

PDS (The Planetary Data System)

**Information Technology Security
Plan for The Planetary Data
System: [Node Name]**

[Date]

[Location]

IT Security Plan Template for Planetary Data System Nodes

Prepared by:

[Author]
[Title]

Date

Approved by:

[Name]
[Title]

Date

IT Security Plan Template for Planetary Data System Nodes

Change Log

Revision	Date	Sections Changed	Author

Contents

1. Introduction.....	6
1.1 Overview.....	6
1.2 Document Scope.....	7
2. Referenced Documents.....	8
2.1 Controlling Documents.....	8
2.2 Applicable Documents.....	8
3. System Identification.....	8
3.1 Responsibilities.....	8
3.2 Title.....	8
3.3 Operational Status.....	8
3.4 General Description.....	8
3.5 Information Contacts.....	8
4. Information Identification.....	9
4.1 Information Processed.....	9
4.2 FIPS 199 Category.....	9
4.3 Applicable Laws, Policies, and Guidance.....	9
4.4 Loss of System and Data Impact.....	9
4.5 System Value.....	9
5. Information Sharing.....	9
6. Risk Assessment and Analysis.....	9
7. Technical Controls.....	10
8. Public Access Controls.....	10
9. Rules of the System.....	10
9.1 Obtaining a User Account.....	10
9.2 Remote Access.....	10
9.3 User Authentication, Privileges, and Limitations.....	10
9.4 Process for Restoring Service.....	11
9.5 Process for Escorting Personnel.....	11
9.6 Consequences.....	11
10. Personnel Screening.....	11
11. Training.....	11
11.1 Rules of the System.....	11
11.2 Responsibilities.....	11
11.3 Detection and Response.....	11
11.4 Getting Help.....	11
11.5 Center Policies, Procedures, and Guidelines.....	11
12. Contingency Planning.....	12
13. Incident Response.....	12
14. System Interconnection.....	12
15. Review of Security Controls.....	12

IT Security Plan Template for Planetary Data System Nodes

16. Authorization to Process	12
Appendix A	13
Appendix B – System Inventory and Diagrams	14
1. Inventory	14

1. Introduction

1.1 Overview

The Planetary Data System (PDS) includes a federation of geographically distributed Discipline Nodes. Each Discipline Node maintains a data and computing infrastructure to support online archive operations and to provide data distribution services for public access to the archive of scientific data products resulting from NASA planetary missions. Figure 1 shows the organization of the PDS nodes.

This document provides a specific Information Technology Security Plan for the [PDS Node Name]. It covers the IT Security practices at the Discipline Node. This includes the following:

- Identification of systems – this includes systems in the enterprise.
- The information within systems and its classification – this includes the information managed within systems and their risk level should systems be impacted based on the FIPS 199 classification.
- Information sharing with external users – This identifies what and how data is shared externally.
- Risk management – This includes identified risks including known vulnerabilities.
- Technical IT security controls – This includes controls that are in place to mitigate risk to systems. An example set of security controls is identified in Appendix A.
- Public access controls – These are controls that are in place to protect the system from unauthorized public access.
- Personnel screening - These are processes in place to screen potential users of the systems including granting of user accounts on systems.
- Training – These are processes and rules in place to train users on IT security practices.
- Contingency Planning – These are plans and processes for system recovery should it be required do to a disaster situation.
- System Interconnection – These identify the connections between other systems,

IT Security Plan Template for Planetary Data System Nodes

both internally and externally.

- Review of IT Security Controls – This identifies the procedures used to review and audit the IT security controls to ensure compliance.

A separate IT Security plan is maintained by the Engineering Node which includes a compilation of the individual IT Security Plans plus an overall plan for the federation.

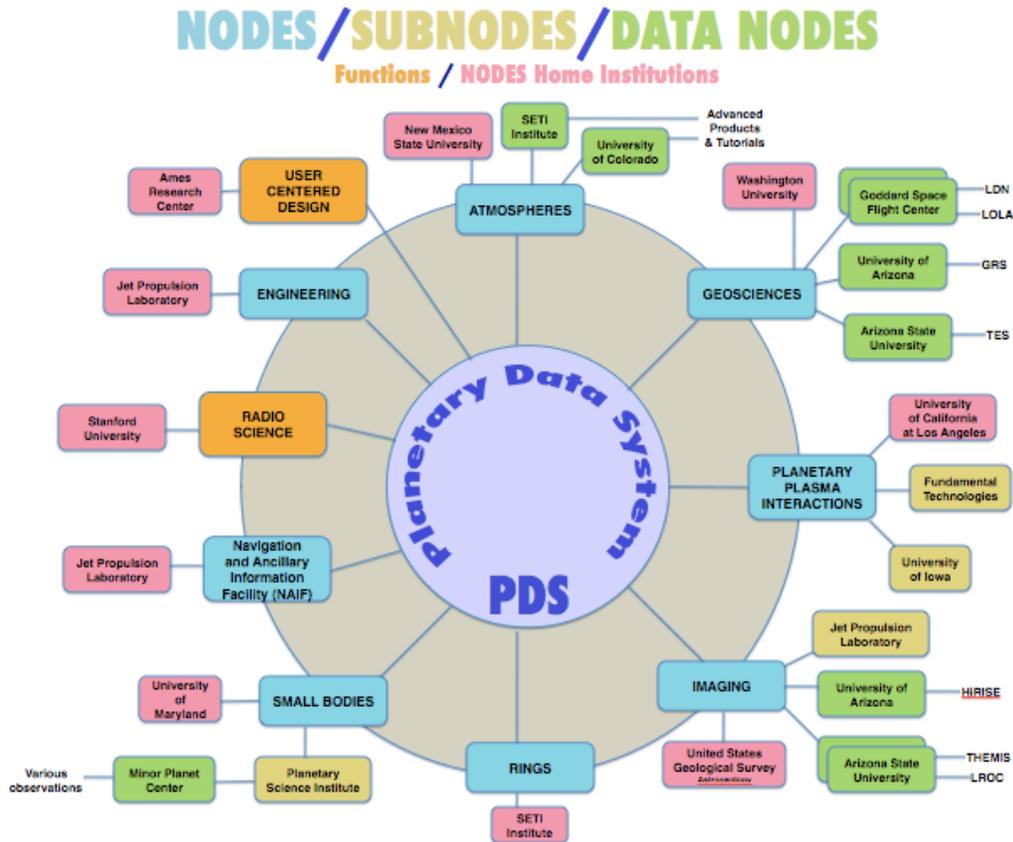


Figure 1: PDS Node Organization

1.2 Document Scope

This document is the Information Technology Security Plan for the PDS node [insert node name]. The remaining PDS nodes are covered by separate plans. The relationship between these plans is described in [Central PDS Plan]. Each of these individual security plans identifies system risks, technical controls, contingency plans, and primary contact information for the local node computing equipment.

2. Referenced Documents

2.1 Controlling Documents

[1] [Any related grant/contract requirements]

2.2 Applicable Documents

[1] [*If applicable, NIST Special Publication 800-53, Revision 3, 05/2010*]

[2] [*Central Plan name*]

[3] [*Any relating Interconnection Security Agreement's*]

3. System Identification

3.1 Responsibilities

[Describe who is responsible for the PDS Node including who is responsible for authorizing the security plan]

3.2 Title

The commonly used name for the equipment covered under this plan is [Name of the Node and/or Computing environment]

3.3 Operational Status

[Describe the operational status of the equipment. For example, is it operational, in development, or a mix of both. Describe the time periods when the equipment is operational, for example if it is available 24/7.]

3.4 General Description

[Provide an overview of the system including what it is used for, what type of users will access the system, what software is utilized or developed on the system, and how it is connected to the network. Diagrams, both for data flow and network, can be included here.]

3.5 Information Contacts

Name	Title	Phone	Email

--	--	--	--

4. Information Identification

4.1 Information Processed

The PDS [Node name] system will [Describe what the information is on the system and how the PDS node will process it]

4.2 (Federal Information Processing Standard (FIPS) 199 Category

FIPS Publication 199 defines three levels of potential impact on an organization or individuals should there be a breach of security. Following these standards, the PDS [Node name] system is classified as a [Low (L), Moderate (M), High (H)] impact system.

4.3 Applicable Laws, Policies, and Guidance

The PDS [node name] computing systems follow the [institutional and/or NASA] guidelines described in [institutional requirements and/or (NASA Procedural Requirements (NPR) 2810.1]

4.4 Loss of System and Data Impact

[Describe the impact if the Node experiences a loss of software, hardware, or network connectivity.]

4.5 System Value

[Describe the cost of replacing the system]

5. Information Sharing

[If applicable, describe how the information held on the system is shared with external entities.]

6. Risk Assessment and Analysis

6.1 Summary of Risk Assessment Findings

The results of the current risk assessment for the PDS [Node name], indicate that the level residual risk to this system is acceptable. The security planning process ensures that security controls are selected and addressed appropriate to the value of the information on the system, and that residual risk is further mitigated by contingency planning. Any remaining known vulnerabilities have been noted, and the plan of actions and milestones (POA&M) toward correction have been identified

6.2 Results of Risk Analysis

Threat sources and potential impacts to the PDS [node name] system are both IT-specific and physical.

Known vulnerabilities are addressed by implementing the protective measures documented in Appendix A and are continually addressed through quarterly and self-initiated vulnerability scans along with a review of protective measures.

The conclusion of this system-specific risk analysis is that the level of residual risk for the PDS [node name] is acceptable.

7. Technical Controls

Appendix A contains the technical controls that respond to the requirements and the risk assessment. These include the technical controls that enforce the rules or policies of the system.

8. Public Access Controls

[Describe how the system is protected from public access]

9. Rules of the System

All users of the PDS [node name] computing equipment must take required security training. Training is available at [node security training program].

9.1 Obtaining a User Account

[Describe how accounts are requested, approved, and how the passwords are disseminated.]

9.2 Remote Access

[If applicable, describe how remote access is granted.]

9.3 User Authentication, Privileges, and Limitations

[Describe rules relating to user authentication and privileges. For example, “When authenticating a user, the systems will not display the passwords in clear text. All system passwords are encrypted when stored and are restricted from the user’s view. Users are not permitted to include passwords in scripts or programs.

The System Administrator sets the privileges and limitations for the user accounts within this system.

In the event of a security or system failure, a user’s privileges may be revoked while the user is active on the system. In this case, the System Administrator will attempt to

contact the user before any changes are made so that the user can gracefully log off. A contact list with at least two methods of communication has been established for this purpose and is posted at”]

9.4 Process for Restoring Service

Procedures for restoring service after system crashes or unplanned outages are outlined in the *[Contingency plan name]*.

9.5 Process for Escorting Personnel

[If applicable, describe process for escorting personnel to access equipment physically.]

9.6 Consequences

[Describe the consequences of users not abiding by the security rules of the system per their training.]

10. Personnel Screening

Users are granted privileges as necessary for the performance of their job within this system. The number of privileged users who can bypass security and process controls is [x].

11. Training

11.1 Rules of the System

[Describe how users are trained on the rules of the system.]

11.2 Responsibilities

[Describe who is responsible for completing training.]

11.3 Detection and Response

[Describe how users are trained on detection and response of security incidents.]

11.4 Getting Help

[Describe how users are trained to request help.]

11.5 Center Policies, Procedures, and Guidelines

[Describe any related training required by the Node facility]

12. Contingency Planning

Plans and procedures for continuing PDS [Node name] operations after a natural or human-caused disaster can be found in the *[Contingency Plan name]*. *Contingency Plans* are managed in a separate plan and delivered to the PDS Management Node at Goddard Space Flight Center. These plans are available, should it be requested.

13. Incident Response

[Describe who should be notified in the case of a security incident.]

14. System Interconnection

[Describe how this system connects to others both at the facility and within PDS. Include any related diagrams.]

15. Review of Security Controls

[Describe how the IT system is audited and what is done with the results of the audit. For example “IT Systems are subject to independent audit to verify that the planned controls have been implemented and are effective. Within the PDS [Node name] system, verification is composed of three parts:

- Quarterly network scans for vulnerabilities conducted by [who will perform the scan]
- on-site examination of configuration settings and other system information by an auditor/System Administrator; and
- on-site inspection of remaining controls, such as physical security, password dissemination procedures, etc., by a field auditor.

Any problems found during an audit, that cannot be immediately corrected become audit findings. All findings are reviewed by [Security group name]. Valid findings will result in problem tickets being created; tickets must be closed (fixed, waived, or have a lien) within the prescribed time specified on the ticket. Corrective actions taken in response to a ticket are verified by [Security group name] before the associated ticket is closed. Vulnerabilities discovered by network scans are first reviewed by [Security group name] for validity. “]

16. Authorization to Process

By signing the approval page of this document, the PDS [Node name] Managers and Systems Engineer state that this plan adequately secures the system, its data, and its operation.

Appendix A

Technical Controls – [NOTE: Discipline Nodes should identify their own technical controls.]

Unique ID	Requirement Text
1	
2	
3	
4	
5	
6	
7	
...etc	

Appendix B – System Inventory and Diagrams

1. Inventory

1.1 Hardware

[Include hardware list]

1.2 Software

[Include software list]