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.

UNIVERSITY OF CALIFORNIA
UC RIVERSIDE

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, California Department of Education Security Requirements, Committee for the Protection of Human Subjects Data Security Requirements

Date Approved:	

Revision History

Date	By	Contact Information	Description
Sept. 3, 2025	Nick Christopher	nickolas.christopher@ucr.edu	Added CPHS security requirements addendum

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**
• N/A	• N/A

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.

Addendum - CPHS Security Requirements

Note: These controls were retrieved on Sept. 3, 2025, from
https://www.chhs.ca.gov/wp-content/uploads/2022/03/Data-Security-Requirements-2012-04-20.pdf.

Administrative Safeguards

All persons with access to PID are trained on privacy and security, and sign a confidentiality agreement. All persons with access to PID are subject to a background check, or a thorough reference check.

Control Statement: UCR personnel complete security awareness training annually. All UCR employees undergo background checks prior to employment. The PI will sign a confidentiality statement with the California Department of Education.

Researcher has obtained and submitted a statement form [sic] a governmental agency indicating that the release of the desired data is legal and that the agency is willing to release the desired data to the researcher

Control Statement: This is the responsibility of the PI.

Researcher has committed that data will not be reused or provided to any unauthorized person or entity (unauthorized means that the person or entity does not have a need to access the data for purposes of the research project approved by CPHS).

Control Statement: This is the responsibility of the PI.

Researcher has committed that information will not be published that could possibly be used to identify an individual subject.

Control Statement: This is the responsibility of the PI.

Researcher has provided adequate justifications for the quantity of the data requested, the years and the variables.

Control Statement: This is the responsibility of the PI.

Researcher has requested no more than the minimum necessary data to perform the research.

Control Statement: This is the responsibility of the PI.

Access to data is limited only to those with a need to know for purposes of implementing or evaluating the research.

Control Statement: This is covered by existing access controls noted in this plan.

Researcher has justified why unique identifiers other than social security numbers cannot be used.
Control Statement: This is the responsibility of the PI.

Researcher has committed to ensuring that subjects will not be identifiable in any published articles.
Control Statement: This is the responsibility of the PI.

Researcher has described appropriate and sufficient methods to protect the identity of individual subjects when small cells or small numbers and/or data linkage to another data set are involved in the research project.
Control Statement: This is the responsibility of the PI.

If the data set is to be linked with any other data sets, the Researcher has identified all data sets and each of the variables to be linked, with justification for each linkage.
Control Statement: This is the responsibility of the PI.

If a third party is being used to perform data matching, Researcher has provided evidence of the third parties' ability to protect PID, including third parties' ability to comply with all the CPHS data security requirements.
Control Statement: This is the responsibility of the PI.

Researcher will provide CPHS with a letter certifying that PID has been destroyed and/or return the disc with PID to the data source once research is concluded.
Control Statement: This is the responsibility of the PI. The Unit IT Service Provider will assist with data destruction if required.

Chief Information Officer, Privacy Officer, or Security Officer or equivalent position of the researcher's institution will certify the CPHS Data Security Requirements are met.
Control Statement: A signed letter will be provided by UCR.

<u>Physical Safeguards</u>
Research records will be protected through the use of locked cabinets and locked rooms; PID in paper form will not be left unattended unless locked in a file cabinet, file room, desk, or office.
Control Statement: This is addressed by existing controls described in this plan.

Data will be destroyed or returned as soon as it is no longer needed for the research project.

Control Statement: This is addressed by existing controls described in this plan.

PID in paper form is disposed of through confidential means, such as cross cut shredding or pulverizing.

Control Statement: This is addressed by existing controls described in this plan.

Faxes with PID are not left unattended, and fax machines are in secure areas.

Control Statement: Faxes are not used in this project.

Mailings of PID are sealed and secured from inappropriate viewing; mailings of 500 or more individually identifiable records of PID in a single package, and all mailings of PID to vendors/contractors/co-researchers are sent using a tracked mailing method, which includes verification of delivery and receipt, such as UPS, U.S. Express Mail, or Federal Express, or by bonded courier.

Control Statement: Mailing of PID are not used in this project.

PID in paper or electronic form, e.g., stored on laptop computers and portable electronic storage media (e.g., USB drives and CDs), will never be left unattended in cars or other unsecured locations.

Control Statement: All PID will remain stored on the secured analysis computer. The secured analysis computer will remain in a locked server room.

Facilities which store PID in paper or electronic form have controlled access procedures, and 24 hour guard or monitored alarm service.

Control Statement: PID is stored on a secured analysis computer in a server room with controlled access. The server room has an alarm that will alert UC Police Department.

All servers containing unencrypted PID are housed in a secure room with controlled access procedures.

Control Statement: N/A - All data is encrypted.

Identifiers will be stored separately from analysis data.

Control Statement: The PI will separate student IDs from analysis data after the data cleaning process is complete.

All disks with PID will be destroyed

Control Statement: This is addressed by existing controls described in this plan.

Electronic Safeguards

Computer access will be protected through the use of encryption, passwords, and other protections, as follows:

- All workstations that contain PID have full disc encryption that uses FIPS 140-2 compliant software.
- All laptops that contain PID have full disc encryption that uses FIPS 140-2 compliant software.
- All PID on removable media devices (e.g. USB thumb drives, CD/DVD, smartphones, backup tapes) are encrypted with software which is FIPS 140-2 compliant.
- All workstations, laptops and other systems that process and/or store PID have security patches applied in a reasonable time frame.
- Sufficiently strong password controls are in place to protect PID stored on workstations, laptops, servers, and removable media.
- Sufficient system security controls are in place for automatic screen timeout, automated audit trails, intrusion detection, anti-virus, and periodic system security/log reviews.
- All transmissions of electronic PID outside the secure internal network (e.g., emails, website access, and file transfer) are encrypted using software which is compliant with FIPS 140-2.
- PID in electronic form will not be accessible to the internet.
- When disposing of electronic PID, sufficiently secure wiping, degaussing, or physical destruction is used.

Control Statement: All parts of the Electronic Safeguards are addressed by existing controls described in this plan.

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...	9/5/2025 | 10:02 AM PDT
Unit IT Director and Unit Information Security Lead	Raymond Holguin	DocuSigned by: Raymond Holguin [illegible]	9/5/2025 | 9:26 AM PDT
Chief Information Security Officer	Dewight Kramer	[illegible] CE77FA9503B743A...	9/18/2025 | 10:32 AM PDT

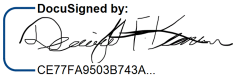
Certificate Of Completion

Envelope Id: 0E0360A0-D819-4D11-A2AA-5D4431A0D461
Status: Completed
Subject: Complete with Docusign: UCR Data Security Plan - Sovero Dept of Education.pdf
Source Envelope:
Document Pages: 22
Signatures: 3
Certificate Pages: 5
Initials: 0
AutoNav: Enabled
EnvelopeId Stamping: Enabled
Time Zone: (UTC-08:00) Pacific Time (US & Canada)

Envelope Originator:
Nickolas Christopher
100 Phoenix Dr.Suite 111
Lansing, MI 48108
nickolas.christopher@ucr.edu
IP Address: 70.167.110.242

Record Tracking

Status: Original
9/5/2025 9:06:37 AM
Holder: Nickolas Christopher
nickolas.christopher@ucr.edu
Location: DocuSign

Signer Events	Signature	Timestamp
Dewight Kramer dewight.kramer@ucr.edu CISO University of California, Riverside Security Level: Email, Account Authentication (None)	DocuSigned by:  CE77FA9503B743A... Signature Adoption: Drawn on Device Using IP Address: 104.48.80.214 Signed using mobile	Sent: 9/5/2025 9:11:55 AM Viewed: 9/18/2025 10:31:56 AM Signed: 9/18/2025 10:32:05 AM
Electronic Record and Signature Disclosure: Not Offered via Docusign		
Raymond Holguin raymond.holguin@ucr.edu Interim Chief Information Officer University of California, Riverside Security Level: Email, Account Authentication (None)	DocuSigned by:  60249849BAA64D2... Signature Adoption: Pre-selected Style Using IP Address: 99.106.102.11	Sent: 9/5/2025 9:11:56 AM Viewed: 9/5/2025 9:22:58 AM Signed: 9/5/2025 9:26:10 AM
Electronic Record and Signature Disclosure: Not Offered via Docusign		
Veronica Sovero vsovero@ucr.edu Security Level: Email, Account Authentication (None)	Signed by:  6538CD489CF841F... Signature Adoption: Pre-selected Style Using IP Address: 47.144.130.83	Sent: 9/5/2025 9:11:56 AM Viewed: 9/5/2025 10:02:36 AM Signed: 9/5/2025 10:02:54 AM
Electronic Record and Signature Disclosure: Accepted: 9/5/2025 10:02:36 AM ID: 681dc6f1-7383-4d50-ba1b-d821a0729009		

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp
Charles Forsyth charles.forsyth@ucr.edu Director of Research Computing University of California, Riverside Security Level: Email, Account Authentication (None)	COPIED	Sent: 9/18/2025 10:32:07 AM Viewed: 9/18/2025 10:33:41 AM

Electronic Record and Signature Disclosure:
Not Offered via Docusign

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	9/5/2025 9:11:56 AM
Certified Delivered	Security Checked	9/5/2025 10:02:36 AM
Signing Complete	Security Checked	9/5/2025 10:02:54 AM
Completed	Security Checked	9/18/2025 10:32:07 AM

Payment Events	Status	Timestamps

Electronic Record and Signature Disclosure

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, Internet2 OBO University of California, Riverside (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a $0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact Internet2 OBO University of California, Riverside:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:
To contact us by email send messages to: Shelley.Gupta@ucr.edu

To advise Internet2 OBO University of California, Riverside of your new email address

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at Shelley.Gupta@ucr.edu and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

To request paper copies from Internet2 OBO University of California, Riverside

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to Shelley.Gupta@ucr.edu and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with Internet2 OBO University of California, Riverside

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;

ii. send us an email to Shelley.Gupta@ucr.edu and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: https://support.docusign.com/guides/signer-guide-signing-system-requirements.

Acknowledging your access and consent to receive and sign documents electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

By selecting the check-box next to 'I agree to use electronic records and signatures', you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify Internet2 OBO University of California, Riverside as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by Internet2 OBO University of California, Riverside during the course of your relationship with Internet2 OBO University of California, Riverside.