Data Security Plan

Urban_Change_Detection_Phase_2

Generated by Ursa DSP

2025-12-23

Instructions

<p>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").</p> <p>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.</p> <p>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.</p> <p>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."</p> <p>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.</p> <p>If you have any questions regarding this form, contact the Information Security Office Risk Team at iso-risk@ucr.edu.</p>

Research Project Data Security Plan

<p>This project, "Urban Change Detection Phase 2," led by Dr. Sarah Connor of the Department of Geospatial Sciences, involves the analysis of high-resolution satellite imagery provided by the National Geospatial-Intelligence Agency (NGA). The data is classified as Controlled Unclassified Information (CUI). To comply with strict data security standards (NIST 800-171), all data storage and processing will occur exclusively on a dedicated air-gapped server running the Linux operating system, located physically within the Secure Research Lab. The server is strictly isolated from all public and campus networks to prevent unauthorized remote access.</p> <p>Data will be transferred to the secure environment via authorized Secure Transfer methods managed by the Unit Information Security Lead (UISL), John Smith. Researchers are prohibited from removing data from the air-gapped server or transferring it to personal devices, laptops, or unauthorized external storage. All CUI data will be retained until the project retention date of 2030-01-01. Upon conclusion of the retention period, the data and storage media will be destroyed using a DoD-compliant wipe (e.g., DoD 5220.22-M) to render the information irretrievable.</p>

Revision History

<table> <thead> <tr> <th style="text-align: left;">Date</th> <th style="text-align: left;">By</th> <th style="text-align: left;">Contact Information</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td style="text-align: left;">[Current Date]</td> <td style="text-align: left;">John Smith</td> <td style="text-align: left;">john.smith@university.edu</td> <td style="text-align: left;">Initial creation of Data Security Plan for Urban Change Detection Phase 2</td> </tr> </tbody> </table>

Table of Contents

Executive Summary

<p>The 'Urban Change Detection Phase 2' project, led by Principal Investigator Dr. Sarah Connor within the Department of Geospatial Sciences, involves the analysis of high-resolution satellite imagery to detect longitudinal changes in urban infrastructure. The data supporting this research is provided by the National Geospatial-Intelligence Agency (NGA) and is classified as Controlled Unclassified Information (CUI). Due to the sensitivity of the data, this Data Security Plan (DSP) implements strict security controls aligned with NIST 800-171 and CMMC standards.</p> <p>All CUI data will be stored and processed exclusively on a dedicated air-gapped server running the Linux operating system, located within the physically secured Secure Research Lab. This infrastructure is isolated from all public and private networks to prevent unauthorized remote access or data exfiltration. Data ingestion will occur via approved secure transfer methods. Access to the air-gapped environment is restricted solely to authorized personnel listed in this plan. Data will be retained until January 1, 2030, after which it will be destroyed using a Department of Defense (DoD) compliant wiping standard.</p>

Purpose

<p>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 National Geospatial-Intelligence Agency (NGA). 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.</p> <p>This plan applies to both raw data received, any copies of the raw data and any derivatives and output of analysis thereof.</p>

Stakeholders, Roles, and Responsibilities

<p>All stakeholders are responsible for reporting any suspected or confirmed incident or breach of data security to the Lab Director, UISL, and ISO immediately.</p> <ul> <li> <p><strong>Principal Investigator (PI):</strong> Lead researcher for <strong>Urban Change Detection Phase 2</strong> (Dr. Sarah Connor).</p> <ul> <li>Full access to the data on the secured air-gapped server.</li> <li>No administrative access to the secured air-gapped server.</li> <li>Responsible for holding backup of data in escrow.</li> <li>Responsible for supervising all research conducted using the data.</li> <li>Shared responsibility with UISL for ensuring ongoing compliance with all elements of this plan.</li> </ul> </li> <li> <p><strong>Unit Information Security Lead for Geospatial Sciences (UISL):</strong> Staff member appointed by the Dean of Geospatial Sciences with responsibility for information security (John Smith).</p> <ul> <li>Full access to data on the secured air-gapped server.</li> <li>Administrative access to the secured air-gapped server.</li> <li>Responsible for supervising Unit IT personnel with administrative access to the secured air-gapped server and data.</li> <li>Shared responsibility with PI for ensuring ongoing compliance with all elements of this plan.</li> </ul> </li> <li> <p><strong>UC Riverside Information Security Office (ISO):</strong> UC Riverside central information security office, under the direction of the Chief Information Security Officer (CISO).</p> <ul> <li>No access to data.</li> <li>No access to secured air-gapped server.</li> <li>Responsible for reviewing this plan, including approval of any future changes prior to implementation.</li> <li>CISO is the responsible official for signing the data agreement with the NGA.</li> </ul> </li> <li> <p><strong>National Geospatial-Intelligence Agency (NGA):</strong> Agency providing the data for the sole purpose of the investigation described in the data agreement (Attachment 1: NGA Data Sharing Agreement).</p> <ul> <li>Originator of data.</li> <li>No access to secured air-gapped

server.</li> </ul> </li> <li> <p><strong>Service Provider or IT Director for Geospatial Sciences:</strong> IT service provider responsible for provisioning, configuring, and managing the IT infrastructure used for processing the data, under the direction of the UISL.</p> <ul> <li>Full access to data on the secured air-gapped server.</li> <li>Administrative access to the secured air-gapped server.</li> <li>Responsible for provisioning, deploying, and maintaining the IT environment for the secured air-gapped server.</li> </ul> </li> <li> <p><strong>Project Researcher (Researcher):</strong> A researcher attached to the research project who will have access to the raw data under the direction of the PI.</p> <ul> <li>Full access to data on the secured air-gapped server.</li> <li>No administrative access to the secured air-gapped server.</li> </ul> </li> </ul>

Configuration of Secured Computing and Storage

<h3>Access Control</h3> <p><strong>Objective:</strong> Limit access to Institutional Information and IT Resources.</p> <p><strong>UC and Project Requirements (NIST 800-171/CMMC)</strong> * <strong>Local Console Access Only:</strong> Due to the air-gapped configuration, no remote access (e.g., RDP, SSH, VNC) is permitted. Access to the server is restricted to the physical console located in the Secure Research Lab. * <strong>Account Management:</strong> Unique local user accounts will be provisioned only for the PI and authorized Project Researchers listed in this plan. Guest or shared accounts are strictly prohibited. * <strong>Authentication:</strong> Multi-factor authentication (MFA) or strong password policies meeting UC Class 4 standards (minimum 12 characters, complexity requirements) will be enforced for local login. * <strong>Least Privilege:</strong> Administrative (root/sudo) access is restricted to the designated Unit IT Director/UISL (John Smith) for maintenance purposes. Researchers will hold standard user privileges. * <strong>Session Termination:</strong> Automatic screen locking will be enabled after 15 minutes of inactivity, requiring re-authentication to unlock.</p> <h3>Encryption</h3> <p><strong>Objective:</strong> Ensure appropriate access to protect UC Institutional Information and IT Resources.</p> <p><strong>Controls</strong> * <strong>Data at Rest:</strong> The Linux server storage volumes will be encrypted using LUKS (Linux Unified Key Setup) with AES-256 encryption. This includes swap partitions to prevent data leakage. * <strong>Removable Media:</strong> Any external media used for data ingress/egress (e.g., for transferring NGA data or updates) must be encrypted using FIPS 140-2 compliant algorithms (AES-256). * <strong>Key Management:</strong> Encryption keys/passphrases will be managed by the UISL and stored in a secure, separate location from the hardware.</p> <h3>Physical and Environmental Security</h3> <p><strong>Objective:</strong> Ensure

appropriate physical access to protect UC IT Resources and Institutional Information.</p> <p><strong>Controls</strong> * <strong>Location:</strong> The air-gapped server is physically located in the Secure Research Lab within the Department of Geospatial Sciences. * <strong>Access Controls:</strong> Entry to the lab is controlled via electronic key card and/or physical key, restricted to authorized personnel. A physical access log will be maintained. * <strong>Monitoring:</strong> The server room is monitored by 24/7 video surveillance. The server itself will be physically secured (e.g., locked rack or Kensington lock) to prevent removal. * <strong>Hardware Security:</strong> All physical ports not required for operation (e.g., unused USB ports) will be physically blocked or logically disabled in the BIOS/OS.</p> <h3>Protection from Malware and Intrusion</h3> <p><strong>Controls</strong> * <strong>Antivirus:</strong> The server will run Linux-compatible antivirus software (e.g., ClamAV). Since the system is air-gapped, virus definitions will be manually updated monthly via secure, scanned removable media by the UISL. * <strong>File Integrity Monitoring:</strong> A file integrity monitoring tool (e.g., AIDE) will be installed to detect unauthorized changes to system binaries and configuration files. * <strong>Media Scanning:</strong> Any removable media introduced to the environment must be scanned for malware on a separate, isolated scanning station before being connected to the air-gapped server.</p> <h3>Backup</h3> <p><strong>Controls</strong> * <strong>Method:</strong> Backups of CUI data will be performed manually onto encrypted external hard drives. * <strong>Storage:</strong> Backup media will be stored in a GSA-approved security container or a locked fireproof safe separate from the server location, accessible only by the PI and UISL. * <strong>Retention:</strong> Backups will be retained according to the project lifecycle and NGA requirements, then destroyed via DoD-approved wipe methods.</p> <h3>Logging and Auditing</h3> <p><strong>Objective:</strong> Proper logging and monitoring are required practices for recording events and generating evidence.</p> <p><strong>Controls</strong> * <strong>Local Logging:</strong> The Linux Audit framework (auditd) will be configured to log security-relevant events, including successful/failed logins, privilege escalation (sudo), and file access modification. * <strong>Log Retention:</strong> Logs will be retained locally for at least one year. Due to the air-gapped nature of the system, logs cannot be exported to a central SIEM; therefore, the UISL will conduct a manual review of logs on a monthly basis. * <strong>Audit Trails:</strong> The system will maintain an automated audit trail sufficient to reconstruct security-relevant events.</p> <h3>Control of Operational Software</h3> <p><strong>Controls</strong> * <strong>Whitelisting:</strong> Only software explicitly required for the analysis of satellite imagery (e.g., QGIS, GDAL, Python scientific stack) and system maintenance is permitted. * <strong>Installation Restrictions:</strong> Software installation capabilities are restricted to the UISL (root user). Researchers cannot install or modify system software. * <strong>Port Control:</strong> USB ports are logically restricted to allow only authorized, encrypted mass storage devices identified by hardware ID, preventing the use of unauthorized peripherals.</p> <h3>Vulnerability &amp; Patch Management</h3> <p><strong>Controls</strong> * <strong>Manual Patching:</strong> Due to the lack of internet connectivity, the UISL will implement a monthly maintenance cycle. Security patches for the Linux OS and application software will be downloaded to secure media on a connected workstation, scanned, and manually applied to the air-gapped server. * <strong>Vulnerability Assessment:</strong> The UISL will perform periodic vulnerability assessments using portable scanning tools or local agents to verify the security posture.</p> <h3>Communications Security</h3> <p><strong>Objective:</strong> Ensure the security of Institutional Information regarding network isolation.</p> <p><strong>Controls</strong> * <strong>Air-Gap Enforcement:</strong> All network interface cards (NICs), including Ethernet, Wi-Fi, and Bluetooth, will be physically removed or disabled at the BIOS and OS kernel level. * <strong>Isolation:</strong> The server will have no physical or logical connection to the campus network, the public Internet, or any other system. * <strong>Data Transfer:</strong> Data transfer from the NGA to the server will occur solely via the approved Secure Transfer method (encrypted physical media), following strict chain-of-custody procedures.</p>

Transfer of Data from [EXTERNAL PARTY] to UC Riverside

<ol> <li> <p><strong>Data Encryption and Preparation</strong>: Before transmission to UC Riverside, the National Geospatial-Intelligence Agency (NGA) will encrypt the Controlled Unclassified Information (CUI) data in ZIP format utilizing AES-256 encryption. The encryption passphrase shall be unique and consist of no less than 10 alphanumeric characters, strictly excluding common words, phrases, or names.</p> </li> <li> <p><strong>Initial Transmission</strong>: The encrypted ZIP file will be stored in a secure Microsoft 365 SharePoint repository and shared with the Unit Information Security Lead (UISL). The encryption passphrase for the ZIP file will be transmitted separately to the UISL via telephone (out-of-band communication).</p> </li> <li> <p><strong>Transfer to Portable Media</strong>: Once the encrypted ZIP file has been accessed by the UISL, it will be downloaded and copied directly onto a dedicated encrypted USB flash drive.</p> </li> <li> <p><strong>Transfer to Secure Infrastructure</strong>: The UISL will physically transport the encrypted USB flash drive to the Secure Research Lab. The encrypted ZIP file will be transferred to the air-gapped Linux server (secured analysis computer), retaining the encrypted copy on the USB flash drive.</p> </li> <li> <p><strong>Decryption</strong>: The UISL will decrypt the ZIP file solely on the air-

gapped Linux server.</p> </li> <li> <p><strong>Backup and Key Management</strong>: The UISL will provide the encrypted USB flash drive to the Principal Investigator (PI) to serve as a backup of the original data, along with the encryption key for the USB drive (distinct from the ZIP file passphrase). The USB flash drive will be stored in a locked location (e.g., desk drawer in the PI's office), and the encryption key for the USB drive will be stored in a separate locked location to ensure physical separation of the cryptographic key and the encrypted media. The UISL will escrow the encryption passphrase for the ZIP file in a secure, institutional password management system. In the event of a failure of the secured analysis computer, the PI may contact the UISL to perform data recovery.</p> </li> <li> <p><strong>Verification and Sanitization</strong>: The PI will confirm the successful data decryption and integrity on the air-gapped server. Upon this confirmation, the UISL will securely destroy the copy residing on SharePoint in accordance with NIST 800-88 media sanitization guidelines.</p> </li> </ol>

Operational Use of Secured Analysis Computer

<h3>Operational Use of Secured Analysis Computer (Air-Gapped Server)</h3> <p><strong>1. Secure Environment and Isolation</strong> The secured analysis computer is a standalone, air-gapped Linux server located in the Secure Research Lab. It is physically isolated from the university network and the internet to ensure the confidentiality of the Controlled Unclassified Information (CUI) provided by the NGA. No network interfaces (wired or wireless) will be enabled during the storage or processing of the data.</p> <p><strong>2. Data Transfer Procedures</strong> To maintain the air-gapped integrity of the system, the following procedures regarding the use of removable media will be strictly enforced:</p> <ul> <li><strong>Dedicated Media:</strong> A FIPS 140-2 compliant encrypted USB flash drive will be provisioned specifically for project use. This drive is distinct and separate from the flash drive used for the backup of the original data.</li> <li><strong>Exclusive Transfer Method:</strong> Only this specific encrypted drive will be used to move data, scripts, or outputs to or from the secured analysis computer.</li> <li><strong>Key Management:</strong> Only the Principal Investigator (Dr. Sarah Connor) and approved researchers listed in this Data Security Plan will have access to the encryption key or passphrase for the encrypted USB flash drive.</li> </ul> <p><strong>3. Restrictions on Data Movement</strong> * <strong>Data Ingress:</strong> Only statistical analysis scripts, code, or approved software updates intended for use in the project's specific analytical workflow will be copied from other computers to the encrypted USB flash drive for transfer to the secured server. All files will be scanned for malware prior to introduction to the air-gapped environment. * <strong>Data Egress:</strong> Only aggregated, de-identified data (e.g., summary statistics, charts, or non-sensitive outputs)

will be copied from the secured analysis computer to the encrypted USB flash drive for use in other applications or reporting. * <strong>Prohibited Content:</strong> No other data sets, applications, executables, documents, or files other than those explicitly noted above will be copied to or from the secured analysis computer.</p> <p><strong>4. Operational Exceptions</strong> Any operational need to remove un-aggregated, identifiable data or raw CUI from the secured analysis computer must be approved in advance, in writing, by both the PI and the Unit Information Security Lead (John Smith).</p>

Cyclical Security Review

<p>At least once every three months, the Unit IT Service Provider, in coordination with the Unit Information Security Lead (UISL), will perform a comprehensive security review and maintenance of the air-gapped secured analysis server to ensure ongoing compliance with NIST 800-171 and CUI protection requirements.</p> <p>The cyclical review will consist of the following actions: * <strong>Log Analysis:</strong> A manual review of local system, application, and security logs (e.g., Linux audit logs, authentication logs) to identify anomalies, failed authentication attempts, or potential intrusion indicators. * <strong>Patch Management:</strong> Installation of operating system and security patches using offline methods. Updates will be acquired via a secure, network-connected staging machine, scanned for malware, and transferred to the air-gapped server via approved secure transfer media. * <strong>Access Verification:</strong> Verification that active user accounts are limited to current, authorized research personnel and that file system permissions remain correctly configured to restrict access to CUI. * <strong>Physical Inspection:</strong> Inspection of the physical server for signs of tampering, unauthorized peripheral connections, or breach of physical security controls within the Secure Research Lab. * <strong>Documentation:</strong> Completion of a maintenance checklist recorded in the UC Riverside ITS ServiceNow instance or the lab's physical maintenance log.</p> <p>Any identified vulnerabilities, deviations from the system security plan, or suspicious log activity will be reported immediately to the PI and UISL for remediation. Suspected incidents will be escalated to the Information Security Office (ISO) in accordance with the incident response plan.</p>

Data Retention & Destruction

<p>At the conclusion of the research period (scheduled retention date: 2030-01-01), or upon the termination of the agreement with the National Geospatial-Intelligence Agency (NGA), all

Controlled Unclassified Information (CUI) and derived data will be securely destroyed from UC Riverside systems.</p> <p>The storage volumes on the air-gapped Linux server will be fully erased using a secure deletion tool (e.g., <code>shred</code> or <code>scrub</code>) configured to meet the DoD 5220.22-M (seven random overwrite passes) standard. Any removable media used for secure transfer will be sanitized using the same DoD 5220.22-M standard or physically destroyed in accordance with NIST 800-88 Guidelines for Media Sanitization.</p> <p>Upon completion of the destruction process, the Principal Investigator and Unit Information Security Lead will verify the sanitization. A Certificate of Sanitization will be generated and retained to attest that the data has been rendered irretrievable.</p>

Security Plan Review

<p>● This plan will be reviewed at least annually by the Principal Investigator (Dr. Sarah Connor) and the Unit Information Security Lead (John Smith) to verify continued compliance with NIST 800-171 standards and NGA requirements.</p> <p>● Any risks, vulnerabilities, or changes in the operating environment identified will be documented and added to the security plan following the process defined under Security Plan Changes.</p> <p>● During the review process, the PI will conduct a formal review of the list of authorized personnel with physical access to the Secure Research Lab and logical access to the air-gapped server. The PI will ensure that access is immediately revoked for any individuals who no longer require access to the CUI data.</p>

Violations of Data Security Plan

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

Security Plan Changes

<p>Any changes to the IT environment, architecture, or policies used for processing the NGA CUI data will be documented; approved by the Principal Investigator (Dr. Sarah Connor) and the Unit Information Security Lead (John Smith); and submitted to the Information Security Office (ISO) for review and approval before implementation.</p> <p>Additionally, any changes to the list of researchers with access to the 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.</p>

Agreement & Signatures

<p>The undersigned agree to abide by this security plan.</p> <p>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.</p> <table> <thead> <tr> <th style="text-align: left;">Role</th> <th style="text-align: left;">Name</th> <th style="text-align: left;">Signature</th> <th style="text-align: left;">Date</th> </tr> </thead> <tbody> <tr> <td style="text-align: left;">Principal Investigator</td> <td style="text-align: left;">Dr. Sarah Connor</td> <td style="text-align: left;"></td> <td style="text-align: left;"></td> </tr> <tr> <td style="text-align: left;">Unit Information Security Lead</td> <td style="text-align: left;">John Smith</td> <td style="text-align: left;"></td> <td style="text-align: left;"></td> </tr> <tr> <td style="text-align: left;">Chief Information Security Officer</td> <td style="text-align: left;"></td> <td style="text-align: left;"></td> <td style="text-align: left;"></td> </tr> </tbody> </table>