Data Security Plan

Sanitization_Test

Generated by Ursa DSP

2025-12-23

Instructions

This document should be completed by the Unit Information Security Lead (UISL) or Unit IT Director. It will be reviewed by an ISO team member (“ISO Assessor”).

The Lab Director and/or researchers are responsible for providing data security requirements to the UISL or Unit IT Director. The Unit IT Service Provider is responsible for determining and implementing technical solutions.

The technical solution must meet or exceed the UC IS-3 policy, UC Minimum Security Standard and the standard required by the external party.

The UC IS-3 policy requires all researchers to “develop and follow an information security plan that manages security risk over the course of their project.”

Each section contains IS-3 requirements and example controls. Units should complete the controls to meet or exceed all data security requirements. Controls implemented to meet external party requirements should be listed in the appropriate rows.

If you have any questions regarding this form, contact the Information Security Office Risk Team at iso-risk@ucr.edu.

Research Project Data Security Plan

Research Project Name: Sanitization Test **External Party:** State of California **Principal Investigator:** Chuck Forsyth **Lab Director:** Chuck Forsyth **Project Researcher(s):** Chuck Forsyth **Unit:** Research Computing **Department:** Research Computing **Unit IT Director or UISL:** Kelton Adey **Unit Service Provider or IT Director:** Research Computing **ISO Assessor:** [ISO Assessor Name] **CISO:** [CISO Name] **Protection Level:** P4 (High) **Availability Level:** A2 **Meets or Exceeds the Following Compliance Standards or Policies:** UC IS-3, UC Minimum Security Standard, NIST 800-171, State of California Data Security Requirements

Date Approved: [Date]

Revision History

Date	By	Contact Information	Description
[Current Date]	Kelton Adey	[Email Address]	Initial Draft

Revision History

Date	By	Contact Information	Description
2025-10-01	Kelton Adey	kelton.adey@ucr.edu	Initial Document Creation
2025-10-15	Chuck Forsyth	chuck.forsyth@ucr.edu	Final verification of the sanitized output pipeline and updates to P4 data handling controls

Table of Contents

Executive Summary

The **Sanitization Test** project, led by Principal Investigator Chuck Forsyth within the Department of Research Computing, involves the final verification of a sanitized output pipeline utilizing sensitive infrastructure data regarding California urban centers provided by the State of California. Due to the **Protection Level 4 (P4)** classification of the dataset, the project employs a strict security posture compliant with university and state standards.

All sensitive data will be received via secure transfer methods and stored exclusively within a segregated, encrypted **cloud environment (AWS/GCP)** running a hardened Linux operating system. Data analysis will occur solely within this secure cloud infrastructure. To mitigate risk, **no P4 data will be downloaded to local workstations, laptops, or portable storage media**. Access is strictly limited to the Principal Investigator and authorized research staff listed in this plan.

The data will be retained until the project retention date of **2030-01-01**. Upon expiration of this period or the conclusion of the research, all data and associated storage volumes will be destroyed using **DoD-compliant wiping procedures** to ensure the information is irretrievable.

Purpose

The purpose of this data security plan (“Plan”) is to document the security measures and policies for handling data shared with the Principal Investigator (“PI”) by the State of California. If this agreement is executed, all members of the research team with access to the data are contractually obligated to follow all aspects of the plan. The goal of the protections outlined in the plan is to prevent persons who are not signatories, or otherwise authorized, from gaining access to the data.

This plan applies to both raw data received, any copies of the raw data and any derivatives and output of analysis thereof.

Stakeholders, Roles, and Responsibilities

All stakeholders are responsible for reporting any suspected or confirmed incident or breach of data security to the Lab Director, UISL, and ISO immediately.

- **Principal Investigator (PI):** Lead researcher for **Sanitization Test**.
    - Name: **Chuck Forsyth**
    - Full access to the data on the secured analysis computer.
    - No administrative access to the secured analysis computer.
    - Responsible for holding backup of data in escrow.
    - Responsible for supervising all research conducted using the data.
    - Shared responsibility with UISL for ensuring ongoing compliance with all elements of this plan.
- **Unit Information Security Lead (UISL) for Research Computing:** Staff member appointed by the Unit Head with responsibility for information security.
    - Name: **Kelton Adey**
    - Full access to data on the secured analysis computer.
    - Administrative access to the secured analysis computer.
    - Responsible for supervising Unit IT personnel with administrative access to the secured analysis computer and data.
    - Shared responsibility with PI for ensuring ongoing compliance with all elements of this plan.
- **UC Riverside Information Security Office (ISO):** UC Riverside central information security office, under the direction of the Chief Information Security Officer (CISO).
    - No access to data.
    - No access to secured analysis computer.

  - Responsible for reviewing this plan, including approval of any future changes prior to implementation.
  - CISO is the responsible official for signing the data agreement with the State of California (if required by the agency; otherwise, the PI assumes this responsibility).

- **State of California:** Agency providing the data for the sole purpose of the investigation described in the data agreement.
  - Originator of data.
  - No access to secured analysis computer.
- **Service Provider or IT Director for Research Computing:** IT service provider responsible for provisioning, configuring, and managing the IT infrastructure used for processing the data, under the direction of the UISL.
  - Full access to data on the secured analysis computer.
  - Administrative access to the secured analysis computer.
  - Responsible for provisioning, deploying, and maintaining the IT environment for the secured analysis computer.
- **Project Researcher (Researcher):** A researcher attached to the research project who will have access to the raw data under the direction of the PI.
  - Full access to data on the secured analysis computer.
  - No administrative access to the secured analysis computer.

Configuration of Secured Computing and Storage

Access Control

Objective: Limit access to Institutional Information and IT Resources.

UC Requirements (BFB-IS-3 Section 9)	Controls
Least Privilege: Units must ensure access follows Need to	**Cloud IAM:**• Access to Cloud resources is restricted via Identity and Access Management (IAM) roles enforcing Least Privilege.•

UC Requirements (BFB-IS-3 Section 9)	Controls
Know and Least Privilege principles.	Administrative console access requires UCR Single Sign-On (SSO) with Multi-Factor Authentication (MFA).
Network Routing: Units must route network access to P4 data through secure access control points.	**Network Access:**• Access to Linux instances is permitted only via UCR Campus VPN or designated secure gateway IPs.• Direct public internet access to data processing instances is blocked.• Administrative access is routed through a Bastion/Jump host.
Unique Accounts: Each Workforce Member must have a unique user account.	**Authentication:**• Shared root accounts are prohibited. Individual named user accounts are provisioned for Project Researchers.• SSH Key-based authentication is required; password-based login is disabled.• Automatic session timeouts are configured for shell access.

Encryption

Objective: Ensure appropriate physical access to protect UC Institutional Information and IT Resources.

UC Requirements (BFB-IS-3 Section 10)	Controls
Data in Transit: Units must encrypt P3+ data transmitted over a network.	**Transport Encryption:**• All data transfers utilizing the Secure Transfer method employ TLS 1.2 or higher.• SSH v2 is used for all system administration and internal data movement.
Data at Rest: Units must encrypt P4 data stored on any electronic media.	**Storage Encryption:**• Cloud block storage volumes and object storage buckets are encrypted using provider-managed keys (AES-256) or customer-managed keys via Cloud KMS.• Swap space and temporary directories used during the sanitization process are encrypted.

Physical and Environmental Security

Objective: Ensure appropriate access to protect UC IT Resources and Institutional Information.

UC Requirements (BFB-IS-3 Section 11)	Controls
Physical Safeguards: Units must implement and review physical security elements.	**Cloud Infrastructure:**• The project utilizes a FedRAMP-authorized Cloud Service Provider (AWS/GCP).• The Cloud Provider is responsible for physical security of the data centers, including perimeter fencing, biometric entry controls, and 24/7 surveillance.
Off-site Protection: Ensure P4 data is not taken off-site unencrypted.	**No Local Data:**• P4 sensitive infrastructure data remains exclusively within the secure cloud environment.• No raw data is downloaded to local workstations, laptops, or portable media.• Workstations are used only as secure terminals to access the cloud environment via VPN.

Protection from Malware and Intrusion

UC Requirements (BFB-IS-3 Section 12.2)	Controls
Monitoring: Monitor IT Resources to detect signs of attack or compromise.	**Threat Detection:**• Trellix HX (FireEye) agent is installed on all Linux instances for endpoint detection and response (EDR).• Cloud-native threat detection services (e.g., GuardDuty or Security Command Center) are enabled to monitor for malicious network activity and unauthorized API calls.• ClamAV is installed for file-level scanning where appropriate.

Backup

UC Requirements (BFB-IS-3 Section 12.3)	Controls
Recoverability: Ensure Availability Level 3+ is backed up and recoverable.	**Encrypted Snapshots:**• Automated, encrypted snapshots of storage volumes containing configuration and code are taken daily.• Raw P4 data is retained only for the duration of the sanitization test lifecycle; transient backups utilize encrypted cloud storage buckets with strict retention policies.• Backups are geographically replicated to a secure secondary region for disaster recovery.

Logging and Auditing

Objective: Proper logging and monitoring are required practices for recording events and generating evidence.

UC Requirements (BFB-IS-3 Section 12.4)	Controls
Event Logging: Comply with UC Event Logging Standard.	**Centralized Logging:**• OS logs (syslog, auth.log) and Cloud Audit logs are exported to a central logging repository (e.g., Google Chronicle or AWS CloudWatch).• Logs capture successful and failed login attempts, privilege escalation (sudo), and object access.• Logs are retained for a minimum of 3 years.
Log Review: Independently review privileged accounts periodically.	**Audit Review:**• The UISL reviews administrative access logs and cloud audit trails monthly to identify anomalies.• Alerts are configured for modifications to IAM policies or security group rules.

Control of Operational Software

UC Requirements (BFB-IS-3 Section 12.5)	Controls
Change Management: Approval for software installation and configuration changes.	**Software Minimization:**• Only software essential for the sanitization pipeline and OS operation is installed.• Installation of new software packages requires PI or UISL approval.• The environment utilizes immutable infrastructure principles where possible (re-deploying rather than patching live systems) to maintain software integrity.

Vulnerability & Patch Management

UC Requirements (BFB-IS-3 Section 12.6)	Controls
Patching: Use supported and patched	**Vulnerability Management:**• Qualys Cloud Agent is installed on all active instances to provide continuous vulnerability assessment.• Automated patching pipelines are configured to apply critical security

UC Requirements (BFB-IS-3 Section 12.6)	Controls
versions of hardware and software.	updates to the Linux OS within 14 days of release.• Machine images (AMIs/Images) are regularly refreshed to ensure new instances boot with the latest security patches.

Communications Security

Objective: Ensure the security of Institutional Information in transit on networks and between parties.

UC Requirements (BFB-IS-3 Section 13)	Controls
Segmentation: Segment networks for P3+ data.	**Virtual Private Cloud (VPC):**• Cloud network subnets are strictly segmented; data processing nodes reside in private subnets with no direct internet ingress.• Security Groups/Firewall rules block all inbound traffic by default, allowing only SSH traffic from the secure Bastion host or VPN concentrator.• Outbound traffic is restricted via NAT Gateway to specific required repositories and services only.

Transfer of Data from [EXTERNAL PARTY] to UC Riverside

1. **Provisioning Access:** The State of California will provide the Principal Investigator (PI) or Unit Information Security Lead (UISL) with secure access credentials and connection details for their secure file transfer system (e.g., SFTP or HTTPS).
2. **Secure Connection:** The PI or UISL will connect to the Secured Analysis Computer (AWS/GCP Cloud Instance) via the UCR Campus VPN and/or designated management gateway.
3. **Direct Transfer:** The UCR contact will access the State of California's file transfer system **exclusively** from within the Secured Analysis Computer. The data will be downloaded directly to the encrypted storage volume on the Secured Analysis Computer.
4. **Data Isolation:** To maintain the security boundary, the data will **not** be downloaded, stored, or cached on any local workstations, laptops, or portable storage media (e.g., USB drives) during the transfer process.

5. **Verification:** Upon successful completion of the transfer, the PI will verify the integrity of the data on the Secured Analysis Computer.

Operational Use of Secured Analysis Computer

System Access * Access to the secured analysis computer (Linux Cloud Instance) is restricted to the Principal Investigator (PI) and approved researchers listed in this plan. * Researchers must connect via the UCR Campus VPN using Multi-Factor Authentication (MFA) before establishing a secure SSH connection to the instance.

Data Storage and Handling * All P4 sensitive infrastructure data provided by the State of California must be stored within the designated encrypted cloud storage volume on the secured analysis computer. * Secure files shall not be moved, copied, or backed up to any unauthorized external storage or cloud buckets.

Data Transfer Procedures * **Input:** Only statistical analysis scripts and approved configuration files intended for the "Sanitization Test" project will be transferred to the secured analysis computer using approved Secure Transfer methods (e.g., SFTP, SCP). * **Output:** Only the final sanitized output pipeline data—verified to be aggregated and de-identified—will be copied from the secured analysis computer for use in other applications.

Restrictions and Exceptions * No other data sets, applications, executables, documents, or files other than those noted above will be copied to or from the secured analysis computer. * Any operational need to remove un-aggregated, identifiable, or raw infrastructure data from the secured analysis computer must be approved in advance and in writing by the PI and the Unit Information Security Lead (UISL). * Use of the secured analysis computer for personal activities or purposes unrelated to this project is strictly prohibited.

Cyclical Security Review

- At least once annually, Service Provider personnel will perform maintenance on the secured analysis environment, consisting of the elements described in this section.
- The PI or other researcher should open a ticket for Research Computing to complete the cyclical security review.
- Service Provider personnel (including Systems Team, ISO, and other teams as needed) will use this plan to ensure all controls remain in place.

- Special note must be taken regarding the following controls:
    - Cloud Project IAM access (AWS/GCP).
    - Cloud storage bucket access permissions.
    - Cloud firewall policies and Security Groups.
    - Cloud logging settings (log router and log destinations).
    - Verify Linux system logs are being received in the central logging repository (e.g., Google Chronicle).
    - Verify logs are exported to the designated cloud storage bucket for retention.
    - Ensure all security updates are being applied at least monthly.
    - OS accounts (verify only appropriate researchers listed on this plan have accounts).
- The maintenance will be tracked in ServiceNow, including a completed checklist of all required actions.
- Any deviations from the configuration specified in this plan or anomalies identified in the logs will be reported to the PI and UISL who will determine any required remediation and escalate any suspected security incident or breach to the ISO.

Data Retention & Destruction

UC Requirement: When handling Institutional Information classified at Protection Level 3 or higher, Workforce Members may need to employ stronger methods of disposal at a more granular level to ensure that data is truly irretrievable. (Disposal of Institutional Information)

At the conclusion of the research period approved by the State of California, including any term extensions, or by the retention date of **2030-01-01**, the data will be securely deleted from the cloud environment (AWS/GCP).

- **Virtual Storage Sanitization:** Prior to the decommissioning of the cloud infrastructure, the storage on the secured Linux analysis instances will be fully erased using a secure deletion tool (e.g., `shred` or `scrub`) configured to meet the **DoD 5220.22-M (seven random overwrite passes)** standard.
- **Infrastructure Termination:** Following the secure overwrite process, the virtual machine instances and all associated storage volumes will be securely terminated and deleted from the cloud provider account.

- **Crypto-Shredding:** Any encryption keys used to decrypt the data or protect storage volumes will be securely deleted, rendering any potential residual raw data unrecoverable.
- **Verification:** The Principal Investigator (Chuck Forsyth) and Unit Information Security Lead (Kelton Adey) will verify and document the destruction of the data and keys.

Security Plan Review

- This plan will be reviewed at least annually by the Principal Investigator (PI) and Unit Information Security Lead (UISL) to verify continued compliance. Any risks identified will be added to the security plan following the process defined under Changes.
- During the review process, the PI will review the list of people with access to the data and ensure that access is revoked for any who no longer require access.

Violations of Data Security Plan

Any violations of the data security plan shall be reported immediately to the Principal Investigator (PI), Unit Information Security Lead (UISL), Unit IT Director, and Chief Information Security Officer (CISO).

Security Plan Changes

Any changes to the IT environment or policies used for processing the data will be documented; approved by the PI and UISL; and submitted to the ISO for review and approval before implementation.

Agreement & Signatures

The undersigned agree to abide by this security plan.

Any researchers who will be granted access to the data covered by this plan in the future will be required to read, agree, and sign this plan or an addendum to this plan.

Role	Name	Signature	Date
Principal Investigator	Chuck Forsyth		

Role	Name	Signature	Date
Unit Information Security Lead	Kelton Adey		
Chief Information Security Officer			