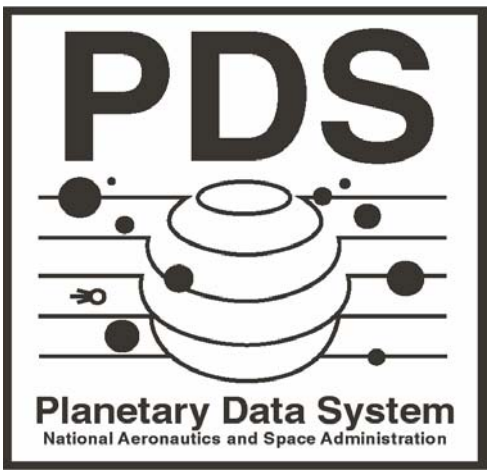
Planetary Data System

Archive Integrity Requirements: Archive Data Integrity, Tracking and Availability

DRAFT

September 20, 2007

Version 0.10070920



JPL

Jet Propulsion Laboratory
Pasadena, California

JPL D-xxxxx

CHANGE LOG

Revision	Date	Description	Author
Start Draft	2007-08-29	First Draft of Combined Documents	S. Hughes
0.10070829	2007-09-04	EN Review of document	D. Crichton, R. Joyner, S. Hughes
0.10070920	2007-09-20	WG Review of document	M. Gordon, E. Guninness, S. Hughes

Table of Contents

1 Introduction

At the meeting in Nov/2006, the Management Council adopted a policy to ensure the integrity of the PDS archive as follows:

Each node is responsible for periodically verifying the integrity of its archival holdings based on a schedule approved by the Management Council. Verification includes confirming that all files are accounted for, are not corrupted, and can be accessed regardless of the medium on which they are stored. Each node will report on its verification to the PDS Program Manager, who will report the results to the Management Council.

The purpose of this document is to document the combined requirements, based on this policy, which describe how the PDS addresses the integrity, tracking and availability of its data holdings. This encompasses three areas.

1) Data integrity addresses file corruption during the preservation and transfer of data to and from PDS.

2) Data tracking focuses on tracking the status of data from its delivery by the data providers through the PDS to the deep archive, NSSDC (PDS Requirement 2.2.2). Tracking is differentiated into delivery tracking, primarily tracking data from the data provider to the PDS and archive tracking, the tracking of data within the PDS archive. The archive tracking function includes making an inventory of all files and ensuring that all files archived by the PDS are accounted for and available to the community. Within the PDS, files are components of collections. These collections include data products, data deliveries and data sets.

3) Data availability addresses the availability of its data holdings. This encompasses the need for backups in the case of "disaster recovery" (PDS Requirement 4.1.4) or simple data loss and the need for "continuous operations" (PDS Requirement 2.10.1).

Chapters 6, 7 and 8 address requirements for each of the above three areas. They are based on policies, the PDS Level 3 Requirements, and use cases which were individually developed by each of the above areas.

1.1 Controlling Documents

[1] Planetary Data System (PDS) Level 1, 2 and 3 Requirements, May 26, 2006.

1.2 Applicable Documents

[2] Planetary Data System Data Integrity Use Cases, DRAFT, Sep 05, 2006, Version 0.10060926.

[3] Planetary Data System Archive and Delivery Tracking Use Cases, DRAFT, January 29, 2007, Version 0.10070129.

[4] Planetary Data System Archive Data Availability Use Cases, DRAFT, July 31, 2007, Version 0.10070731.

[5] Planetary Data System Engineering Node Mirror documentation. http://pds-engineering.jpl.nasa.gov

1.3 Document Maintenance

This document and the use cases specified herein will be kept under configuration control by the PDS Engineering Node.

2 Definitions

The following definitions are used in the requirements.

1. **Acceptance Status** – A status indicating whether a data delivery has been accepted.
2. **Actors** - An actor is a person, organization, or external system that plays a role in one or more interactions with your system
3. **Archive Manifest** – An archive manifest is a list of files contained in a repository. The information for each file should include at least filename, file checksum, and the checksum type. The list of files should includes at least those that comprise data sets that have a status indicating the data set has passed peer review or is being saved long-term.
4. **Authorized Actor** – An actor who has been approved to be informed of actions by the system. For tracking system notification, authorized actors are a subset of tracking system actors that have been specifically authorized to be informed of specific actions by the system.
5. **Data Consumer -** Entities that receive data from PDS.
6. **Data Product** – A data product label and one or more data objects.
7. **Data Product Label** – One or more data object descriptions.
8. **Data Set** – A data set is a set of data products collected for a specific purpose and all related ancillary data and documentation.
9. **Delivery Manifest** – The delivery manifest is a list of files in a delivery. The information for each file should include at least the file name, the file checksum, and the checksum type.
10. **Delivery Status –** A status indicating whether a data delivery has been successfully transferred.
11. **File** – A collection of bytes stored as a single unit within a file system.
12. **Manifest** - A manifest is a list of items. For the purpose of tracking, the manifest is a list of files and will include at a minimum the filenames, checksum, and checksum type. (See Archive Manifest and Delivery Manifest).
13. **Product Collection** – A product collection is a set of data products collected for a specific purpose.
14. **PDS Node** – Any PDS node including Discipline Nodes, Data Nodes, and the Engineering Node. The Discipline Nodes include both science and support nodes.
15. **PDS Resource –** A PDS Resource is any web resource, accessible via http protocol, that has been ingested into the PDS main catalog Resource tables. Information required for each resource includes an identifier, name, type, description, URL, and associated data sets.
16. **Physical Media –** Any computer system device used for short or long term storage of data including but not limited to optical media, tape, and magnetic disk.

17. **Primary Repository -** A primary repository is the principal location for a Node's data holdings. Primary repositories are managed by the PDS Discipline Nodes and maybe online or offline.
18. **Repository Inventory –** The repository inventory is a list of primary and secondary repositories that contain PDS data sets. Each data set that is to be made available for online access must be resident in a primary repository and should be resident in a secondary repository. Note that the inverse, the primary and secondary repositories for each data set is also maintained.
19. **Secondary Repository -** A secondary repository contains a copy of a Node's primary repository. This may be online or offline.
20. **Tertiary Repository –** A deep archive provides long term preservation of a data holding
21. **Use cases**. A use case describes a sequence of actions that provide something of measurable value to an actor.
22. **Volume** – Any organized collection of files that reside on physical media for the purpose of near term storage, online access, data submission, electronic distribution, or long-term archive. Note that this definition includes the PDS archive volume.

3 Applicable PDS Policies

1. Archive Integrity Policy (November 2006)

The following policy, adopted by the Management Council (MC), addresses how the PDS will protect the integrity of its holdings:

Each node is responsible for periodically verifying the integrity of its archival holdings based on a schedule approved by the Management Council. Verification includes confirming that all files are accounted for, are not corrupted, and can be accessed regardless of the medium on which they are stored. Each node will report on its verification to the PDS Program Manager, who will report the results to the Management Council.

2. Data Delivery Policy (October 2005)

The following policy, adopted by the Management Council (MC), addresses the data deliveries to PDS and their management:

Data producers shall deliver one copy of each archival volume to the appropriate Discipline Node using means/media that are mutually acceptable to the two parties. The Discipline Node shall declare the volume delivery complete when the contents have been validated against PDS Standards and the transfer has been certified error free.

The receiving Discipline Node is then responsible for ensuring that three copies of the volume are preserved within PDS. Several options for "local back-up" are allowed including use of RAID or other fault tolerant storage, a copy on separate backup media at the Discipline Node, or a separate copy elsewhere within PDS. The third copy is delivered to the deep archive at NSSDC by means/media that are mutually acceptable to the two parties.

3. Backup and Recovery Policy (November 2006)

Each node is responsible for defining and implementing a disaster recovery plan which covers loss of data and/or system functionality within guidelines provided by the Management Council. The plan shall be delivered to and approved by the PDS Program Manager.

4 PDS Level 3 Requirements

The following Level 3 requirements were used to derive the level 4 requirements in this document.

2.2.2 PDS will track the status of data deliveries from data providers through the PDS to the deep archive

2.5.1 PDS will develop and publish procedures for accepting archival data

2.5.2 PDS will implement procedures for accepting archival data

2.5.3 PDS will inform a data provider why a rejected archival product does not meet archiving standards

2.6.2 PDS will maintain appropriate storage for the PDS archive

2.6.3 PDS will integrate the catalog with the system for tracking data throughout the PDS

2.8.1 PDS will maintain a distributed archive where holdings are maintained by Discipline Nodes, specializing in subsets of planetary science

2.9.1 PDS will accept and distribute only those items which are not restricted by the International Traffic in Arms Regulations (ITAR)

2.10.1 PDS will monitor the system and ensure continuous operation

3.2.3 PDS will provide mechanisms to ensure that data have been transferred intact. (Note that 3.2.1 and 3.2.2 specify that mechanisms must be available to transfer data to users both online and offline.)

3.3.6 PDS will develop and maintain a mechanism for notifying subscribed users when a data set is released or updated.

4.1.2 PDS will develop and implement procedures for periodically ensuring the integrity of the data

4.1.3 PDS will develop and implement procedures for periodically refreshing the data by updating the underlying storage technology.

4.1.5 PDS will meet U.S. federal regulations for preservation and management of the data through its Memorandum of Understanding (MOU) with the National Space Science Data Center (NSSDC)

5 Notation

The numbering of the requirements in this document will be formatted as **Ln.AA.BB.N**, where:

- **Ln** indicates the requirement level number.
- **AA** is an acronym representing the requirement category:
  - **DI –** Data Integrity
  - **DT –** Delivery Tracking
  - **AT –** Archive Tracking
  - **AV –** Data Availability
- **BB** is a two letter acronym for the requirement subcategory. (Optional)
- **N** is a unique number for the requirement.

Following the text of a requirement may be a reference to the requirement from which it was derived. The reference will be in parenthesis.

A paragraph following a requirement, which is indented and has a reduced font size, represents a comment that provides additional insight for the requirement. This comment should not be considered part of the requirement for development or testing purposes.

6 Data Integrity Level 4 Requirements

This section details the level 4 requirements for Data Integrity. These requirements are derived directly from the level 3 requirements [1] and the associated Data Integrity Use Cases [2].

L4.DI.1- PDS will only accept data files that are not corrupted. (2.5.1, UC-1)

L4.DI.2 - PDS will provide procedures for verifying that a data submission has not been corrupted. (2.5.1, UC-1)

L4.DI.3 - PDS will ensure that a *PDS Data Node* verifies their data submissions are not corrupted prior to submission to a PDS Node. (2.5.2, UC-4)

L4.DI.4 - PDS will ensure that archival data to be delivered between *PDS Discipline Nodes* has not been corrupted prior to transfer (2.5.2, UC-8)

L4.DI.5 - PDS will ensure that data submitted from a data provider have not been corrupted (2.5.2, UC-1)

L4.DI.6 - PDS will ensure that data submitted from a *PDS Data Node* have not been corrupted (2.5.2, UC-4)

L4.DI.7 - PDS will ensure that archival data transferred between *PDS Discipline Nodes* have not been corrupted (2.5.2, UC-8)

L4.DI.8 - PDS will require a data provider, *PDS Data Node*, or *PDS Discipline Node* to resubmit data that have been corrupted during transfer (2.5.3, UC-1, UC-4, UC-8)

L4.DI.9 - PDS will ensure that a user receiving data from the PDS can verify the data have been successfully transferred (3.2.3, UC-2)

L4.DI.10 - PDS will periodically verify that data holdings have not been corrupted based on a schedule determined by the PDS Management Council (4.1.2, UC-5)

L4.DI.11 - PDS will verify that data holdings are not corrupted prior to migrating to another medium (4.1.3, UC-6)

L4.DI.12 - PDS will ensure that data migrated from one medium to another have been successfully migrated and not corrupted during the transfer (4.1.3, UC-6)

L4.DI.13 - PDS will ensure that the archival data holdings, to be submitted to the deep archive (NSSDC) for preservation, are not corrupted (4.1.5, UC-3)

L4.DI.14 - PDS will request the deep archive (NSSDC) verify that the archival data holdings submitted to the NSSDC have been received intact (4.1.5, UC-3)

L4.DI.15 - PDS will request the deep archive (NSSDC) verify that the archival data holdings recovered from the NSSDC are not corrupted (4.1.5, UC-7)

L4.DI.16 - PDS will ensure that the archival data holdings received from the deep archive (NSSDC) are not corrupted (4.1.5, UC-7)

7 Tracking Level 4 Requirements

Data tracking focuses on tracking the status of data from its delivery by the data providers through the PDS to the deep archive, NSSDC. Tracking is differentiated into delivery tracking, primarily tracking data from the data provider to the PDS and archive tracking, the tracking of data within the PDS archive.

The following requirements are for data tracking within the PDS. They are derived directly from the PDS Level 3 requirements [1] and the Archive and Delivery Tracking Use Cases [3].

7.1 Delivery Tracking Requirements

Delivery tracking encompasses the process of tracking files associated with data deliveries from any data provider through to the acceptance of the data by a PDS Node. These requirements are on the data tracking system, a subsystem that tracks data delivery events and their statuses. An important feature suggested by these requirements allows for data deliveries to be successfully transferred to but not necessarily accepted by a PDS node until reviewed. This "escrow" feature ensures that only data deliveries that meet certain criteria are actually accepted. These requirements are derived from level one, two, and three PDS requirements, PDS Tracking Use Cases, and PDS Policies.

7.1.1 General (GR)

L4.DT.GR.1 – The Delivery Tracking System shall track the contents of a data delivery identifying each file associated with a delivery (UC-1.2, 2.2.2)

L4.DT.GR.2 – The Delivery Tracking System shall allow verification that the contents of a data delivery package matches its delivery manifest by checking that every file listed in the manifest is in the package and vice versa. (2.2.2)

L4.DT.GR.3 – The Delivery Tracking System shall notify actors about events including scheduled events associated with deliveries and any change in delivery or acceptance statuses. (3.3.6)

> **The PDS Notification/Subscription system could be extended to fulfill this requirement. The notification of an actor will be triggered by an event. Various requirements in the following sections will signal events. The delivery plan will provide a list of actors to be notified for specific events. The subset of "authorized" actors will also be provided in the delivery plan.**

L4.DT.GR.4 – The Delivery Tracking System shall allow authorized actors to set the tracking system statuses. (UC-1.2)

L4.DT.GR.5 – The Delivery Tracking System shall allow the generation of reports detailing the statuses of past and projected future data delivery events. (UC-4, UC-5, 2.2.2)

7.1.2 Data Provider Delivers Data (DP)

L4.DT.DP.1 – The Delivery Tracking System shall track data delivery events and their statuses based on a negotiated delivery plan between a data provider and a PDS Node. (UC-1.3, UC-6, 2.2.2, 2.6.2, 2.9.1)

> **Possible data delivery events include Delivery to PDS, and Acceptance by PDS. Each delivery event can have one or more event statuses which are captured by respectively, Delivery_Status and Acceptance_Status. On integration with the PDS Notification system, these delivery events will be added to the already existing Release and Archive events.**

L4.DT.DP.2 – The Delivery Tracking System shall be configured based on a data delivery plan that has been negotiated between a Data Provider and a PDS Node. (UC-1.1, 2.2.2)

L4.DT.DP.3 – The Delivery Tracking System shall maintain the delivery status of a data delivery from a Data Provider to a PDS Node. (UC-1.2, 2.2.2)

L4.DT.DP.4 – The Delivery Tracking System shall be able to signal an event to notify authorized actors of a change in the delivery status. (UC-6, 2.2.2)

L4.DT.DP.5 – The Delivery Tracking System shall allow a PDS Node to accept, reject or mark as incomplete a data delivery depending on whether the delivery is acceptable according to negotiated delivery parameters. (2.2.2)

L4.DT.DP.6 – The Delivery Tracking System shall be able to signal an event to notify authorized actors of a change in a data delivery's acceptance status. (UC-6, 2.2.2)

L4.DT.DP.7 – The Delivery Tracking System shall allow the withdrawal of a data delivery. (2.2.2)

> **The assumption is that the data provider will re-submit the data delivery later.**

7.1.3 Data Node Termination (NT)

L4.DT. NT.1 – The Delivery Tracking System shall support the dissolution of a Data Node and the transfer of the Data Note's holdings to a permanent PDS Node. (UC-3, 2.2.2)

> **The requirements in section 5.2 apply after the Data Node assumes the role of Data Provider.**

7.2 Archive Tracking Requirements

The following requirements are for archive tracking. In this document, "archive tracking" encompasses the tracking of data holdings in the PDS archive and are levied on the PDS to track data files, data products, data volumes, and data sets from the acceptance of the data at a PDS Node through to the submission of the data to the NSSDC. These requirements are on the PDS to track the files in the archive as a whole, spanning all nodes. An important feature suggested by these requirements allows for data deliveries to be successfully transferred to but not necessarily accepted by the NSSDC until reviewed. This "escrow" feature is implemented implicitly by differentiating between the transfer to and acceptance of a package by the NSSDC. In other words, a delivery can be successfully transferred but not necessarily accepted until the NSSDC has ensured that the delivery meets certain criteria. These requirements are derived from level one, two, and three PDS requirements, PDS Tracking Use Cases, and PDS Policies.

7.2.1 General (GR)

L4.AT.GR.1 – The PDS shall be able to provide an accounting of all files in the archive (PDS Policy, 2.2.2 - see Policies Section)

L4.AT.GR.2 – The PDS shall be able to verify that all files in the archive are accessible. (4.1.1)

L4.AT.GR.3 – PDS shall preserve information required to verify the original file delivered to PDS node has not been corrupted. (4.1.1)

> **A possible implementation would be maintaining the original checksum value for each file and using that value throughout the end-to-end system.**
>
> **Several Data Integrity requirements are also related including L4.DI.3, L4.DI.4, L4.DI.5, L4.DI.6, L4.DI.7, L4.DI.9, L4.DI.10, L4.DI.11, L4.DI.12, L4.DI.13, L4.DI.16).**

L4.AT.GR.4 – The PDS shall maintain status and location information for each data set and volume in the archive in a common catalog. (2.2.2, 2.6.3).

The PDS Catalog tracks data collections including data sets, volumes, and data deliveries. Specific information beyond data collection information to be tracked includes the curating_node_id, distribution_node_id, backup_node_id, archive_status, acceptance_status, delivery_status, nssdc_id, etc.

L4.AT.GR.5 – The PDS shall notify actors about events including scheduled events associated with deliveries within or from the PDS archive and any change in delivery or acceptance statuses. (3.3.6)

This requirement focuses primarily on the NSSDC interface. The PDS Notification/Subscription system could be extended to fulfill this requirement. The notification of an actor will be triggered by an event. Various requirements in the following sections will signal events. The delivery plan will provide a list of actors to be notified for specific events. The subset of "authorized" actors will also be provided in the delivery plan.

7.2.2 Data Transfer between PDS Nodes (TR)

L4.AT.TR.1 – The PDS shall be able to track the transfer of files from one PDS Node archive repository to another (2.2.2, 2.6.3).

7.2.3 Preservation of Data at NSSDC (NS)

L4.AT.NS.1 – The PDS shall be able to track the transfer of a data set from a PDS Node to the NSSDC for long term preservation. (UC-3, 2.2.2, 2.9.1)

Possible data delivery events include Transfer to NSSDC. Each delivery event can have one or more event statuses which are captured by the NSSDC_Transfer_Status. On integration with the PDS Notification system, these delivery events will be added to the already existing Release and Archive events.

A related Data Integrity requirement is L4.DI.14.

7.2.4 Data Inventory Reporting (IR)

L4.AT.IR.1 – The tracking system shall generate reports on its data holdings including the location, status, and integrity of data deliveries, data volumes, data sets, data products and their associated files. These reports shall be generated periodically according to applicable PDS policies and also be available for generation on demand. (DI UC-6, 2.2.2, 2.6.3, PDS Policy, 2.2.2 - see Policies Section)

8 Data Availability Level 4 Requirements

The following requirements for data availability are derived from the PDS Level 3 Requirements [1] and the Data Availability Use Cases [4]. *Data availability* addresses only PDS archive repositories and not the underlying software systems provided by the nodes for distributing the data from the repositories. These repositories include the primary, secondary and tertiary repositories and involve all nodes, the NSSDC, and sites used for secondary repositories or backups. This supports the "three copy" rule that PDS imposed with the October 2005 policy on data delivery.

Availability of data is supported by two critical PDS Level 3 requirements that identify the need for "continuous operations" (2.10.1) and "disaster recovery" (4.1.4). From the perspective of providing both continuous operations and disaster recovery for the archive, the use cases described in [4] were based on several assumptions. These assumptions were reviewed by the Management Council at the August 2007 meeting. In some instances, a trade off between integrity of the archive and quality of service needs to be made. In those instances, the emphasis is on the integrity of the archive.

For the purposes of data availability, the following assumptions are made:

1) There are three copies of the archived data. For this document these copies are called a) the primary repository, b) the secondary (aka backup, mirror) repository, and c) the tertiary (aka deep archive) (source: PDS Policy on Data Delivery, October 2005).

2) The primary repository is accessible online except in a few specific instances, such as infrequently used Radio Science data sets. The secondary repository can be off-line (source: PDS Management Council discussion, August 2007).

3) For disaster recovery such as a major earthquake in Southern California or St. Louis Missouri, at least two of the repositories must be at more than one geographically distinct location (source: various PDS Management Council discussions)

4) As per PDS policy, each PDS Node is to develop a disaster recovery plan to be submitted to and approved by the PDS management council. In this plan, the perceived risks and types of disasters will be documented and solutions appropriate to the individual node, including the rationale for the choice of geographically distinct locations for each repository, will be provided (source: PDS policy on backup and recovery).

5) As per PDS requirements (4.1.5) the PDS places a copy of its data holdings into the NSSDC to meet U.S. Federal regulations for the preservation of data. It is assumed that NSSDC

policies and procedures ensure the long-term preservation of data consistent with U.S. Federal regulations, allow for the recovery of data from its repositories, and are committed to supporting a recovery interface with the PDS. The NSSDC is to have a tertiary (deep archive) copy of the data. It is also assumed that the PDS Management Council will want the recovery interface tested.

6) The concept of "continuous operations" requires that the PDS have operating requirements that strive to achieve a maximum "quality of service" (QoS) rating for its users. The following operational scenarios are provided together with their assumptions in order to provide a basis for the availability requirements.

a) Optimal Operational Scenario - It is desirable that data and services of high interest to the PDS user community are available world-wide 24x7 and experience limited downtime.

b) Routine Operational Scenario[1]

1) An on-line primary data repository at a node should never be unavailable for longer than 24 hours.

2) An off-line primary data repository at node should be able to make data available for distribution to a user within 72 hours.

3) Over weekends, holidays, or other situations where node staff are unavailable, additional delays in service may occur.

c) Loss-of-data Scenario – In case of a loss-of-data event at a node but where operational capability is not impaired, restoration of the data from a backup should occur within 1 week.

d) Catastrophic Scenario[2] - In the case of a catastrophic event at a node where there is a loss-of-data and all operational capability, the primary data repository should be available within one month at either the original or an alternate node. The level of service provided will include at least the retrieval of data files using file identifiers over simple internet and file system protocols.

Figure 1 illustrates the data availability use case scenarios associated with the primary, secondary, and tertiary repositories. If the primary repository is online, then the data is

[1] An MC member suggested the restoration of off-line data could be reduced to 24 hours and that delays from weekends/holidays could be made implicit.

[2] An MC member argued that the catastrophic recovery time should be phrased in terms of availability of funding; It was countered that funding is really a management issue and shouldn't necessarily be folded into requirements.

transferred over the internet via an electronic download. If the primary repository is offline then the data may be brought on-line and transferred or distributed using some type of physical media.

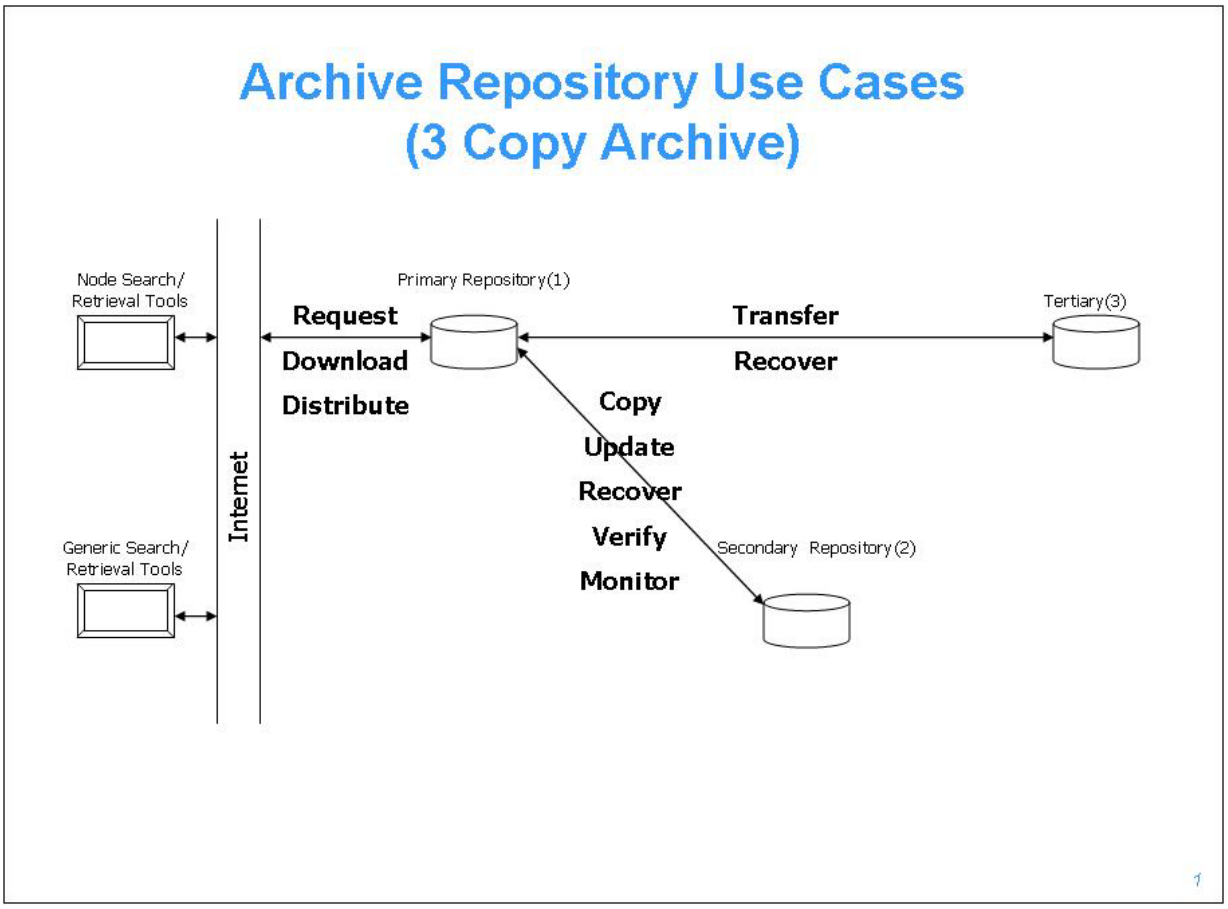


Figure 1 – Archive Repositories

The following identify the Level 4 requirements for data availability. The specific subcategories of these requirements include (General Requirement (GR), Secondary Requirement (SR), and Tertiary Requirement (TR)).

L4.AV.GR.1 – PDS shall ensure that data of high interest to the world-wide Planetary Science community has online access with minimal downtime. [2.10.1, 2.8.1]

L4.AV.SR.1 – PDS shall have a secondary copy of all archived data at one or more facilities at geographically distinct locations in order to support continuous operations. [2.10.1, UC-1]

L4.AV.SR.2 – PDS shall verify that a secondary copy of data is available for the successful recovery of data in a primary repository. [2.10.1, 4.1.2, UC-5]

Note: Level 5 requirements will address the tests necessary to ensure successful recovery including data integrity and access mechanisms.

L4.AV.SR.3 – PDS shall ensure that all secondary copies of data are synchronized[3] with their primary copies. [2.10.1, UC-2]

L4.AV.SR.4 – PDS shall maintain operational procedures for recovering files for the primary repository from the secondary copies. [4.1.4, UC-3, UC-4]

L4.AV.TR.1 – PDS shall deliver a tertiary copy of all archived data to an offsite location that meets U.S. federal regulations for preservation and management of the data.
[4.1.5]

L4.AV.TR.2 – PDS shall verify that a tertiary copy of data is available for the successful recovery of data in a primary repository. [2.10.1, 4.1.2, UC-5]

Note: Level 5 requirements will address the types of testing necessary to ensure that the recovery interface works.

L4.AV.TR.3 – PDS shall ensure that tertiary copies of data are synchronized[3] with their primary copies. [2.10.1, UC-2]

L4.AV.TR.4 – PDS shall maintain operational procedures for recovering files for the primary repository from the tertiary copies. [4.1.4, UC-3, UC-4]

[3] MC consensus is that "synchronized" copies means periodically doing spot check comparisons, including the *single* NSSDC copy, to ensure that the copies are the same and accessible. This does not require that every data set be checked within any specific time frame nor does it require that PDS delve into NSSDC backup systems. MC Meeting 8/6/07, D. Simpson.