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 (https://policy.ucop.edu/doc/7000543/BFB-IS-3), UC Minimum Security Standard (https://security.ucop.edu/files/documents/policies/minimum-security-standard.pdf) 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.

Do local admissions guarantees at in-state publics reduce inequities in college-going for Black and Hispanic Students? Evidence from the California State University System

Data Security Plan

Research Project Name:	**Do local admissions guarantees at in-state publics reduce inequities in college-going for Black and Hispanic Students? Evidence from the California State University System**
External Party:	California Department of Education
Principal Investigator:	Veronica Sovero
Project Researcher(s):	
Unit:	College of Humanities, Arts, and Social Sciences (CHASS)
Department:	Department of Economics
Unit Information Security Lead (UISL):	Raymond Holguin
Unit Service Provider or IT Director:	James Lin
ISO Assessor:	Nick Christopher
CISO:	Dewight Kramer
Protection Level:	P4
Availability Level:	
Meets or Exceeds the Following Compliance Standards or Policies:	UC IS-3, UC Minimum Security Standard
Date Approved:	

Revision History

Date	By	Contact Information	Description

Table of Contents

Executive Summary

Public universities play a crucial role in providing access to higher education for historically underrepresented groups (Goodman et al., 2017). A prime example is the California State University (CSU) system, the largest public university system in the United States, serving over 450,000 students. Research has shown that these colleges are significant drivers of economic mobility (Chetty et al., 2020). The CSU local admissions priority guarantees admission to academically qualified students at their assigned local CSU campus, provided they complete the A-G subject area coursework. While in theory the local admissions priority was designed to provide guaranteed acceptance to academically qualified students, in practice many CSU campuses have experienced increased demand without a corresponding increase in capacity. When a particular campus declares program or campus impaction, CSU may establish additional admissions criteria. This project will investigate whether the CSU's local admissions priority, and its weakening through program impaction, has altered college enrollment patterns for underserved student populations.

All data for this project will be stored on a Windows 11 workstation. Controls listed in the plan focus on security of the local machine and remote access to it. No data will be stored in the cloud.

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 California Department of Education. 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 *Do local admissions guarantees at in-state publics reduce inequities in college-going for Black and Hispanic Students? Evidence from the California State University System* ("Project").
    - 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 CHASS: Staff member appointed by the Dean of CHASS with responsibility for information security.
    - 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.
- Chief Information Security Officer ("CISO"): responsible for security functions at UC Riverside
    - No access to data.
    - No access to the secured analysis computer.
    - Responsible for reviewing and approving this plan.
- UC Riverside Information Security Office ("ISO"): UC Riverside central information security office, under the direction of the Chief Information Security Officer.
    - No access to data.
    - No access to the secured analysis computer.
    - Responsible for reviewing this plan, including approval of any future changes prior to implementation.
- California Department of Education ("CDE"): Organization providing the data for the sole purpose of the investigation described in the data agreement
    - Originator of data.
    - No access to the secured analysis computer.

- Service Provider or IT Director for CHASS: IT service provider responsible for provisioning, configuring, and managing the IT infrastructure used for processing the data, under the direction of the UISL.
    - Note: Access described below will be limited to a subset of career CHASS IT staff members. No student employees will have access.
    - 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 secured 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**
• Units must ensure that access to Institutional Information follows the Need to Know and Least Privilege principles. • Access to networks and network services must follow the Least Privilege Principle. • Units must route network access to Institutional Information classified at Protection Level 4 through secure access control points. • Units must monitor network access to Institutional Information classified at Protection Level 3 or higher to detect unauthorized access. • Units must limit access to authorized users and prevent unauthorized access to Institutional Information and IT Resources. • Each Workforce Member and student must have a unique user account to distinguish that user from other users.	• Access to the secured analysis server/workstation will be permitted only via UCR Campus VPN (GlobalProtect), which is protected using multi-factor authentication. • User accounts will be provisioned only for project researchers. • Administrative accounts will be limited to IT staff, principal investigator, and lab managers. • Automatic screen locking after 15 minutes of inactivity will be enabled via GPO.
External Party Requirements	**Controls**
• [Same as above]	• [Same as above]

Encryption

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

UC Requirements (*BFB-IS-3 Section 10*)	**Controls**
• Units must encrypt Institutional Information classified at Protection Level 3 or higher when transmitted over a network. • Units must encrypt Institutional Information classified at Protection Level 3 or higher when stored on portable electronic media or portable computing devices. • Units must encrypt Institutional Information classified at Protection Level 4 when stored on any electronic media.	• The secured workstation will be encrypted using Microsoft BitLocker AES-256 encryption. • Data in transit will be secured by TLS 1.2 or newer, including remote access protocols. Unencrypted communications or access will not be used or permitted.
External Party Requirements	**Controls**
• Each party acknowledges that access to the CDE-supplied data and any study work containing PII shall be limited to the Principal Investigator and Study Project Staff who are identified in Attachment D and any other persons approved by the CDE in writing who have signed Attachment D. CDE-supplied data and study work containing PII will use TLS 1.2 encryption and FIPS 140-2 mode or FIPS 140-2 approved ciphers during transmission.	• This secured workstation will have FIPS-validated mode enabled. This ensures all required encryption will use the Windows FIPS 140-2 validated module.

Physical and Environmental Security

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

UC Requirements (*BFB-IS-3 Section 11*)	**Controls**
● Units must implement and review at least these elements of physical security: ○ Statutory, regulatory and contractual requirements. ○ Institutional Information Classification. ○ Area entry safeguards and controls protecting physical access to Institutional Information and IT Resources. ○ Plans for ensuring that Institutional Information classified at Protection Level 3 or higher is not left unsecured and/or where unauthorized individuals can access it. ○ Administrative and physical controls on third-party access and supervision. ● Units must ensure that physical access to secured areas is based on job responsibilities. ● Workforce Members must protect IT Resources from unauthorized access, loss, theft or damage. ● Units must ensure that Institutional Information classified at Protection Level 3 or higher is not taken or transmitted off-site unless authorized by the appropriate Workforce Manager or Institutional Information Proprietor. ● Units must ensure that Institutional Information classified at Protection Level 3 or higher is adequately protected both on- and off-site.	● The secured analysis computer will be physically located in the CHASS server room. ● The server room is locked with a physical key. Only the IT and other necessary staff have access to the office.
External Party Requirements	**Controls**
● Each Party acknowledges that CDE-supplied data is to be	● [Same as above]

securely stored in a locked repository identified as the physical location of the data in this Attachment.	

Protection from Malware and Intrusion

UC Requirements (*BFB-IS-3 12.2*)	**Controls**

• Units must ensure that any device connected to an authenticated or protected Location network complies with the UC Minimum Security Standard.
• Units must monitor IT Resources to detect signs of attack or compromise when any of the following are present:
  ○ Institutional Information classified at Protection Level 2 or higher.
  ○ IT Resources classified at Protection Level 3 or higher.
  ○ IT Resources classified at Availability Level 3 or higher.
	• Trellix HX is installed on the secured workstation. Trellix HX provides endpoint protection, detection, and response capabilities, including malware detection.

External Party Requirements	**Controls**
• Each party acknowledges that all computer systems (hardware and software applications) used to perform this Study shall be properly secured and maintained. This includes ensuring all security patches, upgrades, and anti-virus updates are applied as appropriate to the computer systems that are used to conduct this study.	• [Same as above]

Backup

UC Requirements (*BFB-IS-3 12.3*)	**Controls**
• Units must ensure that Institutional Information classified at Availability Level 3 or higher is backed up and recoverable. • Units must comply with UC Records Retention Schedule for retention of backups. • Units must protect backups according to the Protection Level of the Institutional Information they contain. • Units must ensure that portable backup media meet the portable media requirements outlined in the IS-3 policy. • Units must document and execute a plan to test restoration of Institutional Information from backups. • Units must maintain a backup catalog that shows the location of each backup and retention requirements.	• As all derivative analyses can be re-created from the original data, there is no need to backup data or applications stored on the secured analysis computer.
External Party Requirements	**Controls**
• [Insert external party requirement]	• [Insert applicable controls]

Logging and Auditing

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

UC Requirements (*BFB-IS-3 12.4*)	**Control**
• Units must comply with the UC Event Logging Standard for IT Resources when storing, processing or transmitting Institutional Information. • Units must obtain approval for erasing, purging or trimming event logs through the change management process.	• Windows Event Log will be configured to send audit logs to Google SecOps. Google SecOps is monitored by the UCR Security Operation Team.

• Units must protect logs according to the Protection Level of the Institutional Information they contain and may not release them without proper authorization.
• Units must retain logs according to external obligations as well as the requirements in the UC Records Retention Schedule, contracts, regulations, litigation holds or preservation orders.
• For Institutional Information classified at Protection Level 3 or higher, and IT Resources classified at Protection or Availability Level 4, Unit Information Security Leads must independently review privileged accounts periodically to ensure that:
  ○ Only authorized activity occurred.
  ○ Anomalies are analyzed and corrective actions are implemented.
• For Institutional Information classified at Protection Level 3 or higher, Units must limit access to administrative logs using the Need to Know Principle.	

External Party Requirements	**Controls**
• N/A	• N/A

Control of Operational Software

UC Requirements (*BFB-IS-3 12.5*)	**Controls**
• Units must obtain approval for software installation, configuration changes and updates on production systems through the Location change management process.	• In addition to Windows 11, associated system components, and system updates, only the applications listed in this section are permitted on the secured analysis computer.

	○ Stata ○ R ○ Dropbox ● All other applications and services will be disabled and, if possible, removed.
External Party Requirements	**Controls**
● N/A	● N/A

Vulnerability & Patch Management

UC Requirements (*BFB-IS-3 12.6*)	**Controls**
● Units must only use supported and patched versions of hardware and software.	● Qualys Cloud Agent will be installed for vulnerability management. ● All software will be configured to update automatically when patches are available. Automatic updates will be managed by GPO.
External Party Requirements	**Controls**
● Each party acknowledges that all computer systems (hardware and software applications) used to perform this Study shall be properly secured and maintained. This includes ensuring all security patches, upgrades, and anti-virus updates are applied as appropriate to the computer systems that are used to conduct this study.	● [Same as above]

Communications Security

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

UC Requirements (*BFB-IS-3 Section 13*)	**Controls**
● Units must place IT Resources processing Institutional Information classified at Protection Level 3 or higher on segmented networks restricted to IT Resources also classified at Protection Level 3 or higher. Units must protect the ingress and egress points via appropriate network security controls and/or intrusion detection/prevention tools/technologies approved by the CISO. ● Units must authenticate administrator access to IT Resources that process Institutional Information classified at Protection Level 3 or higher through a managed access control point. ● Units must turn off or disable unused ports, protocols and services for IT Resources processing Institutional Information classified at Protection Level 3 or higher. ● Units must ensure that IT Resources processing Institutional Information classified at Protection Level 3 or higher use secure versions of network services. ● Units must ensure that network devices used to control access to Institutional Information classified at Protection Level 4: ○ Use the most restrictive rules possible. ○ Allow only authorized connections. ○ Detect and log unauthorized access or access attempts.	● A network-based firewall will be implemented to restrict traffic to and from the secured analysis computer. ● Outbound access will be permitted by default. ● Unnecessary network services will be disabled. ● The UCR Information Security Office operates an intrusion detection system at the border of UCR's network. Alerts and suspicious activity are monitored by the Security Operations Team. ● Trellix HX is installed on the local secured workstation and provides additional intrusion detection capabilities ● Remote access to the machine will only be available via UCR Campus VPN.

○ Review the network access rules. ● Units must ensure that the transfer of Institutional Information classified at Protection Level 3 or higher between UC Locations, to Suppliers, or to external entities/organizations use appropriate security controls approved by the CISO and Institutional Information Proprietor.	
External Party Requirements	**Controls**
● N/A	● N/A

Transfer of Data from the California Department of Education to UC Riverside

1. Transfer of data from the California Department of Education will occur over the Internet directly to the secure analysis computer CDE's SFTP service or other service chosen by CDE.

Operational Use of Secured Analysis Computer

- The secured analysis computer will be used only for research purposes. Personal use of the computer is not permitted.
- Only project research members will have access to the computer.
- Any operational need to remove un-aggregated, identifiable data from the secured analysis computer must be approved in advance by the PI and UISL.

Cyclical Security Review

- At least annually, Service Provider and ISO personnel will perform a review of the secured system to ensure appropriate configurations according to this plan remain in place.

- 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 California Department of Education, including any term extensions to the original agreement approved by the California Department of Education, the data will be securely deleted from UC Riverside systems.
    - The storage on the secured analysis computer will be fully erased using a tool meeting the DOD 5220.22-M (seven random overwrite passes) standard.
    - Any encrypted USB flash drives (backup of original data; analysis script and aggregated data transfer) will be fully erased using a tool meeting the DOD 5220.22-M (seven random overwrite passes) standard.

Security Plan Review

- This plan will be reviewed at least annually by the PI and 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 PI, UISL, Unit IT Director and 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	Veronica Sovero	Signed by: Veronica Sovero 6538CD489CF841F...	6/16/2025 | 8:21 PM PDT
Unit IT Director	James Lin		
Unit Information Security Lead	Raymond Holguin	DocuSigned by: Raymond Holguin	6/19/2025 | 2:17 PM PDT
Chief Information Security Officer	Dewight Kramer	DocuSigned by: 60249849BAA64D2... CE77FA9503B743A...	6/17/2025 | 2:36 PM PDT