-house, or hosted in the cloud and configured (or developed) by the College, Service Provider, or Supplier. These applications represent significant resources, knowledge, and expenditures for UC. They may also present significant cyber risks if not configured properly and/or developed according to secure software development practices. As with other policies in these guidelines, the goal is to ensure that such IT Resources maintain confidentiality, protect integrity, and ensure availability. Procuring or developing such applications must follow the standards in Appendix J: Secure Software Configuration and Development and the UC Davis Bidding Guidelines.[26]

[26] https://supplychain.ucdavis.edu/sites/g/files/dgvnsk2181/files/inline-files/UCDavisBiddingMatrix070118.pdf

Appendix A: Device Support Policies

Device Support Policies may be customized to the individual needs of the units.

Devices per Workforce Member

To maintain efficient support, no more than 2 devices of any type (workstation, laptop, phone, or tablet) per Workforce Member shall be supported by the Service Provider (e.g. the Computing Resources Unit for the CA&ES Dean's Office).

Personal devices

Support for personal devices may be limited by the Service Provider for the Unit, as follows:

- Configuration of Office 365 or DavisMail
- Configuration of access to remote services such as VPN or Box
- Configuration of 2-factor authentication

Appendix B: Minimum Security Standards

#	Topic	Requirement[27]	CA&ES Standard
1	Anti-malware	Anti-malware software must be installed and running up-to-date definitions.	Sophos or BitDefender with central console
2	Patching	Supported security patches must be applied to all operating systems and applications.	BigFix on Windows and MacOS, Puppet on Linux
3	Privileged accounts	Non-privileged user accounts must be used and only elevated to root or Administrator when necessary.	Local user admin managed with LAPS in uConnect
4	Encryption	Laptops and mobile devices must be encrypted. Separately, Institutional Information classified at Protection Level 3 or higher must be encrypted when stored on Laptops and mobile devices.	Windows: BitLocker MacOS: FileVault
5	Session timeout	Devices used to store or access Institutional Information or IT Resources classified at Protection Level 2 or higher must employ lockout/screen-lock mechanisms or session timeout or to block access after a defined period of inactivity (15 minutes or Location limit). Mechanisms must require re-authentication before a return to interactive use.	Windows: 15 minutes by group policy MacOS: 15 minutes by screensaver setting
6	Password/PIN	Secure devices with a strong password, PIN, smart card or biometric lock.	Duo for all campus accounts. At least a 6-digit PIN.
7	Physical security	Devices and Institutional Information must be physically secured.	Servers in Data Center. Workstations in locked offices or laboratories using key cards inventoried by PEAKS. External security cameras where appropriate monitored by UCD Police according to policy.
8	Backup	Institutional Information classified at Availability Level 3 or higher must be backed up and recoverable. Backups must be protected according to the classification level of the information they contain.	CrashPlan for all laptops. DPM for servers. Box for all business data.
9	Portable media	Backups and portable media containing Institutional Information classified at Protection Level 4 must be encrypted and safely stored.	Minimize use of portable media; use CrashPlan for Backups or Box for storage
10	Host-based firewall	If host-based firewall software is available on a device, it must be running and configured to block all inbound traffic that is not explicitly required for the intended use of the device.	Network firewalls with ingress and egress rules
11	Approval and inventory	Make sure devices can be secured before making a purchasing decision. Make sure IT Resources and Institutional Information are appropriately recorded in Location inventory.	PEAKS
12	Supported Operating Systems	Run a version of the operating system that is supported by the vendor.	macOS 10.13 or 10.14 Windows 10 Ubuntu 18.04

Commented [j14]: Win 8.1 is still supported through 1/10/2023. We still have around 140 Win 8.1 systems we are in the process of upgrading to Win 10 (our upgrade is related to the likely upcoming EOL of Box Sync, not compatible with Win 8.1). We would need a little bit more time before we can close off support for Win 8.1.

[27] https://security.ucop.edu/files/documents/policies/minimum-security-standard.pdf

Appendix C: Warranty and Replacement Schedule

The Warranty and Replacement schedule may be customized to the individual needs of the units.

Warranties

Warranties are purchased for the duration of the Replacement Schedule, where possible. Apple and some other vendors only have 3 year warranties; the last year(s) of service may still be supported. Alternately, units may specify desktops and laptops from these vendors with a 3 year replacement schedule.

Replacement Schedule

- Desktops: 5 years
- Laptops: 4 years
- Mobile devices (phones and tablets): 3 years
- Monitors: 8 years

There are instances in which the Replacement Schedule may be accelerated by a year, e.g. high-performance lab computers or workstations for faculty or staff with compute-intensive workloads.

Funding

The Dean's Office funds workstations for career/permanent positions in central administrative units as follows:

- Desktops: $800
- Laptops: $1400
- Laptop Dock (keyboard, mouse): $250
- Monitors: $500

These amounts are intended to cover the full cost for standard configurations procured through AggieBuy. Any costs beyond these levels for custom configurations must be covered by unit funds. Mobile devices and their plans are also covered by unit funds.

Workstation standards

A desktop system is a tower or mini chassis, two monitors (or a single widescreen), a keyboard, and a mouse.
A laptop system is a laptop, dock, two monitors (or single widescreen), keyboard, and a mouse.

Multiple offices

The Dean's Office will cover one office workstation. Additional office workstations must be covered by unit funds. Note that in the case of laptop systems, additional docks and monitors are all that are required.

Appendix D: Privileged Account Policies

Privileged accounts are used to administer IT Resources. Examples include:

- Local administrator account on a laptop
- "root" access to the network firewall
- uInform access to uConnect administration tools

Privileged accounts must have a strictly defined scope of access, and must be used only when required, only for how long required.

In accordance with the UC Account and Authentication Management Standards[28], privileged account access is provided on a strictly necessary basis. An example would be a faculty member traveling internationally or in locations with poor internet access for which the Service Provider is unable to provide an acceptable level of service.

Privileged account use may be logged as required by policy (e.g. PCI DSS standards[29]).

As needed, systems on which privileged account access was granted may be rolled back or reimaged to a state before the privileged account actions were taken.

[28] https://security.ucop.edu/files/documents/policies/account-and-authentication-management-standard.pdf
[29] https://www.pcisecuritystandards.org/document_library

Appendix E: Supported Software Standard

The Supported Software Standard may be customized to the individual needs of the units.

Software Installation

To ensure compliance with licensing, all software must be installed by BigFix[30] (MacOS, Windows) or Puppet (Linux).[31]

Email and Calendar Standard

The standard for email and calendar is Office 365.[32]

Personal device access to Institutional Data

The standard for access by personal devices is Office 365, Box[33], or Remote Desktop.

Supported Software List

- .NET 3.5
- 3DF Zephyr Free
- 7-Zip 16.04
- Adobe Acrobat DC 2017
- Adobe Creative Cloud
- ArcGIS 10.5
- ArcGIS Online
- ArcGIS Pro
- AutoCAD 2017
- Box for Office
- Box Tools
- California Wildlife Habitat Relationships
- Cytoscape 3.6.0
- DNR GPS 6.1.0.6
- Easy GPS 5.79.0.0
- EndNote X7 17.7.1
- FileZilla Client 3.29.0
- Flapjack v1.16.10.31
- GeoDa 1.12
- Git Bash
- Google Chrome
- Google Earth Pro 7.3.0

[30] https://itcatalog.ucdavis.edu/service/bigfix
[31] https://puppet.ucdavis.edu
[32] https://365.ucdavis.edu
[33] https://box.ucdavis.edu

- Grasshopper
- GWR4 4.09
- IDL 8.4 and ENVI 5.2
- Integrated Genome Browser 9
- Irricad Pro V15
- Java 8 Update 152
- Java 8 Update 162
- Lumion 8.3
- Marxan
- MEGA 7
- Microsoft Office 2019
- Model Viewer
- ModelMuse
- Mozilla Firefox
- Notepad++ 7.5.3
- Pix4Dmapper
- PSPP
- PuTTy 0.70
- QGIS 2.18.15
- R for Windows 3.4.3
- Rhinoceros 5.14
- RhinoTerrain 2 LAB
- RStudio 1.1.383
- SketchUp Pro 2018
- Tablet v1.17.08.17
- Vectorworks 2018
- Vector NTI v11
- Windows Subsystem for Linux
- WinSRFR 4.1.3
- WinSIPP3

Appendix F: Encryption Standards

Android
Default

iOS
Default

Linux
Encrypt the /home directory

MacOS
FileVault

Windows
BitLocker

Appendix G: Backup Standards

Backup Standards may be customized to the individual needs of the units, excepting Institutional Information classified at A3 or P3.

Android

Google account

iOS

iCloud account

Commented [RK15]: Are you purchasing ICloud storage for all of your users?

Laptops

CrashPlan[34]

[34] https://itcatalog.ucdavis.edu/service/crashplan

Appendix H: Data Storage, Retention, and Disposal Standards

Data Storage

A unit share is a location that stores information accessible to multiple Workforce Members. A home directory is a location that stores information accessible to a single Workforce Member.

A secure encrypted fileserver is encrypted, network isolated to specifically allow only authorized users, and has access controls audited on a quarterly basis.

A secure encrypted service is encrypted, requires 2-factor authentication for authorized users, and has access controls audited on a quarterly basis.

Data Type	Location[35]
Personal Information	Box home directory
Institutional Information	Box unit share
PII low level	Box unit share
Student education records	Box unit share
Credit Card or Payment Card Industry (PCI) information	Secure, encrypted fileserver or service
Export Controlled Research (ITAR, EAR)	Secure, encrypted fileserver or service
Medical/Health Information	Secure, encrypted fileserver or service
Protected Health Information (HIPAA)	Secure, encrypted fileserver or service
Attorney/Client Privileged Information	Secure, encrypted fileserver or service
Federal Information Security Management Act (FISMA) Data	Secure, encrypted fileserver or service
IT Security Information	Secure, encrypted fileserver or service
Other Sensitive Institutional Data	Secure, encrypted fileserver or service
Personally Identifiable Information (PII) High Level	Secure, encrypted fileserver or service
Personally Identifiable Information (PII) Moderate Level	Secure, encrypted fileserver or service
Sensitive Identifiable Human Subject Research	Secure, encrypted fileserver or service
Student Loan Application Information (GLBA)	Secure, encrypted fileserver or service

Retention Schedule

The University of California Records Retention Schedule[36] is defined by BFB-RMP-1: University Records Management Program[37] and comprises hundreds of record types. Additional polices

[35] Based on the Data Sensitivity Guide for Box. https://cloud.ucdavis.edu/services/box-davis
[36] https://recordsretention.ucop.edu
[37] https://policy.ucop.edu/doc/7020453/BFB-RMP-1

apply in the event of "pending, foreseeable, or ongoing litigation; an investigation; or an ongoing audit pertaining to the records"; contact the appropriate records management coordinator for further guidance.[38]

Disposal Methods:

Guidelines from the UC Institutional Information Disposal Standard.[39] See §§3-4 for a definition of terms and requirements.

	Institutional Information Protection Level[40]			
Device/Data Location	*P1*	*P2*	*P3*	*P4*
Hard disk drives – portable or internal	Delete	Clear	Purge	Purge/Destroy
Logical Storage	Logical Delete	Logical Delete	Cryptographic Erase	Cryptographic Erase
Optical disk – read only (CD_ROM, DVR_ROM, etc.)	Destroy	Destroy	Destroy	Destroy
Optical disk – read/write (CD-R/W, DVD-R/W, etc.)	Delete	Clear	Destroy	Destroy
Other embedded storage devices	Delete	Clear	Purge	Purge
Portable media – electronic (thumb drive, USB stick)	Delete	Clear	Purge	Destroy
Portable magnetic media – tape	Delete	Degauss	Destroy	Destroy
Solid state drives (SSD)	Delete	Cryptographic Erase	Cryptographic Erase	Cryptographic Erase

[38] https://www.ucop.edu/information-technology-services/initiatives/records-management/records-management-committee.html
[39] https://security.ucop.edu/files/documents/policies/uc-institutional-information-disposal-standard.pdf
[40] https://security.ucop.edu/policies/institutional-information-and-it-resource-classification.html

Appendix I: Information Security Incident Response Plan Requirements

The minimum standards for an Information Security Incident Response Plan is given by the UC Information Security Incident Response Standard.[41] This plan must be on file for every Unit, and include the following elements:

1. Identify Incident Response Team members.
    a. Determine and assign roles.
    b. Describe responsibilities for a role's duties pertaining to Incident response.
2. Indicate when to use the plan.
    a. Define Significant Incident.
    b. Define Routine Incident.
3. Assign to a role the responsibilities of entering information into SIREN.
4. Create an Information Security Incident Communication Plan and identify how and when to use the plan. This will also address privacy Incidents.
5. Determine if Counsel should lead the investigation and Incident response. This review and determination should occur at an early stage of the Incident response process and be reviewed when new pertinent information arises.
6. Determine Location procedures for Incident handling (run-books, playbooks, etc.).
    a. Determine how to gather evidence for detection and analysis.
        i. Collect and review initial Incident logs and information.
    b. Conduct Incident prioritization.
        i. In the absence of accurate inventory and based on the risk associated with the event, the LLA and IRTC must treat the event as a Significant Incident during the initial triage.
    c. Document the Incident.
        i. Use the Location reporting tool(s) (e.g., ServiceNow).
        ii. Evaluate the initial information about the Incident using the Incident classification criteria.
        iii. Incident characteristics:
            1. Impact to Protection Level and Availability Level.[42]
            2. Number of records affected.
        iv. Open a case in SIREN as needed for Significant Incidents.
        v. Create other supporting documentation, which can include:
            1. Meeting minutes.
            2. Communication record.
            3. Decisions log.

[41] https://security.ucop.edu/files/documents/policies/incident-response-standard.pdf
[42] https://security.ucop.edu/policies/institutional-information-and-it-resource-classification.html

d. Include procedures for containment, eradication and recovery.
    i. Identify and engage relevant expertise.
    ii. Implement a containment strategy.
    iii. Properly gather, handle and preserve evidence.
    iv. Eradicate/remove the unauthorized tools used and the vulnerabilities present during the Incident.
    v. Recovery.
e. Conduct forensic analysis.
    i. Identify when to engage with forensic vendors/services.
f. Determine when to engage the UC Security Incident Response Coordination (SIRC).
g. Indicate when to engage supporting ISACs (e.g., National Health, Research and Education, Multi-State, etc.).
h. Explain when to engage with law enforcement.
    i. UCPD.
    ii. External law enforcement agencies.
    iii. Coordinate California Department of Justice, California Highway Patrol, other states' law enforcement, FBI or other federal law enforcement engagement with UCOP's Systemwide CISO's office, c3@ucop.edu.
i. Identify when to engage research sponsors and/or partners.
j. Determine when to notify affected individuals and/or regulatory agencies.
k. Develop a process to identify and comply with short notification deadlines (e.g., evolving state regulations, the 72-hour deadline to notify regulators as required by the General Data Protection Regulation (GDPR), the duty to notify certain federal contracting parties within one hour of discovery, the duty to notify payment card processors or merchant banks of certain payment card incidents within 24 hours, etc.).

7. Note how and when to account for special circumstances, such as:
    a. In the case of a suspected insider threat and/or when a particular Incident Response Team member is a person of interest, the Incident Response Coordinator, LLA or CRE will remove that person from the Incident Response Team.
    b. At the determination of the LLA, some individuals or teams may not lead investigations within their own areas of responsibility in order to avoid possible conflicts of interest.
8. Establish the process for coordination with:
    a. Location Counsel.
    b. UCOP's Cyber-risk Coordination Center (C3).
    c. UCOP's Office of General Counsel (OGC).
9. Develop a plan for post-Incident activity.
    a. Evaluate lessons learned.
    b. Report findings.
    c. Conduct Incident follow-up.
    d. Take required technical actions.
    e. Review procedures and team effectiveness.
    f. Develop recommendations and next steps.

10. Plan for periodic testing of the Information Security Incident Response Plan.

Appendix J: Secure Software Configuration and Development

Software Configuration Standards[43]

1. General options
   a. Enable appropriate security controls
   b. Enable auditing to detect malicious actions
   c. Configure application as "secure by default"
2. Secure communications protocols
   a. Disable unencrypted protocols when encrypted protocols are available
      i) Protection Level 3 or higher must be transmitted using secure protocols
   b. TLS 1.2 or later must be used for:
      i) Credential exchange
      ii) Transmission of data at Protection Level 3 or higher
      iii) CISO-approved cipher for TSL must be used
   c. HTTPS must be forced (no HTTP connections)
   d. Certificate authority-signed certificates must be used (e.g. no self-signed certificates)
   e. Anonymous connections are only allowed for data at Protection Level 1
3. Default credentials must be removed
4. File and cloud access to files and information must be set to appropriate (e.g. "need to know") levels
   a. CISO-approved methods for authentication must be used
5. Local and cloud access to administrative consoles must be restricted to intended parties
   a. Unique service account credentials must be set for each logical part of the application
   b. Re-use of credentials is prohibited
   c. Credentials must be encrypted in transit and at-rest
   d. Service account use must conform with UC Account and Authentication Management Standard.[44]
   e. Supplier remote access must be secured with multifactor authentication and unique credentials
   f. Session time-outs must be set to CISO approved values
6. Separate applications and databases
   a. Applications at Protection Level 3 must have separated application and database servers
7. Software version and patching
   a. Operating systems and patching must comply with the UC Minimum Security Standard.[45]
   b. Other software and patching must comply with the UC Minimum Security Standard.
8. Development and test systems

[43] Summarized from https://security.ucop.edu/files/documents/policies/secure-software-configuration-standard.pdf
[44] https://security.ucop.edu/files/documents/policies/account-and-authentication-management-standard.pdf
[45] https://security.ucop.edu/files/documents/policies/minimum-security-standard.pdf

   a. Separate, secure test and development systems must be configured to protect production systems, Institutional Information, and credentials appropriately
   b. Systems must be placed on approved Location network designed for protection of Institutional Information and IT Resources
9. Character encoding must be UTF-8 or standard character set which enables full input validation
10. Applications storing Protection Level 3 or higher must comply with the UC Event Logging Standard.[46]
11. Hardening scripts must be executed for applications and operating systems processing or storing Protection Level 3 or higher data.
12. Encryption at Rest must be enabled for Institutional Information classified at Protection Level 3 or higher.
13. Backup and archival
   a. Encrypt Protection Level 3 or higher data stored on removable media
   b. Meets record retention schedule.[47]
   c. Meets business continuity requirements.[48]
14. Security agents such as anti-malware, logging, firewalls, intrusion detection, and compliance tools must be installed as required by the Location ISMP.
15. APIs, interfaces, and data transfers
   a. Protection Level 3 or higher data must be secured by authentication and encryption
   b. API keys must be managed per the UC Encryption Key and Certificate Management Standard.[49]

Secure Software Development Standards[50]

The CA&ES Software Development Lifecycle (SDLC) includes the following security elements:

- Security planning using secure cloud-based infrastructure (Azure[51]) with an Attestation of Compliance[52] to the latest Payment Card Industry Data Security Standard (PCI DSS)
- Threat modeling via tabletop exercise from SANS trained IT Workforce Members
- Design incorporates security and privacy guards
- Secure system architecture using web-application firewalls (CloudFlare[53]), secured cloud services (Azure), secured authentication (CAS[54] or AzureAD[55]), systems and exception reporting (Stackify[56]), and secure database and file access (SQLAzure or Azure blob storage)

[46] https://security.ucop.edu/files/documents/policies/event-logging-standard.pdf
[47] https://recordsretention.ucop.edu
[48] https://policy.ucop.edu/doc/7020451/BFB-IS-12
[49] https://security.ucop.edu/files/documents/policies/encryption-key-and-certificate-management-standard.pdf
[50] Adapted from https://security.ucop.edu/files/documents/policies/secure-software-development-standard.pdf
[51] http://azure.microsoft.com/en-us/
[52] https://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx
[53] https://www.cloudflare.com
[54] https://cas.ucdavis.edu
[55] https://azure.microsoft.com/en-us/services/active-directory/
[56] https://stackify.com

- Documentation on GitHub project pages[57]
- Change management using GitFlow[58] workflow, GitHub issues[59], and/or ServiceNow[60]
- Testing using xUnit.net[61]
- Automated software deployment using Octopus Deploy[62] and/or Azure Kudu[63]
- Separate roles of Project Manager, Enterprise Software Architect, Security Developer, Unit Test Developer, Database Developer, and User Interface Designer

The CA&ES standard is that a software fix should be able to be planned, tested, documented, and deployed in a repeatable fashion as quickly as business needs dictate. Software must be easily patchable to continue to meet business needs and security requirements. The following items correspond to §4.1-10 in the UC Secure Software Development Standard.

1. Software Development Process
    a. Code Reviews are conducted regularly by the CA&ES Enterprise Software Architect, Scott Kirkland.
    b. Security reviews conducted by the CA&ES Security Developer, John Knoll, who maintains a GIAC Certified Web Application Defender (GWEB) credential.
    c. Code commits are done in GitHub, with automated xUnit testing (written and maintained by the CA&ES Unit Test Developer, Jason Sylvestre) run by AppVeyor.[64]
    d. Secure, automated code testing/checking is pending replacement of the campus AppScan[65] service.
2. Input Validation
    a. Performed on all user-facing fields via various libraries to sanitize, protect against buffer overflow, array index, or parameter manipulation.
    b. SQL queries are not directly exposed in the application, Object Relational Mapping[66] libraries such as Entity Framework[67] are used instead. This guards against a wide range of SQL attacks. Custom queries against Location databases are developed by the CA&ES Database Developer, Ken Taylor.
    c. .NET MVC[68] is used to rationalize application URLs, preventing credentials, access tokens, PII, or PHI in URIs.
3. Exception and Error Handling
    a. Stackify is used to record exceptions and error handling.

[57] https://help.github.com/articles/user-organization-and-project-pages/
[58] https://datasift.github.io/gitflow/IntroducingGitFlow.html
[59] https://guides.github.com/features/issues/
[60] https://ucdavisit.service-now.com/
[61] https://xunit.github.io
[62] https://octopus.com
[63] https://github.com/projectkudu/kudu/wiki/Process-Threads-list-and-minidump-gcdump-diagsession
[64] https://www.appveyor.com
[65] https://itcatalog.ucdavis.edu/service/application-security-consulting
[66] https://en.wikipedia.org/wiki/Object-relational_mapping
[67] https://docs.microsoft.com/en-us/ef/ef6/index
[68] https://www.asp.net/mvc

    b. Try-catch and/or exception handling is used throughout the applications on the front-end (Javascript[69]) and back-end (C#[70] or NodeJS[71]).
4. Cross Site Scripting
    a. HTML Encoding[72] is used to guard against Cross-Site Scripting attacks.
    b. CSRF tokens[73] used to guard against Cross-Site Request Forgery.
5. Insecure Direct Object References
    a. Are not used.
6. Logging
    a. Stackify is used to log application events and exceptions.
7. TLS and Secure APIs
    a. HTTPS is enforced on both Azure and CloudFlare.
    b. HTTP is disabled on both Azure and CloudFlare.
    c. TLS 1.2 is enabled on Azure.
    d. APIs are encrypted with separate cryptographic keys.
    e. Authentication is performed via CAS using its APIs.[74]
8. Credentials/Passphrases
    a. Passphrases are randomly generated and stored securely encrypted in 1Password for Teams.
    b. Credential lockout policies are enforced via CAS.
    c. Credential protocol exchange is mediated via CAS.
9. Session and Logout
    a. Session timeouts are enforced via CAS.
    b. Session tokens are generated securely via CAS.
    c. Session tokens are deleted and newly created via CAS.
    d. Session tokens are invalidated on logout via CAS.
    e. CAS uses TLS 1.2.
    f. CAS performs logout and prominently displays a logout screen.
    g. Application state is committed or rolled back by the ORM on logout.
10. Federated Authentication/SAML/Shibboleth
    a. Campus CAS, Shibboleth, and/or AzureAD is used for authentication.
11. File Management
    a. File resources in Azure use random GUID.
12. Secure Configuration
    a. Configuration of applications follow the Software Configuration Standards.
13. Documentation
    a. Code documentation and procedures will be maintained in the UC Davis GitHub[75] and ServiceNow instances.

[69] https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Statements/try...catch
[70] https://docs.microsoft.com/en-us/dotnet/csharp/language-reference/keywords/try-catch
[71] https://nodejs.org/en/
[72] https://docs.microsoft.com/en-us/dotnet/api/system.web.mvc.htmlhelper.encode?view=aspnet-mvc-5.2
[73] https://docs.microsoft.com/en-us/aspnet/core/security/anti-request-forgery?view=aspnetcore-2.2
[74] https://apereo.github.io/cas/5.1.x/protocol/CAS-Protocol-Specification.html
[75] https://github.com/ucdavis

14. Version Control
    a. Software is developed in the UC Davis GitHub instance.
    b. Test and Production systems are in separate Azure instances.
    c. GitFlow process is used to track development, test, and production versions
    d. GitHub pull requests[76] are used to track changes and GitHub repository permissions[77] are used to prevent unauthorized merges.

[76] https://help.github.com/articles/about-pull-requests/
[77] https://help.github.com/articles/repository-permission-levels-for-an-organization/