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.

Evaluation of Prison to Employment Initiative
Data Security Plan

Research Project Name:	Evaluation of Prison to Employment Initiative
External Party:	California Department of Corrections & Rehabilitation
Lab Director:	Dr. Sharon Oselin
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:	Mike Kennedy
Unit Service Provider or IT Director:	ITS Systems, ITS Research Computing
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, CDCR Data Sharing Agreement
Date Approved:	02/16/2024

Revision History

Date	By	Contact Information	Description

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 by the California Department of Corrections & Rehabilitation (CDCR). This data will be used to estimate the effect of participation in a P2E program on 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.

The PIs have an approved data security plan for data provided by a separate state agency (the California Workforce Development Board, CWDB) for this same project. Both the data provided by the CDCR and CWDB are required to complete the evaluation covered by Interagency Agreement No. M63330-7120 (XXXX).

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 Corrections & Rehabilitation (CDCR). 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 the Evaluation of the Prison to Employment Initiative.
    - 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 for ITS (UISL): ITS staff member 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.
- 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 the secured analysis computer.
    - Responsible for reviewing this plan, including approval of any future changes prior to implementation.
    - CISO is the responsible official for signing the data agreement with the CDCR.
- CDCR: The CDCR is the agency providing the data for the sole purpose of the investigation described in the data agreement. (Attachment 1: CDCR Data Sharing Agreement)
    - Originator of data.
    - No access to the secured analysis computer.
- Service Provider for the School of Public Policy (SPP): IT service provider responsible for provisioning, configuring, and managing the IT infrastructure used for processing the data, under the direction of the UISL.
    - Full access to data on the secured analysis computer.
    - Administrative access to the secured analysis computer.
    - Responsible for provisioning, deploying, and maintaining the IT environment for the secured analysis computer.

- Project Researcher (Researcher): a researcher attached to the research project who will have access to the raw data under the direction of the PI.
    - Full access to data on the secured analysis computer.
    - No administrative access to the secured analysis computer.

Configuration of Secured Computing and Storage

Access Control & Management

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 Control: • User access to the secured analysis server/workstation will be permitted only via UCR Campus VPN (GlobalProtect), which is protected using multi-factor authentication. • Administrative access is available through UCR Campus VPN and secured enterprise management systems and networks. • Local, non-administrative accounts will be created for each researcher on their secured analysis computer. • Only researchers who have signed this security plan will be granted accounts. • A group policy will be configured to enforce the UC password strength standard (https://security.ucop.edu/files/documents/policies/account-and-authentication-management-standard.pdf) • 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.
External Party Requirements	**Controls**

● Minimum Necessary. Only the minimum necessary amount of source data, including, but not limited to CDCR PHI, PI, and other confidential data required to perform necessary business functions may be copied, downloaded, or exported. ● Access Controls. The system providing access to any source data, including, but not limited to CDCR PHI, PI, and other confidential data must use role based access controls for all user authentications, enforcing the principle of least privilege. ● User IDs and Password Controls. All users must be issued a unique user name for accessing any source data, including, but not limited to CDCR PHI, PI, and other confidential data. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within 24 hours. Passwords are not to be shared. Passwords must be at least eight (8) characters long and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every ninety (90) calendar days, preferably every sixty (60) calendar days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard: ○ Upper case letters (A-Z) ○ Lower case letters (a-z) ○ Arabic numerals (0-9) ○ Non-alphanumeric characters (punctuation symbols) ● System Timeout. The system providing access to any source data, including, but not limited to CDCR PHI, PI, and other confidential data must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity. ● Warning Banners. All systems providing access to any source	● Researchers will regularly check to ensure only necessary data will be retained on the secured analysis computer. ● Authorized users will be prompted to change their default credentials at least every 90 days using Windows group policy. ● The secured analysis computers display a warning banner stating the data is confidential, systems are logged, and is accessible only by authorized users. Authorized users are directed to log off if they do not agree with these terms. ● Group policies will be applied:... [insert more here]

data, including, but not limited to CDCR PHI, PI, and other confidential data must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.	

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.	● GCP Compute Engine encrypts disks using AES-256 by default. Disk encryption will use Google-managed keys. ● Access to the secured analysis computer is permitted using RDP requiring TLS v1.2 or newer and AES-256. ● Access to RDP is permitted only over UCR Campus VPN. ● No data will be stored on portable media or devices.
External Party Requirements	**Controls**

• Server Security. Servers containing unencrypted source data, including, but not limited to CDCR PHI, PI, and other confidential data must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review. • Removable media devices. All electronic files that contain any source data, including, but not limited to CDCR PHI, PI, and other confidential data data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, CD/DVD, cellular devices, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128 bit or higher, such as AES. • Transmission encryption. All data transmissions of any source data, including, but not limited to CDCR PHI, PI, and other confidential data outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128 bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing PHI can be encrypted. This requirement pertains to any type of source data, including, but not limited to CDCR PHI, PI, and other confidential data in motion such as website access, file transfer, and E-Mail. • Workstation/Laptop encryption. All workstations and laptops that process and/or store any source data, including, but not limited to CDCR PHI, PI, and other confidential data must be encrypted using a FIPS 140-2 certified algorithm which is 128 bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the CDCR Information Security Office (ISO).	• Same as above.

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 located in a Google Cloud Platform datacenter in the US. Google is responsible for physical security. (https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate)
External Party Requirements	**Controls**

● Supervision of Data. No source data, including, but not limited to CDCR PHI, PI, and other confidential data in paper form shall be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. No source data, including, but not limited to CDCR PHI, PI, and other confidential data in paper form shall be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes. ● Escorting Visitors. Visitors to areas where any source data, including, but not limited to CDCR PHI, PI, and other confidential data are contained shall be escorted and all source data, including, but not limited to CDCR PHI, PI, and other confidential data shall be kept out of sight while visitors are in the area. ● Confidential Destruction. All source data, including, but not limited to CDCR PHI, PI, and other confidential data must be disposed of through confidential means, such as cross cut shredding and pulverizing.	● Note: The external party's physical and environment requirements pertain to the use of paper documents or physical data. Only digital data will be used for this project, so there are no additional controls required.

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.	● Windows Defender will be installed and configured with the latest updates. ● Windows Defender will be configured to send all malware, intrusion or other security events to Windows Event Log. ● FireEye HX will be installed and configured with the latest updates to log all malware intrusion or other security incidents. ● Qualys Cloud Agent will be installed to track software vulnerabilities.
External Party Requirements	**Controls**
● Antivirus software. All workstations, laptops and other systems that process and/or store any source data, including, but not limited to CDCR PHI, PI, and other confidential data must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily. ● Intrusion Detection. All systems involved in accessing, holding, transporting, and protecting any source data, including, but not limited to CDCR PHI, PI, and other confidential data that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.	● 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**
• No requirements provided by external party as pertains to backup	• Same as above.

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. ● 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 analysis computer will be configured to send Windows Event logs to Google Chronicle and to a Google Cloud Storage bucket. ● The secured analysis computer will be configured to retain operating system logs, including security, system and application logs, for at least six (6) months to conform with Cyclical Security Review.
External Party Requirements	**Controls**

• System Logging. The system must maintain an automated audit trail which can identify the user or system process which initiates a request for any source data, including, but not limited to CDCR PHI, PI, and other confidential data, or which alters any source data, including, but not limited to CDCR PHI, PI, and other confidential data. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If any source data, including, but not limited to CDCR PHI, PI, and other confidential data are stored in a database, database logging functionality must be enabled. Audit trail data must be archived for three (3) years after occurrence. • Log Reviews. All systems processing and/or storing any source data, including, but not limited to CDCR PHI, PI, and other confidential data must have a routine procedure in place to review system logs for unauthorized access.	• The secured analysis computer will be configured to audit logon events and object access • A folder will be designated for secured data. That folder will have access audit logging enabled. All secured data must remain in the designated folder. • Windows event logs will be exported to Google Chronicle and to a GCP storage bucket. • Logs exported to Google Chronicle will be retained for 1 year. • Logs exported to the GCP storage bucket will be retained for 3 years. • Logs processed by Chronicle are reviewed for alerts by the UCR Information Security Office Operations Team as part of daily operations.

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 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.
External Party Requirements	**Controls**
● No requirements provided by the external party as pertains to operational software.	● Same as above.

Vulnerability & Patch Management

UC Requirements (*BFB-IS-3 12.6*)	**Controls**
● Units must only use supported and patched versions of hardware and software.	● All Windows patches will be applied monthly using scheduled SCCM or GCP VM Manager Patch jobs. ● Researchers are additionally responsible for patching any installed applications used for research.
External Party Requirements	**Controls**
● Patch Management. All workstations, laptops, cellular devices, and other systems that process and/or store any	● Same as above.

source data, including, but not limited to CDCR PHI, PI, and other confidential data must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within thirty (30) calendar days of vendor release. Applications and systems that cannot be patched due to operational reasons must have compensatory controls implemented to minimize risk, where possible.	

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. ○ 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.	● GCP firewall policies will block all inbound traffic that is not explicitly required per this plan. ○ Inbound traffic allowed: RDP from Campus VPN, Administrative and system management sessions and access for ITS administrators ● Outbound traffic will be restricted to Qualys and Trellix cloud services, CDCR SFTP, UCR SCCM, Chronicle and other hosts as required for this project.
External Party Requirements	**Controls**

Additional Requirements

External Party Requirements	Controls
Employee Training. All non-California Department of Corrections and Rehabilitation (CDCR) workforce members who assist in the performance of functions or activities on behalf of the requester or CDCR, or access or disclose any source data, including, but not limited to CDCR protected health information (PHI), personal information (PI), and other confidential data must complete information privacy and security training, at least annually. Each workforce member who receives information privacy and security training must sign a certification document indicating the member's name and the date on which the training was successfully completed. These signed certification documents must be retained by the data requester for CDCR inspection for a period of six (6) years following expiration/termination of the specified Data Sharing Agreement (DSA).	● All UCR employees complete standard security awareness training annually. Completion of training is recorded in the awareness training record. Records are not physically signed, but are tied to the UCR employee's individual user account. Records are retained for at least 6 years. ● The PI shall ensure all personnel involved in handing CDCR data complete the annual security awareness training.
Employee Discipline. Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.	● Workforce members who violate UC IS-3 (Electronic Information Security) policy are subject to disciplinary sanctions.
Confidentiality Statement. All persons that will be working with any source data, including, but not limited to CDCR PHI, PI, and other confidential data must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to any source data, including, but not limited to CDCR PHI, PI, and other confidential data.	● This security plan serves as a confidentiality statement/acknowledgement.

The statement must be renewed annually. The data requester shall retain each workforce member's written confidentiality statement for CDCR inspection for a period of six (6) years following expiration/termination of the specified DSA.	
Background Check. Before a workforce member may access any source data, including, but not limited to CDCR PHI, PI, and other confidential data, the workforce member shall undergo, at no cost to CDCR, a state and federal fingerprint-based background check conducted by the Department of Justice (DOJ). A criminal history that warrants substantial concerns on the part of CDCR, as a result of either the initial DOJ background check or any subsequent criminal record review, shall exclude the workforce member from access to any source data, including, but not limited to CDCR PHI, PI, and other confidential data.	• This has been completed in advance. Any new researchers will undergo background checks.
System Security Review. The data requester must ensure audit control mechanisms that record and examine system activity are in place. All systems processing and/or storing any source data, including, but not limited to CDCR PHI, PI, and other confidential data must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.	• The PI and/or UISL will request the Information Security Office perform a security assessment of the security analysis computer once annually. This is described in the Cyclical Security Review below.

Transfer of Data from the CDCR to UC Riverside

1. CDCR will provide the appropriate UCR contact access and credentials for the CDCR file transfer server.
2. The UCR contact will access the CDCR file transfer server using the secured analysis computer.

3. CDCR files will be transferred directly from CDCR file transfer server to the UCR secured analysis computer and placed in the designated folder.
4. CDCR secure files will not be retained or transferred anywhere outside of the secure analysis computer.

Operational Use of Secured Analysis Computer

- Researchers must use UCR Campus VPN to access the secured analysis computer. Once connected to Campus VPN, researchers may use Remote Desktop to access the secured analysis computer.
- CDCR secure files will be stored in C:\Secured Data on the secured analysis server.
- Secure files shall not be moved or copied to any other folder or system.
- Derivatives or copies of secure files used for analysis may be stored in subfolders of C:\Secured Data.

Unacceptable Use of Secured Analysis Computer

The secured analysis computer will only be used for activities directly related to this project. Use of the secured analysis computer for any purpose other than conducting research for or activities in support of this project is prohibited.

Cyclical Security Review

- At least once annually, Service Provider personnel will perform maintenance on the secured analysis computer, consisting of the elements described in this section.
- The PI or other researcher should open a BearHelp request for ITS to complete the cyclical security review.
- Service Provider personnel (including Systems Team, ISO and other teams as needed) will use this plan to ensure all controls remain in place.
    - Special note must be taken to the following controls:
        - GCP Project IAM access
        - GCP storage bucket access
        - GCP firewall policies
        - GCP logging settings (log router and log destinations)
        - Verify Windows event logs are being received in Chronicle.
        - Verify Windows event logs are exported to the designed cloud storage bucket.
        - Ensure all security updates are being applied at least monthly.
        - OS accounts (only appropriate researchers on this plan have accounts)
- The maintenance will be tracked in ServiceNow, including a completed checklist of all required actions.

- Any deviations from the configuration specified in this plan or anomalies identified in the logs will be reported to the PI and UISL who will determine any required remediation and escalate any suspected security incident or breach to the ISO.

Data Retention & Destruction

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

- At the conclusion of the research period approved by the CDCR, including any term extensions to the original agreement approved by the CDCR, the secure data will be securely deleted from UC Riverside systems.
    - The GCP Compute Engine virtual machine and storage disk will be deleted.
    - Per GCP standards, data is deleted from GCP's active systems around 2 months from user deletion. After about 6 months, all backups expire and are overwritten.
- In the event the data sharing agreement between the UCR Presley Center and CDCR is terminated prior to the agreement's natural expiration, the data will be securely deleted from UC Riverside systems.
    - The GCP Compute Engine virtual machine and storage disk will be deleted.
    - Per GCP standards, data is deleted from GCP's active systems around 2 months from user deletion. After about 6 months, all backups expire and are overwritten.
- File access audit logs will be retained for 3 years from the conclusion of the research period. These logs will be retained in a GCP cloud storage bucket. After the retention period has expired, the storage bucket will be deleted.

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.

- The CDCR will be notified by the USIL of any breach or compromise of the security, confidentiality, or integrity of the computerized data where personally identifiable information of a CDCR employee or parolee is or is reasonably believed to have been acquired and/or accessed by an unauthorized person. The USIL will notify the CDCR within 24 hours of learning of the occurrence and comply with all notification actions as required by State policy.

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.

Name	Role	Signature	Date
Sharon Oselin	Principal Investigator	DocuSigned by: Sharon Oselin 0A25A3A48D0B428...	3/15/2024 | 2:31 PM PDT
Mike Kennedy	Unit Information Security Lead	DocuSigned by: DE1263DC29A2431...	3/21/2024 | 3:19 PM PDT
Matthew Mahutga	Researcher	DocuSigned by: Matthew Mahutga A0BD7DA71D264AC...	3/18/2024 | 8:15 AM PDT
Ozkan Eren	Researcher	DocuSigned by: Ozkan Eren 6F8CF56310BD4AE...	3/21/2024 | 11:08 AM PDT
Manjing Gao	Researcher	DocuSigned by: Manjing Gao C82E69494F324F4...	3/15/2024 | 2:47 PM PDT