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.

UC RIVERSIDE
UNIVERSITY OF CALIFORNIA

White Identity and Violence
Data Security Plan

Research Project Name:	White Identity and Violence
External Party:	
Lab Director:	Sean Long
Project Researcher(s):	Sean Long
Unit:	CHASS
Department:	Political Science
Unit IT Director or UISL:	James Lin
Unit Service Provider or IT Director:	James Lin
ISO Assessor:	Nick Christopher
CISO:	Dewight Kramer
Protection Level:	
Availability Level:	
Meets or Exceeds the Following Compliance Standards or Policies:	UC IS-3, UC Minimum Security Standard
Date Approved:	

Revision History

Date	By	Contact Information	Description

Table of Contents

Executive Summary

This data concerns interviews conducted either online or over the phone as well as notes and screen grabs as part of field work conducted on online forums and communities.

All interviews will be conducted on a dedicated computer. This laptop will be used for nothing beyond the project under IRB review. The laptop currently runs Windows 10 and will be completely reformatted with Windows 10 reinstalled afterwards. I will then use a full-disc encryption in order to protect the laptop's internal hard-drive. A copy of Windows Defender will be installed, in addition to the following programs: Signal, Wire, OpenOffice, Tor, Proton VPN, and Firefox. Tor will be the main software used and will connect me to the websites in question.

Fieldwork notes will either be copied from websites or written into Open Office, or they will be screenshots using the Windows Snipping Tool. These notes will be stored on an external hard drive. This hard drive will also be encrypted and password-protected, and it will be kept offline while not actively in use. All notes will use pseudonyms if discussing a persistent individual that I interact with while relying on a protected text file that translates those pseudonyms into user names.

Purpose

The purpose of this data security plan ("Plan") is to document the security measures and policies for handling data gathered by the Principal Investigator ("PI") during the course of his dissertation research. 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 [White Identity and Violence].
    - 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 [UNIT] (UISL): staff member appointed by the Dean of [UNIT] with responsibility for information security.
    - No access to data on the secured analysis computer.
    - No Administrative access to the secured analysis computer.
    - No Unit IT personnel has administrative access to the secured analysis computer and data.
    - Shared responsibility with PI for ensuring ongoing compliance with all elements of this plan.
- UC Riverside Information Security Office (ISO): UC Riverside central information security office, under the direction of the Chief Information Security Officer (CISO).
    - No access to data.
    - No access to secured analysis computer.
    - Responsible for reviewing this plan, including approval of any future changes prior to implementation.
- 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.

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.	● The workstation will only be accessible by the primary researcher.

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 analysis computer will be configured with full-disk encryption using AES-128 or AES-256. ● Data in transit will be secured by TLS 1.2 or newer.

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	● The secured analysis computer will be physically located in the researcher's home address. ● The only individuals with physical access are the researcher and his wife. ● Only the researcher's wife will have physical access, although between sessions data will be stored in a safe which only the researcher will have access to.

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.	

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 log all malware, intrusion or other security incidents.

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.	- All data will be stored on a separate hard drive from the secured analysis computer in order to maintain its physical security, but this data will not be backed up elsewhere.

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.	- The secured analysis computer will be configured to retain logs are per default system settings. -

● 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.	

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 Windows operating system, associated system components, and system updates, only the applications listed in this section are permitted on the secured analysis computer. ○ Signal ○ Wire ○ OpenOffice ○ Tor

	○ Proton VPN ○ Firefox ○ Windows Defender ● All other applications and services will be disabled and, if possible, removed.

Vulnerability & Patch Management

UC Requirements (*BFB-IS-3 12.6*)	Controls
● Units must only use supported and patched versions of hardware and software.	● The operating system, antivirus/antimalware application, and research applications resident on the secured analysis computer will be 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.

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	● The secured analysis computer will have a host-based firewall installed and configured to block all inbound traffic that is not explicitly required per this plan.

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.	● The secured analysis computer will not have outbound network access.

Transfer of Data from [EXTERNAL PARTY] to UC Riverside

N/A

Operational Use of Secured Analysis Computer

- Preparation of secured analysis computer
    - An existing laptop owned by the researcher will be reformatted fully then encrypted.
    - Then, after first installing a VPN, the computer will, with the VPN activated, download approved software.
    - This computer will then serve as a dedicated machine for no other purposes.
- Data security and access
    - An encrypted external hard drive will be provisioned for project use, and only that drive will be used to store data collected with the secured analysis computer.
    - Only the PI will have access to the encryption key for the encrypted external hard drive.
    - Only de-identified data will be copied from the hard drive to other sources for analysis.
    - No other data sets, applications, executables, documents, or other files than those noted above will be copied to or from the secured analysis computer.
    - The secured analysis computer will be password protected, while the hard drive will be physically secured in a safe.
- Research session guidelines
    - When being used for analysis, the computer will be periodically subjected to DNS leak tests and, when using Tor, Tor checks. These will be regularly completed upon starting up the computer and periodically throughout the research session.
    - Upon completing a research session all applications will be closed before disconnecting from Tor.

Cyclical Security Review

- At least once every three months, Service Provider personnel will have a phone conversation with the PI to discuss the use of the computer and ensure the plan is being followed.
-

-

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*)

- The storage on the secured analysis computer and hard drive will be fully erased using a tool meeting the DOD 5220.22-M (seven random overwrite passes) standard upon full completion of the research project

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: Sean Long

Signature: Date: 2/2/2022

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

Name: ___________James Lin__________________

James Lin

Signature:________________________ Date: _________2/9/22____________