## 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.

# Daily Emotional Lives of Students (DELS)
# Data Security Plan

| | |
|---|---|
| **Research Project Name:** | Daily Emotional Lives of Students (DELS) |
| **External Party:** | N/A |
| **Principal Investigator and Lab Director:** | Tabea Springstein |
| **Project Researcher(s):** | Macey Grisso (Lab Manager), Alana Suleiman (Undergraduate Research Assistant), Pareeya Jiyacharoen (Undergraduate Research Assistant), Nancy Zhang (Undergraduate Research Assistant), Jocelyn Aragon (Undergraduate Research Assistant), Phoebe Cheng (Undergraduate Research Assistant), Nikki Doiphode (Undergraduate Research Assistant), Thinh Nguyen (Undergraduate Research Assistant), Yesenaia Contreras-Urrutia (Undergraduate Research Assistant) |
| **Unit:** | CHASS |
| **Department:** | Psychology, Emotional Lives Lab |
| **Unit IT Director or UISL:** | James Lin, Raymond Holguin |
| **Unit Service Provider or IT Director:** | CHASS IT |
| **ISO Assessor:** | Nick Christopher |
| **CISO:** | Dewight Kramer |

| | |
|---|---|
| **Protection Level:** | P4 |
| **Availability Level:** | A2 |
| **Meets or Exceeds the Following Compliance Standards or Policies:** | UC IS-3, UC Minimum Security Standard |
| **Date Approved:** | 02/19/2025 |

**Revision History**

| Date | By | Contact Information | Description |
|---|---|---|---|
| 04/04/2025 | Nick Christopher | nickolas.christopher@ucr.edu | Changed Google Drive to M365 SharePoint |
| 05/09/2025 | Nick Christopher | nickolas.christopher@ucr.edu | Removed Nikhita Bulusu |

# Table of Contents

## Executive Summary

This study recruits undergraduate students for a 21-day experience sampling and mobile sensing study using the m-Path Sense app. Participants complete questionnaires and tasks in-lab, then use the app to answer random surveys about social and emotional processing and collect mobile sensing data (GPS, Wi-Fi, accelerometer, etc.). While survey data is anonymized, mobile sensing data, due to its richness, poses a potential risk to participant identifiability.

Data is initially stored on KU Leuven's Microsoft Azure servers, with mobile sensing data being bundled and transferred to the researchers' secure server and workstations. All raw data will be stored indefinitely in encrypted and password-protected files, with identifiable mobile sensing data kept separately. Contact information will be stored in locked cabinets and an encrypted electronic file on a secure UCR server. Data will be maintained for at least three years post-study, then securely disposed of.

## Purpose

The purpose of this data security plan ("Plan") is to document the security measures and policies for handling data related to the DELS Study. 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 [Daily Emotional Lives of Students (DELS)].
    - Full access to the data on the secured analysis computer.
    - No administrative access to the secured analysis computer.
    - Responsible for holding backup of data in escrow.
    - Responsible for supervising all research conducted using the data.
    - Shared responsibility with UISL for ensuring ongoing compliance with all elements of this plan.
- Unit Information Security Lead (UISL) for CHASS: staff member appointed by the Dean of CHASS with responsibility for information security.
    - Full access to data on the secured analysis computer.
    - Administrative access to the secured analysis computer.
    - Responsible for supervising Unit IT personnel with administrative access to the secured analysis computer and data.
    - Shared responsibility with PI for ensuring ongoing compliance with all elements of this plan.
- 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 [EXTERNAL PARTY] [*NOTE: THIS IS ONLY THE CASE IF THE AGENCY REQUIRES IT, OTHERWISE IT IS THE PI.*]~~
- ~~[EXTERNAL PARTY]: (EXAMPLE STATEMENT) agency providing the data for the sole purpose of the investigation described in the data agreement (Attachment 1: [EXTERNAL PARTY] Data Sharing Agreement)~~
    - ~~Originator of data.~~
    - ~~No access to secured analysis computer.~~
- Service Provider or IT Director for CHASS: IT service provider responsible for provisioning, configuring, and managing the IT infrastructure used for processing the data, under the direction of the UISL.
    - Note: access described below will be limited to a subset of career CHASS IT staff members. No student employees will have access.

    - Full access to data on the secured analysis computer.
    - Administrative access to the secured analysis computer.
    - Responsible for provisioning, deploying, and maintaining the IT environment for the secured analysis computer.
- Project Researcher (Researcher): a researcher (including research assistants) 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

**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.<br>• Access to networks and network services must follow the Least Privilege Principle.<br>• Units must route network access to Institutional Information classified at Protection Level 4 through secure access control points.<br>• Units must monitor network access to Institutional Information classified at Protection Level 3 or higher to detect unauthorized access.<br>• Units must limit access to authorized users and prevent unauthorized access to Institutional Information and IT Resources.<br>• Each Workforce Member and student must have a unique user account to distinguish that user from other users. | M365 Sharepoint or OneDrive<br>• M365 Sharepoint access will be controlled via sharing permissions. PI and lab director will ensure only required staff per this security plan and m-Path have access to the M365 Sharepoint folder.<br><br>Secure Server<br>• The secure server is protected by a firewall managed by the CHASS IT Team.<br>• ~~Access to RDP is available on campus~~.<br>• Off-campus access to the secure server is permitted only via UCR Campus VPN (GlobalProtect). UCR Campus VPN requires multi-factor authentication.<br>• Local accounts are provisioned for PIs and project researchers.<br>• Project data is accessible only to PIs, project researchers and CHASS IT Team.<br><br>Workstations<br>• All workstations will have host-based firewalls enabled to prevent inbound access.<br>• Access to secure data on workstations will be restricted to researchers listed on this plan. |

| | |
|---|---|
| | ● Workstations will be on protected private network |
| **External Party Requirements** | **Controls** |
| ● N/A | ● N/A |

## 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.<br>● Units must encrypt Institutional Information classified at Protection Level 3 or higher when stored on portable electronic media or portable computing devices.<br>● Units must encrypt Institutional Information classified at Protection Level 4 when stored on any electronic media. | M365 SharePoint or OneDrive<br>● M365 SharePoint or OneDrive uses AES-256 encryption for data in transit and at rest.<br><br>Secure Server<br>● The data on the secure server will be stored in an encrypted folder using AES-128 or AES-256.<br>● The passphrase will be known only to CHASS IT personnel and researchers on this plan.<br>● The passphrase will be stored on a separate server in an encrypted file.<br>● The passphrase will only be known to CHASS IT, PI, and lab manager.<br>● The passphrase shall be changed any time anyone who has the passphrase no longer requires access.<br>● Remote Desktop Protocol and any file shares will enforce TLS v1.2 or newer.<br><br>Workstations |

| | |
|---|---|
| | ● All workstations will use full-disk encryption with AES-128 or AES-256. |
| **External Party Requirements** | **Controls** |
| ● N/A | ● N/A |

## 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:<br>○ Statutory, regulatory and contractual requirements.<br>○ Institutional Information Classification.<br>○ Area entry safeguards and controls protecting physical access to Institutional Information and IT Resources.<br>○ 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.<br>○ Administrative and physical controls on third-party access and supervision.<br>● Units must ensure that physical access to secured areas is based on job responsibilities.<br>● Workforce Members must protect IT Resources from unauthorized access, loss, theft or damage. | M365 SharePoint or OneDrive<br>● Google is responsible for physical security of M365 SharePoint or OneDrive.<br><br>Secure Server<br>● The secured server will be physically located in the UCR CHASS HMNSS Building.<br>● The UCR HMNSS 3600 wing has a security system connected to UCPD<br>● The server room has a separate security system connected to UCPD.<br>● Physical keys are used to access the building, the floor of the server room and the server room.<br>● Keys to the server room are restricted to CHASS IT personnel, ITS Network Team, UCR Facilities, and UCPD.<br>● The server room is monitored by motion-detected video security cameras. Security cameras alert on any movement in the server room. |

| | |
|---|---|
| • 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.<br>• Units must ensure that Institutional Information classified at Protection Level 3 or higher is adequately protected both on- and off-site. | Workstations<br>• All lab workstations are locked in Olmsted 2115<br>• Researchers using laptops will take precautions to ensure laptops are kept in their control. (e.g., laptops should not be left unattended in public places, visible in unattended vehicles, etc.) |
| **External Party Requirements** | **Controls** |
| • N/A | • N/A |

## 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.<br>• Units must monitor IT Resources to detect signs of attack or compromise when any of the following are present:<br>  ○ Institutional Information classified at Protection Level 2 or higher.<br>  ○ IT Resources classified at Protection Level 3 or higher.<br>  ○ IT Resources classified at Availability Level 3 or higher. | • The secure server and all workstations will have Trellix HX agent installed.<br>  ○ Trellix reports to a unified cloud console monitored by Trellix and UCR Security Operations |
| **External Party Requirements** | **Controls** |
| • N/A | • N/A |

## 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.<br>• Units must comply with UC Records Retention Schedule for retention of backups.<br>• Units must protect backups according to the Protection Level of the Institutional Information they contain.<br>• Units must ensure that portable backup media meet the portable media requirements outlined in the IS-3 policy.<br>• Units must document and execute a plan to test restoration of Institutional Information from backups.<br>• Units must maintain a backup catalog that shows the location of each backup and retention requirements. | M365 SharePoint or OneDrive<br>• No backups are made of M365 SharePoint or OneDrive contents.<br><br>Secure Server<br>• Backups are stored on another server protected by the CHASS firewall and in the cloud of CHASS IT M365 SharePoint or OneDrive. The backup server is only accessible at the physical console or directly on the private network.<br>• There is no rotation period on the backups.<br><br>Workstations<br>• No backups are made of workstations. |
| **External Party Requirements** | **Controls** |
| • N/A | • N/A |

## Logging and Auditing

Proper logging and monitoring are required practices for recording events and generating evidence.

| **UC Requirements (*BFB-IS-3 12.4*)** | **Control** |
|---|---|

| | |
|---|---|
| • Units must comply with the UC Event Logging Standard for IT Resources when storing, processing or transmitting Institutional Information.<br>• Units must obtain approval for erasing, purging or trimming event logs through the change management process.<br>• Units must protect logs according to the Protection Level of the Institutional Information they contain and may not release them without proper authorization.<br>• 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.<br>• 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:<br>  ○ Only authorized activity occurred.<br>  ○ Anomalies are analyzed and corrective actions are implemented.<br>• For Institutional Information classified at Protection Level 3 or higher, Units must limit access to administrative logs using the Need to Know Principle. | • **EXCEPTION**: All systems are configured with default logging settings.<br>• There is no available logging service to export logs at this time. |
| **External Party Requirements** | **Controls** |
| • N/A | • N/A |

## Control of Operational Software

| **UC Requirements (*BFB-IS-3 12.5*)** | **Controls** |
|---|---|
| ● Units must obtain approval for software installation, configuration changes and updates on production systems through the Location change management process. | Secure Server<br>● The server runs Windows Server 2016.<br>● This is a file server providing storage via network shared drive. No shared or user requested software packages are installed.<br>● Only CHASS IT system administrators have access to make software installations.<br><br>Workstations<br>● Software installations on workstations will be managed by CHASS IT. |
| **External Party Requirements** | **Controls** |
| ● N/A | ● N/A |

## Vulnerability & Patch Management

| **UC Requirements (*BFB-IS-3 12.6*)** | **Controls** |
|---|---|
| ● Units must only use supported and patched versions of hardware and software. | ● Qualys Cloud Agent will be installed on all systems.<br><br>Secure Server<br>● Patches are installed monthly using Windows Server Update.<br><br>Workstations |

| | |
|---|---|
| | ● CHASS IT or ITS Secure Devices will ensure all patches are installed at least monthly. |
| **External Party Requirements** | **Controls** |
| ● N/A | ● N/A |

## 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.<br>● 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.<br>● Units must turn off or disable unused ports, protocols and services for IT Resources processing Institutional Information classified at Protection Level 3 or higher.<br>● Units must ensure that IT Resources processing Institutional Information classified at Protection Level 3 or higher use secure versions of network services. | Secure Server<br>● The secured server is segmented using a CHASS-managed Fortinet firewall.<br>● The firewall includes dynamic threat detection service.<br>● Inbound access is limited to UCR Campus.<br>● Remote access off-campus requires VPN.<br>● Outbound network access is unrestricted to allow for updates and other usage requirements.<br><br>Workstations<br>● All workstations will have host-based firewalls enabled.<br>● Inbound communication will be blocked by default. |

| | |
|---|---|
| • Units must ensure that network devices used to control access to Institutional Information classified at Protection Level 4:<br>  ○ Use the most restrictive rules possible.<br>  ○ Allow only authorized connections.<br>  ○ Detect and log unauthorized access or access attempts.<br>  ○ Review the network access rules.<br>• Units must ensure that the transfer of Institutional Information classified at Protection Level 3 or higher between UC Locations, to Suppliers, or to external entities/organizations use appropriate security controls approved by the CISO and Institutional Information Proprietor. | |
| **External Party Requirements** | **Controls** |
| • N/A | • N/A |

## Transfer of Data from m-Path to UC Riverside

1. m-Path automatically sends data to a UCR-managed M365 SharePoint or OneDrive folder. This folder is owned by the DELS Study Team. (Data remains in the M365 SharePoint or OneDrive folder for 21 days.)
2. Project researchers connect to the secure server and manually download the data from the M365 SharePoint or OneDrive folder to the secured server. No other systems are involved in data transfer.
3. Data will be analyzed on UCR-owned lab computers in the protected network through map network drive to secure server.

## Operational Use of Secure Server and Analysis Workstations

- The secure server is used for transfer of data using secure methods or analysis of data. The secure server shall not be used for any other purpose.

- Workstations used for analysis shall be UCR-owned and comply with the UC Minimum Security Standard, and UC IS-3 P4 requirements. UCR-owned workstations shall not be used for personal use.
- Secure data must only reside on the M365 SharePoint or OneDrive folder and the CHASS secure server.
- Administrative access will be restricted to CHASS IT.

## Cyclical Security Review

- This system shall be reviewed annually to ensure proper controls are in place.
- This system shall be reviewed after any major architectural or configuration changes (e.g., firewall changes, major OS upgrades, etc.)
- CHASS IT Team and the Information Security Office shall conduct annual reviews.
- PI and Lab team shall validate access and permissions to M365 SharePoint or OneDrive folder.

## 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 conclusion of research, PI will request CHASS IT to delete all secure data and backups.
- Any copies of encrypted folder passphrases will be destroyed per the UC Disposal of Institutional Information standard.

## Security Plan Review

- This plan will be reviewed at least annually by the PI and UISL to verify continued compliance. Any risks identified will be added to the security plan following the process defined under Changes.
- During the review process, the PI will review the list of people with access to the data and ensure that access is revoked for any who no longer require access.

## Violations of Data Security Plan

Any violations of the data security plan shall be reported immediately to the PI, UISL, Unit IT Director and CISO.

## Security Plan Changes

Any changes to the IT environment or policies used for processing the data will be documented; approved by the PI and UISL; and submitted to the ISO for review and approval before implementation.

## Agreement & Signatures

The undersigned agree to abide by this security plan.

Any researchers who will be granted access to the data covered by this plan in the future will be required to read ,agree and sign this plan or an addendum to this plan.

| Role | Name | Signature | Date |
|---|---|---|---|
| Principal Investigator | Tabea Springstein | Signed by: Tabea Springstein 2F6214C1D741499... | 5/9/2025 \| 5:22 PM PDT |
| Lab Manager | Macey Grisso | Signed by: Macey Grisso C23839E3E51843B... | 5/9/2025 \| 5:12 PM PDT |
| Unit IT Director and UISL | James Lin | | |
| Project Researcher | Alana Suleiman | | |
| Project Researcher | Pareeya Jiyacharoen | | |
| Project Researcher | Nancy Zhang | | |
| Project Researcher | Jocelyn Aragon | | |

| | | | |
|---|---|---|---|
| Project Researcher | Phoebe Cheng | | |
| Project Researcher | Nikki Doiphode | | |
| Project Researcher | Thinh Nguyen | | |
| Project Researcher | Yesenia Contreras-Urrutia | | |