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.

SOMR BSL3 Lab
Data Security Plan

Research Project Name:	BSL3 Lab
External Party:	N/A
Lab Director:	Tran Phan, Tiffany Kwok (Associate Lab Director)
Project Researcher(s):	Rong Hai, Juliet Morrison, Marcus Kaul, Harrison Dulin, James Stumpf, Paula Da Silva Frost, Ricky Maung, Nina Yuan, Hina Singh, Deepika Bhullar, Rohan Shah, Daniel Ojeda, Erika Hay, Arrmund Neal, and Duo Xu
Unit:	SOMR BSL3 Lab
Department:	Environmental Health and Safety
Unit IT Director or UISL:	Charles Forsyth
Unit Service Provider or IT Director:	UCR ITS
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, Information Systems Security Control Guidance
Date Approved:	2/8/2021

Revision History

Date	**By**	**Contact Information**	**Description**
10/12/20	**Charles Forsyth**	**forsythc@ucr.edu**	**Document Creation**
10/21/20	**Charles Forsyth**	**forsythc@ucr.edu**	**Edits**
10/22/20	**Charles Forsyth**	**forsythc@ucr.edu**	**Adding VLAN details**
01/06/21	**Charles Forsyth**	**forsythc@ucr.edu**	**Editing researcher, director lists**
01/26/21	**Charles Forsyth**	**forsythc@ucr.edu**	**Added appendix, formatting edits**

Table of Contents

Instructions **0**

Executive Summary **3**

Purpose **3**

Stakeholders, Roles, and Responsibilities **3**

Configuration of Secured Workstation and Google Drive **4**

- Physical Access 4
- Network Access Control 4
- Encryption 5
- Access Management 5
- Logging and Auditing Configuration 5
- Endpoint Protection 5
- Vulnerability & Patch Management 5

Operational Use of Secured Workstation **5**

Operational Use of Secure Google Drive **6**

Cyclical Security Review **6**

Backup of Secure Data **6**

Data Retention & Destruction **6**

Security Plan Review **7**

Violations of Data Security Plan **7**

Security Plan Changes **7**

Agreement & Signatures **7**

Appendix **10**

- Requirement to Control Mapping 10

Executive Summary

The SOMR BSL3 Lab researchers will generate data and inventory records related to “Select Agents” on a secure workstation on a ACLs controlled private VLAN located within a secure BSL3 facility. The data itself is stored on a secure google drive which is connected via encrypted communication with the secure workstation. Google Drive Stream is the application that connects the secure workstation and the google drive and uses TLS for encrypted transport.

The secure google drive folder permissions will be configured to deny access to ALL accept specifically named authorized personnel. The specifically named authorized BSL3 lab personnel can access and analyze the generated BSL3 data with their desktops/laptops only via a web browser and encrypted TLS communication. Researchers with remote access to the data need to ensure their desktops/laptops are physically secure, regularly updated, password protected and have updated and functioning antivirus/antimalware if and before it contains BSL3 secure information of any kind. This practice includes researcher desktops/laptops in offices outside the BSL3 registered space. Portable storage devices such as removable hard drives or thumb drives will NOT be used for downloading or storing data.

The BSL3 data will NOT be shared with any other institution or any investigator not explicitly authorized. This restriction applies to source data as well as all derived data files. Any changes in access to the data require explicit approval by the Lab Director.

Purpose

The purpose of this data security plan (“Plan”) is to document the security measures and policies for handling data generated by the BSL3 Lab run by the Lab Director. When this agreement is executed, all members of the BSL3 Lab and 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 BSL3 Lab inventory records, BSL3 generated research data, any copies of the generated research 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.

- Lab Director: lead researcher SOMR BSL3 Lab
  - Full access to the data on the secured workstation.
  - Full access to the data stored on the secure Google Drive.
  - No administrative access to the secured workstation.
  - Responsible for supervising all research conducted using the data.
  - Responsible for ensuring ongoing compliance with all elements of this plan.
  - Responsible for securely configuring Google Drive.
- Unit Information Security Lead for BSL3 Lab (UISL): staff member with responsibility for information security.
  - No access to data stored on the secure Google Drive.
  - No access to the secured workstation.
  - Assists Lab Director with 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 workstation.
  - Responsible for reviewing this plan, including approval of any future changes prior to implementation.
- Service Provider or IT Director for BSL3: IT service provider responsible for provisioning, configuring, and managing the IT infrastructure used for processing the data, under the direction of the UISL.
  - Administrative access to the secured workstation.
  - Responsible for provisioning, deploying, and maintaining the IT environment for the secured workstation and network infrastructure.
- Project Researchers (Researchers): researchers attached to the BSL3 Lab who will have controlled access to the secure data under the direction of the Lab Director.
  - Limited and specific access to select data on secure Google Drive.
  - No administrative access to the secured workstation.
  - Shared responsibility with the Lab Director for ensuring ongoing compliance with all elements of this plan.

Configuration of Secured Workstation and Google Drive

Physical Access

- The secured workstation will be physically located in the secure BSL3 Lab on the UCR campus.
- The BSL3 Lab is locked with a biometric access system at all times.
- Only personnel authorized by the BSL3 Lab Director have access to the facility.
- There will be no physical access to Google Drive.

Network Access Control

- The secured workstation is behind the UCR Internet border firewall.
- The secured workstation is on an ACL controlled and isolated VLAN.

- All inbound connections from outside UCR are blocked. Inbound support and maintenance protocols are allowed only from the Campus Global Protect Admin VPN network. These connections are exclusively for support, patching and OS updates. All other inbound ports and protocols are blocked.
- There is no restriction on outbound connectivity via the VLAN.

Encryption

- Data stored at rest in Google Drive will be secured with AES256 encryption.
- Data in transit with Google Drive will be secured by TLS 1.2 or newer.
- Data stored on the secured workstation will be encrypted using full disk encryption using AES-128 encryption.

Access Management

- Non-administrative domain accounts will be created for each currently authorized researcher and the BSL3 Lab Directors on the secured workstation.
- Access by specifically named researcher to the secured Google Drive from an off-campus desktop or laptop will require MFA and domain passwords meeting or exceeding the UC password strength standard (https://security.ucop.edu/files/documents/policies/account-and-authentication-management-standard.pdf).
- A locally applied security policy will lock the screen of the secure workstation that accesses the secure analysis computer after 15 minutes of no user activity. Re-authentication will be required to unlock the workstation. The authorized workstation user is responsible for locking the secure workstation when not actively using the workstation.

Logging and Auditing Configuration

- The secured workstation will be configured to store domain account access and management logs centrally and are available for investigation.
- Domain account and management logs will be retained for at least 12 months.

Endpoint Protection

- Anti-virus protection is installed and configured on the secure workstation.
- FireEye HX endpoint threat protection is also installed on the secure workstation.

Vulnerability & Patch Management

- The BSL3 Lab secure workstation is a central IT managed desktop environment that receives automatic regular vulnerability and patch management.
- The BSL3 Lab secure workstation will have Qualys Cloud Agent installed to facilitate proactive UCR Information Security Office authenticated vulnerability scans.
- The Lab Director and authorized researchers will be responsible for ensuring the operating system, antivirus/antimalware, and other applications on desktop/laptops that will be used to access the secure Google Drive up to date.

Operational Use of Secured Workstation

- BSL3 Lab inventory and research data will be generated on the secure workstation and stored on Google Drive.

- Only the Lab Director and authorized researchers will have password protected access to the BSL3 Lab secure workstation.
- The authorized workstation users are responsible for locking the secure workstation when not actively using the workstation.

Operational Use of Secure Google Drive

- BSL3 Lab inventory and research data will be generated on the secure workstation and stored on Google Drive via the Google File Stream application.
- The secure Google Drive will be the central repository of the BSL3 Lab inventory and research data.
- Only the Lab Director and authorized researchers will have access to the secure Google Drive.
- The specifically named authorized BSL3 lab personnel can access and analyze the generated BSL3 Lab data with their desktops/laptops only via a web browser and encrypted TLS communication.

Cyclical Security Review

- The logs from the secured workstation, consisting of the elements described in the Logging and Auditing Configuration section above are available for review upon request or investigation.
- The Lab Director will review the secure Google Drive folder and file permissions monthly to ensure only authorized researchers have access to the data.
- Any deviations from the configuration specified in this plan or anomalies identified in the logs will be reported to the Lab Director and UISL who will determine any required remediation and escalate any suspected security incident or breach to the ISO.

Backup of Secure Data

- The secured Google Drive used to store the BSL3 Lab Data utilizes Google’s extremely resilient storage infrastructure internally keeping multiple secure copies and providing 99.978% availability.
- In backup and recovery terms Google Drive has an RPO (Recovery Point Objective) target of zero, and a RTO (Recovery Time Objective) target is instant failover (or zero).
- Deleted files on Google Drive are stored in a Trash folder for 30 days.
- Google Drive has versioning which allows for recovery of corrupted files.
- The secure workstation’s base image is stored by central IT and available to be used to restore the secure workstation when needed.

Data Retention & Destruction

- The Lab Director will be responsible for BSL3 Lab inventory and research data retention and destruction as appropriate for their research.

Security Plan Review

- This plan will be reviewed at least annually by the Lab Director and UISL to verify continued compliance. Any risks identified will be added to the security plan following the process defined under Security Plan Changes.
- During the review process, the Lab Director will review the list of people with access and will ensure that access is revoked for any researcher who no longer requires access and also ensure access is granted to those now requiring access with accomplining signature.

Violations of Data Security Plan

Any violations of the data security plan shall be reported immediately to the Lab Director, 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 Lab Director and UISL; and submitted to the ISO for review and approval before implementation.

Any changes to the list of researchers with access to the BSL3 Lab Data will be reflected in this document as soon as the change is made. This includes the addition of the researcher to this document accompanied by their signature.

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.

Tran Phan, Lab Director — Date

DocuSigned by:
Tran Phan
ACF8A08102F24E2...
2/8/2021 | 4:57 PM PST

Tiffany Kwok, Associate Lab Director — Date

DocuSigned by:
Tiffany Kwok
45AD475A36354DD...
2/17/2021 | 4:20 PM PST

Charles Forsyth, Associate Director of Research Computing — Date

DocuSigned by:
Charles Forsyth
4C912C27FAE844D...
2/8/2021 | 2:27 PM PST

Dewight Kramer, CISO — Date

DocuSigned by:
Dewight F. Kramer
CE77FA9503B743A...
2/8/2021 | 3:19 PM PST

Rong Hai, Researcher — Date

DocuSigned by:
Rong Hai
DC9D281D6A98429...
2/8/2021 | 2:40 PM PST

Juliet Morrison, Researcher — Date

DocuSigned by:
Juliet Morrison
9CC3400C417E487...
2/9/2021 | 3:14 PM PST

Marcus Kaul, Researcher — Date

DocuSigned by:
Marcus Kaul
54B35F55727E469...
2/10/2021 | 10:49 AM PST

Harrison Dulin, Researcher — Date

DocuSigned by:
3130A565945045E...
2/8/2021 | 4:48 PM PST

James Stumpf, Researcher — Date

DocuSigned by:
James Stumpff
93D345829B59476...
2/11/2021 | 9:07 AM PST

Paula Da Silva Frost, Researcher — Date

DocuSigned by:
Paula da Silva Frost
4817A051C0AF4A2...
2/8/2021 | 2:34 PM PST

Ricky Maung, Researcher — Date

DocuSigned by:
Ricky Maung
5A5B60FC712F492...
2/18/2021 | 8:41 AM PST

Nina Yuan, Researcher — Date

DocuSigned by:
Nina Yuan
12EE86446C9E4F7...
2/12/2021 | 4:20 PM PST

Hina Singh, Researcher — Date

DocuSigned by:
Hina Singh
CA66AACBAC154C3...
2/13/2021 | 6:20 PM PST

Deepika Bhullar, Researcher — Date

DocuSigned by:
Deepika Bhullar
DE4845678D954BA...
2/8/2021 | 2:50 PM PST

Rohan Shah, Researcher — Date

____

Daniel Ojeda, Researcher Date

DocuSigned by:
Daniel Ojeda
DC1BF1A26C80420... 2/14/2021 | 10:02 PM PST

____

Erika Hay, Researcher Date

DocuSigned by:
Erika Hay
C55772E57E2E405... 2/8/2021 | 3:47 PM PST

____

Arrmund Neal, Researcher Date

DocuSigned by:
Arrmund Neal
70FFEE50C7CE4E9... 2/8/2021 | 2:58 PM PST

____

Duo Xu, Researcher Date

DocuSigned by:
Duo Xu
BAA6E0D4242D446... 2/8/2021 | 2:30 下午 PST

____

Appendix

Requirement to Control Mapping

Information Systems Security Control Guidance	
Requirement	Control
Network Security – Section 11(c)(9)(i)	● The secured workstation is behind the UCR Internet border firewall. ● The secured workstation is on an ACL controlled and isolated VLAN. ● All inbound connections from outside UCR are blocked. Inbound support and maintenance protocols are allowed only from the Campus Global Protect Admin VPN network. These connections are exclusively for support, patching and OS updates. All other inbound ports and protocols are blocked. ● There is no restriction on outbound connectivity via the VLAN.
Access Authentication – Section 11(c)(9)(ii)	● Only the Lab Director and authorized researchers will have password protected access to the BSL3 Lab secure workstation. ● Access by specifically named researchers to the secured Google Drive from an off-campus desktop or laptop will require MFA and domain passwords meeting or exceeding the UC password strength standard (https://security.ucop.edu/files/documents/policies/account-and-authentication-management-standard.pdf).
Application Systems Security Controls – Section 11(c)(9)(iii)	● Anti-virus protection is installed and configured on the secure workstation. ● FireEye HX endpoint threat protection is also installed on the secure workstation.

Patching – Section 11(c)(9)(iv)	● The BSL3 Lab secure workstation is a central IT managed desktop environment that receives automatic regular vulnerability and patch management.
Backups – Section 11(c)(9)(v)	● The secured Google Drive used to store the BSL3 Lab Data utilizes Google's extremely resilient storage infrastructure internally keeping multiple secure copies and providing 99.978% availability. ● In backup and recovery terms Google Drive has an RPO (Recovery Point Objective) target of zero, and a RTO (Recovery Time Objective) target is instant failover (or zero). ● Deleted files on Google Drive are stored in a Trash folder for 30 days. ● Google Drive has versioning which allows for recovery of corrupted files. ● The secure workstation's base image is stored by central IT and available to be used to restore the secure workstation when needed.

Hardware/Downloadable Devices/ Data storage ● Physical Security ● Data handling and retention ● Peripherals	● The secured workstation will be physically located in the secure BSL3 Lab on the UCR campus. ● The BSL3 Lab is locked with a biometric access system at all times. ● Only personnel authorized by the BSL3 Lab Director have access to the facility. ● There will be no physical access to Google Drive. ● Data stored at rest in Google Drive will be secured with AES256 encryption. ● Data in transit with Google Drive will be secured by TLS 1.2 or newer. ● Data stored on the secured workstation will be encrypted using

	full disk encryption using AES-128 encryption. ● No peripherals are used in this environment.