Data Security Plan

Project_Poseidon:_Mapping_the_Mid-Atlantic_Ridge

Generated by Ursa DSP

2025-12-23

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, UC Minimum Security Standard, and the standard required by the external party (e.g., NIST 800-171 for CUI/Export Control).

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.

Research Project Data Security Plan

Research Project Name: Project Poseidon: Mapping the Mid-Atlantic Ridge
External Party: Atlantis Marine Institute
Principal Investigator and Lab Director: Dr. Arthur Curry
Project Researcher(s): Dr. Arthur Curry
Unit: Department of Oceanography
Department: Oceanography
Unit Information Security Lead (UISL): Mera
Unit Service Provider or IT Director: Mera
ISO Assessor: [Assigned ISO Assessor]
CISO: [Chief Information Security Officer]
Protection Level: P4 (Export Controlled / CUI)
Availability Level: A2

Meets or Exceeds the Following Compliance Standards or Policies: NIST 800-171, CMMC, UC IS-3, UC Minimum Security Standard

Date Approved: [Current Date]

Revision History	Date	By	Description
1.0	[Current Date]	Mera	Initial Draft

Revision History

Date	By	Contact Information	Description
[Current Date]	Mera	mera@oceanography.university.edu	Initial creation of Data Security Plan for Project Poseidon

Table of Contents

- Transfer of Data from Atlantis Marine Institute to UC Riverside
- Operational Use of Secured Analysis Workstation
- Cyclical Security Review
- Data Retention & Destruction
- Security Plan Review
- Violations of Data Security Plan
- Security Plan Changes
- Agreement & Signatures

Executive Summary

Project Poseidon: Mapping the Mid-Atlantic Ridge, led by Principal Investigator Dr. Arthur Curry within the Department of Oceanography, involves the analysis of high-resolution sonar data provided by the **Atlantis Marine Institute**. This data is classified as **Export Controlled** and **Controlled Unclassified Information (CUI)**. To meet the stringent security requirements associated with this classification, this Data Security Plan outlines a dedicated, isolated computing environment.

All research data will be stored and processed exclusively on a **Standalone Linux Workstation** located within a secured facility in the Oceanography Department. This workstation is configured as an air-gapped system with **no internet connectivity** or connection to campus networks. Data transfers to and from the secure workstation will be conducted solely via **Encrypted SSDs** (Solid State Drives). No project data will be stored on cloud services, shared network drives, or unencrypted portable media. At the conclusion of the research, all data storage media will be sanitized in accordance with **DoD 5220.22-M** standards to ensure irretrievability.

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 **Atlantis Marine Institute**. 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):** Dr. Arthur Curry, lead researcher for *Project Poseidon: Mapping the Mid-Atlantic Ridge*.
  - 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 Oceanography:** Mera, staff member appointed by the Dean of Oceanography 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 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 Atlantis Marine Institute.

- **Atlantis Marine Institute:** Agency providing the data for the sole purpose of the investigation described in the data agreement (Attachment 1: Atlantis Marine Institute Data Sharing Agreement).
    - Originator of data.
    - No access to secured analysis computer.
- **Service Provider or IT Director for Oceanography:** 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:** 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

Objective: Limit access to Export Controlled and CUI data to authorized personnel only.

Requirement (NIST 800-171 / CUI)	Controls
Limit information system access to authorized users.	• The standalone Linux workstation operates in an **air-gapped environment** (no network connection).• Access is restricted to the Principal Investigator (Dr. Arthur Curry) and the Unit Information

Requirement (NIST 800-171 / CUI)	Controls
	Security Lead (Mera).• Local accounts are provisioned with unique User IDs; guest accounts are disabled.
Ensure that access to CUI follows the Need to Know and Least Privilege principles.	• **Root/Administrative access** is restricted solely to the UISL for system maintenance.• Standard user accounts are used for data processing and sonar analysis.
Verify and control/limit connections to and use of external information systems.	• No external connections are permitted. WiFi and Bluetooth hardware are physically removed or disabled at the BIOS/Kernel level.
Limit use of portable storage devices on external systems.	• USB ports are administratively restricted to authorized **Encrypted SSDs** only.
Session termination.	• The workstation is configured to automatically lock the screen after **15 minutes** of inactivity, requiring re-authentication to unlock.

Encryption

Objective: Protect the confidentiality of CUI at rest and during physical transfer.

Requirement (NIST 800-171 / CUI)	Controls
Protect the confidentiality of CUI at rest.	• The Linux workstation utilizes **Full Disk Encryption (FDE)** via LUKS (Linux Unified Key Setup) with AES-256 encryption.• Encryption keys are managed by the UISL and stored separately from the device.
Protect the confidentiality of CUI during transfer.	• Data transfer from the Atlantis Marine Institute is conducted exclusively via **Encrypted SSD**.• The external SSD utilizes FIPS 140-2 validated encryption (AES-256) to ensure compliance with Export Control regulations.

Physical and Environmental Security

Objective: Limit physical access to the standalone workstation processing Export Controlled data.

Requirement (NIST 800-171 / CUI)	Controls
Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	• The workstation is physically located in a secure office within the **Department of Oceanography**.• The room is locked when unoccupied; access keys are restricted to the PI and UISL.• The workstation chassis is secured to the desk to prevent theft.
Protect and monitor the physical facility and support infrastructure.	• The workstation screen is positioned away from windows and open doors to prevent unauthorized viewing (shoulder surfing).• Visitors to the lab are escorted at all times.

Protection from Malware and Intrusion

Objective: Maintain system integrity in an offline environment.

Requirement (NIST 800-171 / CUI)	Controls
Monitor, control, and protect organizational communications.	• **Host-based Firewall:** `ufw` or `iptables` is configured to DROP all inbound and outbound network traffic by default, reinforcing the air-gap.
Implement malicious code protection.	• **ClamAV** is installed on the workstation.• Due to the air-gapped nature, virus definitions are manually updated monthly via secure, read-only media prepared on a clean, internet-connected machine.
Monitor information system security alerts and advisories.	• **File Integrity Monitoring (FIM):** AIDE (Advanced Intrusion Detection Environment) is installed to detect unauthorized changes to system files or configurations.

Backup

Objective: Ensure recoverability of CUI without compromising security.

Requirement (NIST 800-171 / CUI)	Controls
Protect the confidentiality of backup CUI at storage locations.	• Backups are performed manually to a dedicated **Encrypted SSD**.• Backup media is stored in a GSA-approved security container or locked safe within the Department of Oceanography when not in use.• No cloud backups are utilized.

Logging and Auditing

Objective: Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized activity.

Requirement (NIST 800-171 / CUI)	Controls
Create and retain system audit logs and records.	• The Linux Audit daemon (`auditd`) is enabled and configured to log security-relevant events, including: login attempts (successful and failed), `sudo` usage, and file access modifications.• Logs are retained locally for a minimum of **one year**.
Review and update logged events.	• The UISL performs a manual review of audit logs **monthly** to identify anomalies or unauthorized access attempts.• Log integrity is verified against FIM baselines.

Control of Operational Software

Objective: Restrict software to the minimum necessary for the research mission.

Requirement (NIST 800-171 / CUI)	Controls
Limit use of organizational portable storage devices on external systems.	• Only software essential for the analysis of sonar data is installed.• Installation of new software requires **Root privileges**, restricted to the UISL.• Unused services, ports, and protocols are disabled or removed.

Vulnerability & Patch Management

Objective: Identify and correct system flaws in a timely manner.

Requirement (NIST 800-171 / CUI)	Controls
Identify, report, and correct information and information system flaws in a timely manner.	• **Manual Patching Process:** Security patches for the Linux OS and sonar applications are downloaded to a clean, internet-connected computer, scanned for malware, transferred to the standalone workstation via encrypted media, and applied.• Patching is performed **monthly** or immediately upon release of critical security updates relevant to the system configuration.

Communications Security

Objective: Prevent unauthorized information transfer.

Requirement (NIST 800-171 / CUI)	Controls
Control information posted or processed on publicly accessible information systems.	• **Air-Gap:** The system is physically disconnected from the internet and all campus networks.• Wireless capabilities (WiFi/Bluetooth) are hardware-disabled.• Data export is strictly controlled via physical encrypted media and logged manually by the PI.

Transfer of Data from [EXTERNAL PARTY] to UC Riverside

1. Before being transported to UC Riverside, **Atlantis Marine Institute** will save the data to a portable Solid State Drive (SSD) encrypted with **AES-256 encryption**.
2. The encryption passphrase shall be unique and be no less than 15 alphanumeric characters. It shall not include common words, phrases, or any names.
3. The Encrypted SSD will be physically transported to the UISL (**Mera**) via a secure courier service with tracking and signature validation required.
4. The encryption key for the SSD will be transmitted to the UISL via telephone or a secure out-of-band communication method.

5. Once the Encrypted SSD has been received by the UISL, it will be secured in a locked location until it is transferred to the secured analysis computer.
6. The UISL will connect the Encrypted SSD directly to the **secured analysis computer** (Standalone Linux Workstation).
7. The UISL will decrypt the files on the secured analysis computer (which is itself encrypted).
8. The Encrypted SSD will be provided to the PI (**Dr. Arthur Curry**) to serve as a backup of the original data. The SSD will be stored in a locked location (e.g., desk drawer or safe in the PI's office), and the encryption key will be kept in a locked location separate from the SSD.
9. The UISL will escrow the encryption key for the SSD in a secure password management system. Should the data need to be decrypted in the future (e.g., in the case of a failure of the secured analysis computer), the PI may contact the UISL to perform the decryption.

Operational Use of Secured Analysis Computer

Operational Use of Secured Analysis Computer

- **Dedicated Infrastructure**: The **Standalone Linux Workstation** is dedicated exclusively to the processing of **Export Controlled** information for **Project Poseidon: Mapping the Mid-Atlantic Ridge**. To maintain the security of Controlled Unclassified Information (CUI), this workstation must remain air-gapped with **no active internet connection**.
- **Secure Transfer Media**: A FIPS 140-2 compliant **Encrypted SSD** (distinct from the media used for system backups) will be provisioned for project use. This Encrypted SSD is the **sole authorized method** to transfer data to or from the secured analysis computer.
- **Key Management**: Access to the encryption key or passphrase for the Encrypted SSD is restricted strictly to the **Principal Investigator (Dr. Arthur Curry)** and approved researchers listed in this Data Security Plan.
- **Data Egress (Output)**: Only **aggregated data** or **analysis results** that do not contain raw Export Controlled information may be copied from the secured analysis computer to the Encrypted SSD for transfer to other systems.
- **Data Ingress (Input)**: Only statistical analysis scripts or code intended for use in one of the **Approved Applications** may be copied from other computers to the Encrypted SSD for transfer to the secured analysis computer.

- **Prohibited Files**: No other data sets, applications, executables, documents, or files other than those noted above will be copied to or from the secured analysis computer.
- **Operational Exceptions**: Any operational need to remove un-aggregated, identifiable, or raw Export Controlled data from the secured analysis computer must be approved in advance and in writing by the **PI** and the **Unit Information Security Lead (Mera)**.

Cyclical Security Review

At least once every three months, Department of Oceanography IT Service Provider personnel, under the supervision of the UISL, will perform a security review and maintenance on the standalone Linux workstation dedicated to **Project Poseidon**. This review ensures ongoing compliance with NIST 800-171 and CMMC standards required for Export Controlled and CUI data.

The maintenance will be tracked as an Incident record in the designated ITS ticketing system (e.g., ServiceNow), including a completed checklist of the following required actions:

- **Offline Patch Management:** Due to the air-gapped configuration required for Export Controlled data, the workstation **will not** be connected to any network. Security patches, OS updates, and antivirus definitions will be transferred and applied manually using authorized, virus-scanned encrypted SSDs.
- **Log Review:** All system, application, and security logs (e.g., `/var/log/audit/audit.log`, `/var/log/secure`, or `/var/log/auth.log`) collected since the previous maintenance window will be reviewed for anomalies. Specific attention will be paid to failed login attempts, privilege escalation (sudo usage), and file access events.
- **Peripheral Auditing:** System logs will be analyzed to verify that only the authorized Encrypted SSDs have been connected to the workstation. Any connection of unapproved USB devices or peripherals will be flagged.
- **Account Verification:** The local user list will be audited to ensure only the Principal Investigator and approved researchers listed in this plan have active accounts. Inactive accounts will be disabled or removed.
- **File Integrity:** File system audit logs for directories containing CUI will be reviewed to verify that permissions remain restricted to authorized personnel.

Any deviations from the configuration specified in this plan, evidence of unapproved peripheral connections, or anomalies identified in the logs will be reported immediately to the PI (Dr.

Arthur Curry) and the UISL (Mera). The UISL will determine required remediation and escalate any suspected security incident or breach to the Information Security Office (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 **Atlantis Marine Institute**, including any term extensions to the original agreement approved by the **Atlantis Marine Institute**, the data will be securely deleted from UC Riverside systems.

- The local storage on the **Standalone Workstation (Linux)** will be fully erased using a tool meeting the **DoD 5220.22-M** (seven random overwrite passes) standard (e.g., `shred` or equivalent).
- The **Encrypted SSD** used for data transfer will be fully erased using a tool meeting the **DoD 5220.22-M** (seven random overwrite passes) standard.
- Any encryption keys or passphrases associated with the project data will be securely purged to render all secured data unrecoverable.
- A Certificate of Sanitization or equivalent log will be generated and retained to verify compliance with NIST 800-171 media sanitization requirements for Controlled Unclassified Information (CUI).

Security Plan Review

- **Annual Compliance Review:** This plan will be reviewed at least annually by the Principal Investigator (Dr. Arthur Curry) and the Unit Information Security Lead (Mera) to verify continued compliance with Export Control regulations, NIST 800-171 standards, and Atlantis Marine Institute requirements.
- **Risk Management:** Any newly identified risks regarding the Standalone Workstation or Encrypted SSD usage will be added to the security plan following the process defined under **Security Plan Changes**.

- **Access Control Audit:** During the review process, the PI will review the list of personnel with physical or logical access to the CUI data. The PI will ensure that access is revoked immediately for any individual who no longer requires access.

Violations of Data Security Plan

Any violations of the data security plan shall be reported immediately to the Principal Investigator (PI), Unit Information Security Lead (UISL), Unit IT Director, and Chief Information Security Officer (CISO).

Security Plan Changes

Any changes to the IT environment or policies used for processing the data will be documented; approved by the Principal Investigator (PI) and Unit Information Security Lead (UISL); and submitted to the Information Security Office (ISO) for review and approval before implementation.

Any changes to the list of researchers with access to the Project Poseidon 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 or an addendum to this plan.

Role	Name	Signature	Date
Principal Investigator	Dr. Arthur Curry		
Unit Information Security Lead (UISL)	Mera		
Chief Information Security Officer (CISO)			
Project Researcher			