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”) and the CISO.

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.

Each section contains either mandatory systemwide requirements or examples. Many of the mandatory systemwide requirements assume the data is classified at protection level 3.

Modify this plan as appropriate based on protection level, systemwide requirements and external party requirements.

If you have any questions regarding this form, contact infosecoffice@ucr.edu.

●

UC RIVERSIDE
UNIVERSITY OF CALIFORNIA

Evaluation of Prison to Employment Initiative
Data Security Plan

Research Project Name:	Evaluation of Prison to Employment Initiative
External Party:	CA Workforce Development Board / CA Economic Development Department
Lab Director:	Dr. Sharon Oselin, Director, Presley Center of Crime & Justice Studies
Project Researcher(s):	PIs/Drs. Sharon Oselin, Ozkan Eren, Matthew Mahutga
Unit:	School of Public Policy
Department:	Presley Center of Crime & Justice Studies
Unit IT Director or UISL:	Eddie Greer
Unit Service Provider or IT Director:	Eddie Greer
ISO Assessor:	Nick Christopher
CISO:	Dewight Kramer
Protection Level:	4
Availability Level:	2
Meets or Exceeds the Following Compliance Standards or Policies:	UC IS-3, UC Minimum Security Standard, Interagency Agreement No. M63330-7120 Exhibit E.
Date Approved:	

Revision History

Date	**By**	**Contact Information**	**Description**
05/12/2021	**Charles Forsyth**	**forsythc@ucr.edu**	**Review and Content Edits**
5/17/2021,5/25/2021	**Charles Forsyth**	**forsythc@ucr.edu**	**Edits and added additional appendix, FireEye install**

5/28/2021	**Charles Forsyth**	**forsythc@ucr.edu**	**Added Home Office information**

Table of Contents

Executive Summary

The Presley Center and PIs/Drs. Sharon Oselin, Ozkan Eren, and Matthew Mahutga will undertake a mixed methods evaluation of the State's Prison to Employment (P2E) Initiative. Material to this protocol, the research team will be provided a de-identified dataset, aggregated from the Economic Development Department's CalJOBS files and the California Workforce Development Board's supplemental data file. This data will be used to estimate the effect of participation in a P2E program on a variety of individual-level labor market outcomes and indicators, as well as the ex-offenders' likelihood of recidivating. The qualitative portion of this project will be conducted using original data collected by UCR researchers and does not make use of the data covered by this security plan.

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 Workforce Development Board (CWDB) / California Economic Development Department (EDD). 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 Evaluation of Prison to Employment Initiative.
    - Full access to the data on the secured analysis computer.
    - Full access to data on the secure storage.
    - 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 for the School of Public Policy (UISL): staff member appointed by the Dean of School of Public Policy with responsibility for information security.
    - Full access to data on the secured analysis computer.

  - Full access to data on the secure storage.
  - 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.
  - No access to the secure storage.
  - 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 CWDB/EDD.
- CWDB/EDD : CWDB/EDD is the agency providing the data for the sole purpose of the investigation described in Exhibit A (Scope of Work) and use as defined in Exhibit E (Special Conditions for Security of Confidential Information), Exhibit E-1 (EDD Confidentiality Agreement), Exhibit E-2 (EDD Indemnity Agreement), and Exhibit E-3 (Statement of Responsibility Information Security Certification) of the contract (Agreement Number: M63330-7120).
  - Originator of data.
  - No access to secured analysis computer.
- Service Provider or IT Director for School of Public Policy: 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 School of Public Policy IT staff members. No student employees will have access.
  - Full access to data on the secured analysis computer.
  - Full access to data on the secure storage.
  - 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 storage.
  - Full access to data on the secured analysis computer.
  - No administrative access to the secured analysis computer.

Configuration of Secured Laptops and Secure Storage

Physical Access

- The secured storage will be physically located in a secure room Sproul Hall.
- The secure analysis computers will be stored in PI Ozkan Eren's office, 4105 Sproul Hall, and PI Matthew Mahutga's office, 1226 Watkins Hall. Sproul Hall and Watkins Hall each

have one mechanical key that is required to enter the building. 4105 Sproul Hall and 1226 Watkins Hall each have a mechanical key that is required to enter the office.

- Mechanical keys to Sproul Hall and to Watkins Hall are provided to faculty, staff, and graduate students who require building access and UCR building officials. Only PI Ozkan Eren and UCR building officials have the mechanical key that unlocks the office at 4105 Sproul Hall. Only PI Matthew Mahutga and UCR building officials have the mechanical key that unlocks the office at 1226 Watkins Hall.
- The secure analysis computers will also be stored in PI Ozkan Eren's home office, and PI Matthew Mahutga's office when the PIs are not on campus. Each will be securely locked in their home offices. Physically secured via a lock on the office door or placed in a locked cabinet when not in use.
- Only the PIs will have access to their Home Offices.

Network Access Control

- The secured analysis computers will have a host-based firewall installed and configured to block all inbound traffic that is not explicitly required per this plan.
- Access to the secured storage will be permitted only via UCR Campus VPN (GlobalProtect), which is protected using multi-factor authentication.

Encryption

- The secured analysis computers will be configured with full-disk encryption using AES-128 or AES-256.
- The secured storage will be encrypted using AES-128 or AES-256.
- The secured analysis server will only be accessed via secure, encrypted communications protocols.
- Data in transit will be secured by TLS 1.2 or newer.

Access Management

- Default credentials shall be changed as soon as practical, preferably prior to being connected to the network.
- Local, non-administrative accounts will be created for each researcher on their secured analysis computer.
- Local, non-administrative accounts will be created for each researcher on the Secure Storage platform
- Only researchers who have signed this security plan will be granted accounts.
- All accounts will be configured with passwords meeting or exceeding the UC password strength standard (https://security.ucop.edu/files/documents/policies/account-and-authentication-management-standard.pdf).
- Researchers granted accounts will complete the EDD Confidentiality Agreement (Exhibit E-1 of Agreement Number: M63330-7120).
- Unit IT personnel will use a local administrator account with a randomly configured password stored in Active Directory. This password will be reset during periodic maintenance.

- A locally applied security policy will lock the computer after 15 minutes of no user activity. Re-authentication will be required to unlock the computer.

Logging and Auditing Configuration

- The secured storage will be configured to retain all possible logs for as long as possible to conform with Cyclical Security Review.
- Windows file system auditing (Audit System Access Control List) policies will be enabled via a local administrative policy on the secure analysis computers for directories containing the data covered by this security plan to ensure that all access to the data is logged, including specific files, access type, and account holder information.

Endpoint Protection

- Windows Defender will be installed and configured with the latest updates on the secure analysis computers.
- Windows Defender will be configured to log all malware, intrusion or other security incidents on the secure analysis computers.
- FireEye HX will be installed and configured with the latest updates to log all malware, intrusion or other security incidents on the secure analysis computers.

Approved Applications

- In addition to the Microsoft Windows operating system, associated system components, and system updates, only the applications listed in this section are permitted on the secured analysis computer.
    - Stata v.16.0 or higher
    - Microsoft Office
- All other applications and services will be disabled and, if possible, removed.

Transfer of Data from CWDB/EDD to UC Riverside

1. Before being transmitted to UC Riverside, CWDB/EDD will encrypt the data in ZIP format with AES-256 encryption.
2. The encryption passphrase shall be unique and be no less than 10 alphanumeric characters. It shall not include common words, phrases or any names.
3. The encrypted file will be stored in SharePoint and shared with the UISL.
4. The encryption key for the file will be transmitted to the UISL via telephone.
5. Once the encrypted file has been received by the UISL, it will be copied to an encrypted USB flash drive.
6. The UISL will transfer the encrypted file to the secured analysis computer, retaining the encrypted copy on the encrypted USB flash drive.
7. The UISL will decrypt the encrypted file on the secured analysis computer (which is itself encrypted).
8. The UISL will provide the encrypted USB flash drive to the PI as a backup of the original data, along with the drive (NOT the ZIP file) encryption key. The USB flash drive will be stored in a locked location (desk drawer in PI Ozkan Eren’s office), and the encryption

key for the USB drive will be stored in a separate locked location (desk drawer in PI Matthew Mahutga's office).

9. The UISL will escrow the encryption key for the ZIP file in a secure password management system. Should the ZIP file need to be decrypted in the future (e.g., in the case of a failure of the secured analysis computer), the PI may contact the UISL to perform the decryption.
10. PIs Ozkan Eren and Matthew Mahugta will confirm the successful data decryption on the secured analysis computers, after which the UISL will destroy the SharePoint copy.

Operational Use of Secured Analysis Computer

- An encrypted network share drive will be provisioned for project use, and only that drive will be used to move data to or from the secured analysis computer.
- The PI, approved researchers and the UISL will have access to the encryption key for the encrypted network share drive.
- Only aggregated, de-identified data will be copied from the encrypted network share drive to the secured analysis computer for use in other applications.
- No other data sets, applications, executables, documents, or other files than those noted above will be copied to or from the secured analysis 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 once every three months, Service Provider personnel will perform maintenance on the secured analysis computer, consisting of the elements described in this section.
- The maintenance will be tracked as an Incident record in the UC Riverside ITS Service Now instance, including a completed checklist of all required actions (see required actions below).
- 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.

Log Review

- All system, application and security logs collected since the previous maintenance window will be reviewed for anomalies and security issues during the cyclical maintenance of the device(s).
- The file system audit logs for the directories containing the data protected by this plan will be compared to verify that no accounts other than system accounts and accounts held by approved researchers have accessed the protected directories.

- Endpoint protection or antivirus logs will be reviewed to identify any malware threats or connection of unapproved peripherals.

Vulnerability & Patch Management

- The operating system, antivirus/antimalware application, and research applications resident on the secured analysis computers will be updated to the current patch levels available from the respective software vendors.
- Patching for medium to critical vulnerabilities and patches will be patched within 30 days, and all other vulnerabilities and patching will be implemented as needed.
- The currently installed set of applications will be compared against the list of approved applications detailed in Approved Applications.

Backup of Data

- 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.

Data Retention & Destruction

- At the conclusion of the research period approved by CWDB/EDD, including any term extensions to the original agreement approved by CWDB/EDD, the data will be securely deleted from UC Riverside systems.
    - The storage on the secured analysis computers 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.
    - The secure storage will be deleted via Cryptographic erasure processes.

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: Principal Investigator

Name: Sharon Oselin

Signature: DocuSigned by: Sharon Oselin 5DFF77EC2952464... Date: 5/28/2021 | 11:21 AM PDT

Role: Unit IT Director/UISL, [UNIT OR TITLE]

Name: Eddie Greer

Signature: DocuSigned by: C941981F8A4C4DD... Date: 5/28/2021 | 11:13 AM PDT

Role: Chief Information Security Officer

Name: Dewight F. Kramer

Signature: DocuSigned by: Dewight F. Kramer CE77FA9503B743A... Date: 6/2/2021 | 8:25 AM PDT

Appendix

Requirement to Control Mapping

UC IS-3	
Requirement	Control
Access Control (*BFB-IS-3 Section 9*) ● 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.	● Default credentials shall be changed as soon as practical, preferably prior to being connected to the network. ● Local, non-administrative accounts will be created for each researcher on their secured analysis computer. ● Local, non-administrative accounts will be created for each researcher on the Secure Storage platform ● Only researchers who have signed this security plan will be granted accounts. ● All accounts will be configured with passwords meeting or exceeding the UC password strength standard (https://security.ucop.edu/files/documents/policies/account-and-authentication-management-standard.pdf). ● Researchers granted accounts will complete the EDD Confidentiality Agreement (Exhibit E-1 of Agreement Number: M63330-7120). ● Unit IT personnel will use a local administrator account with a randomly configured password stored in Active Directory. This password will be reset during periodic maintenance. ● A locally applied security policy will lock the computer after 15 minutes of no user activity. Re-authentication will be required to unlock the computer. ● The secured analysis computers will have a host-based firewall installed and configured to block all inbound traffic that is not explicitly required per this plan.

	● Access to the secured storage will be permitted only via UCR Campus VPN (GlobalProtect), which is protected using multi-factor authentication.
Encryption (*BFB-IS-3 Section 10*) ● 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 analysis computers will be configured with full-disk encryption using AES-128 or AES-256. ● The secured storage will be encrypted using AES-128 or AES-256. ● The secured analysis server will only be accessed via secure, encrypted communications protocols. ● Data in transit will be secured by TLS 1.2 or newer.
Physical and Environmental Security (*BFB-IS-3 Section 11*) ● Units must implement and review at least these elements of physical security: o Statutory, regulatory and contractual requirements. o Institutional Information Classification. o Area entry safeguards and controls protecting physical access to Institutional Information and IT Resources. o 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. o 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	● Anti-virus protection is installed and configured on the secure workstation. ● FireEye HX endpoint threat protection is also installed on the secure workstation.

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.	
Logging and Auditing (*BFB-IS-3 Section 12*) ● 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. ● 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.	● The secured storage will be configured to retain all logs for as long as possible to conform with Cyclical Security Review. ● Windows file system auditing (Audit System Access Control List) policies will be enabled via a local administrative policy on the secure analysis computers for directories containing the data covered by this security plan to ensure that all access to the data is logged, including specific files, access type, and account holder information.

Protection from Malware and Intrusion (BFB-IS-3 12.2) ● 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: o Institutional Information classified at Protection Level 2 or higher. o IT Resources classified at Protection Level 3 or higher. o IT Resources classified at Availability Level 3 or higher.	● Anti-virus protection is installed and configured on the secure workstations. ● FireEye HX endpoint threat protection is also installed on the secure workstations.

Backup (BFB-IS-3 12.3) ● 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.	● A backup of the Original Secure Data will be kept on encrypted removable media and storage in a secure locked cabinet. ● As all derivative analyses can be re-created from the original data, there is no need to back up data or applications stored on the secured analysis computer.

Vulnerability & Patch Management (BFB-IS-3 12.6) ● Units must only use supported and patched versions of hardware and software.	● The secure workstations are central IT managed desktop environments that receive automatic regular vulnerability and patch management.

Interagency Agreement No. M63330-7120 Exhibit E.	
Requirement	Control
● Protect the EDD's and the CWDB's information against unauthorized access, at all times, in all forms of media. Access and use the information obtained under this Agreement only to the extent necessary to assist in the valid administrative needs of the program receiving such information, and only for the purposes defined in this Agreement. ● Extraction or use of the EDD and the CWDB information for any purpose outside the purposes stated in this Agreement is strictly prohibited. The information obtained under this Agreement shall not be reproduced, published, sold, or released in original or any other form not specifically authorized under this Agreement. ● Disclosure of any of the EDD and the CWDB information to any person or entity not specifically authorized in this Agreement is strictly prohibited. Personnel assigned to work with the EDD's and the CWDB's confidential information shall not reveal or divulge to any person or entity any of the confidential information provided under this Agreement except as authorized or required by law.	● Default credentials shall be changed as soon as practical, preferably prior to being connected to the network. ● Local, non-administrative accounts will be created for each researcher on their secured analysis computer. ● Local, non-administrative accounts will be created for each researcher on the Secure Storage platform ● Only researchers who have signed this security plan will be granted accounts. ● All accounts will be configured with passwords meeting or exceeding the UC password strength standard (https://security.ucop.edu/files/documents/policies/account-and-authentication-management-standard.pdf). ● Researchers granted accounts will complete the EDD Confidentiality Agreement (Exhibit E-1 of Agreement Number: M63330-7120). ● Unit IT personnel will use a local administrator account with a randomly configured password stored in Active Directory. This password will be reset during periodic maintenance. ● The secured analysis computers will have a host-based firewall installed and configured to block all inbound traffic that is not explicitly required per this plan.

	● Access to the secured storage will be permitted only via UCR Campus VPN (GlobalProtect), which is protected using multi-factor authentication.
● Take precautions to ensure that only authorized personnel are given access to physical, electronic and on-line files. Store electronic and hard copy information in a place physically secure from access by unauthorized persons. Process and store information in electronic format, such as magnetic tapes or discs, in such a way that unauthorized persons cannot retrieve the information by means of computer, remote terminal, or other means.	● Default credentials shall be changed as soon as practical, preferably prior to being connected to the network. ● Local, non-administrative accounts will be created for each researcher on their secured analysis computer. ● Local, non-administrative accounts will be created for each researcher on the Secure Storage platform ● Only researchers who have signed this security plan will be granted accounts. ● All accounts will be configured with passwords meeting or exceeding the UC password strength standard (https://security.ucop.edu/files/documents/policies/account-and-authentication-management-standard.pdf). ● Researchers granted accounts will complete the EDD Confidentiality Agreement (Exhibit E-1 of Agreement Number: M63330-7120). ● Unit IT personnel will use a local administrator account with a randomly configured password stored in Active Directory. This password will be reset during periodic maintenance. ● The secured analysis computers will have a host-based firewall installed and configured to block all inbound traffic that is not explicitly required per this plan. ● Access to the secured storage will be permitted only via UCR Campus VPN (GlobalProtect), which is protected using multi-factor authentication.
● Secure and maintain any computer systems (network, hardware, and software applications) that will be used in the performance of this	● The operating system, antivirus/antimalware application, and research applications resident on the secured analysis computers will be

Agreement. This includes ensuring that all security patches, upgrades, and anti-virus updates are applied as appropriate to secure data that may be used, transmitted, or stored on such systems in the performance of this Agreement.	updated to the current patch levels available from the respective software vendors. ● The currently installed set of applications will be compared against the list of approved applications detailed in Approved Applications.
● Store all the EDD’s and the CWDB’s confidential documents in a physically secure manner at all times to prevent unauthorized access.	● The secured storage will be physically located in a secure room Sproul Hall. ● The secure analysis computers will be stored in PI Ozkan Eren’s office, 4105 Sproul Hall, and PI Matthew Mahutga’s office, 1226 Watkins Hall. Sproul Hall and Watkins Hall each have one mechanical key that is required to enter the building. 4105 Sproul Hall and 1226 Watkins Hall each have a mechanical key that is required to enter the office. ● Mechanical keys to Sproul Hall and to Watkins Hall are provided to faculty, staff, and graduate students who require building access and UCR building officials. Only PI Ozkan Eren and UCR building officials have the mechanical key that unlocks the office at 4105 Sproul Hall. Only PI Matthew Mahutga and UCR building officials have the mechanical key that unlocks the office at 1226 Watkins Hall.
● Store the EDD’s and the CWDB’s confidential electronic records in a secure central computer facility. Where in-use on a shared computer system or any shared data storage system, ensure appropriate information security protections are in place. University shall ensure that appropriate security access controls, storage protections and use restrictions are in place to keep the confidential information in the	● The secured storage will be physically located in a secure room Sproul Hall. ● The secure analysis computers will be stored in PI Ozkan Eren’s office, 4105 Sproul Hall, and PI Matthew Mahutga’s office, 1226 Watkins Hall. Sproul Hall and Watkins Hall each have one mechanical key that is required to enter the building. 4105 Sproul Hall and 1226 Watkins Hall each have a mechanical key that is required to enter the office.

strictest confidence and shall make the information available to its own personnel on a "need-toknow" basis only.	● Mechanical keys to Sproul Hall and to Watkins Hall are provided to faculty, staff, and graduate students who require building access and UCR building officials. Only PI Ozkan Eren and UCR building officials have the mechanical key that unlocks the office at 4105 Sproul Hall. Only PI Matthew Mahutga and UCR building officials have the mechanical key that unlocks the office at 1226 Watkins Hall. ● The secured analysis computers will have a host-based firewall installed and configured to block all inbound traffic that is not explicitly required per this plan. ● Access to the secured storage will be permitted only via UCR Campus VPN (GlobalProtect), which is protected using multi-factor authentication.
● Store the EDD's and the CWDB's confidential data in encrypted format when recorded on removable electronic storage media, or on mobile computing devices such as a laptop computer.	● The secured analysis computers will be configured with full-disk encryption using AES-128 or AES-256. ● The secured storage will be encrypted using AES-128 or AES-256. ● The secured analysis server will only be accessed via secure, encrypted communications protocols. ● Data in transit will be secured by TLS 1.2 or newer.
● Maintain an audit trail and record data access of authorized users and authorization level of access granted to the EDD's and the CWDB's data, based on job function.	● The secured storage will be configured to retain all possible logs for as long as possible to conform with Cyclical Security Review. ● Windows file system auditing (Audit System Access Control List) policies will be enabled via a local administrative policy on the secure analysis computers for directories containing the data covered by this security plan to ensure that all access to the data is logged, including

	specific files, access type, and account holder information.
● Direct all personnel permitted to use the EDD's and the CWDB's data to avoid leaving the data displayed on their computer screens where unauthorized users may view it. Personnel should retrieve computer printouts as soon as they are generated so that the EDD's and the CWDB's data is not left unattended in printers where unauthorized personnel may access them.	● A locally applied security policy will lock the computer after 15 minutes of no user activity. Re-authentication will be required to unlock the computer.
● Dispose of confidential information obtained from the EDD and the CWDB, and any copies thereof made by the EDD and/or the CWDB, after the purpose for which the confidential information is disclosed is served. Disposal means return of the confidential information to the EDD and the CWDB or destruction of the information utilizing an approved method of confidential destruction, which includes electronic deletion (following Department of Defense specifications) shredding, burning, or certified or witnessed destruction.	● At the conclusion of the research period approved by CWDB/EDD, including any term extensions to the original agreement approved by CWDB/EDD, the data will be securely deleted from UC Riverside systems. ○ The storage on the secured analysis computers 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. ○ The secure storage will be deleted via Cryptographic erasure processes.