Node Requirements

DPN
THE DIGITAL PRESERVATION NETWORK

WHAT IS A NODE?

Nodes are Service Providers and partners in the Digital Preservation Network Federation.

HOW DOES DPN WORK?

The Digital Preservation Network (DPN) serves as a preservation backbone for digital information of interest to the academy. DPN Depositors add digital assets to the Federation by working with an individual DPN Node to ingest and preserve content. This content is then replicated to other DPN Nodes, which together form a heterogeneous network of secure, trustworthy digital archives, each operated under diverse geographical, organizational, financial, and technical regimes. Robust (bit) auditing and repair functions ensure the fixity of content over time. Intellectual property agreements ensure the succession of rights to use of the content through the Federation in the event of dissolution or divestment of content by the original depositor and/or archive.

DEFINITIONS

Administrative Node: The node which serves as the primary contact with the depositor and holds responsibility for the consistency of registry entries. Only the Administrative node can make updates to the DPN registry entry for content.

Ingest Node: DPN Depositors will work directly with one or more DPN Nodes to deposit materials. This node is known as the "Ingest Node" at deposit and "Administrative Node" afterwards.

In-Scope Services: A range of services provided under contract to DPN in support of member data preservation. This includes: preservation of ingested content (ingest, bit level assurance of fixity, event monitoring, inventory reporting), replication services, registry services - including consistency and synchronization, and general system and service availability and customer response.

Replicating Node: DPN will replicate the content from the Ingest Node (see above) to other DPN Nodes, known as Replicating Nodes. Content in Replicating Nodes will be held "dark", and inaccessible except for preservation actions.

FINANCIAL CONSIDERATIONS

As a dark archive, DPN has a desire to drive down the long-term costs of preservation on behalf of its membership. Nodes are compensated on an annual basis for every TB preserved in their archive. The compensation rate is negotiated between the individual Node and DPN. Nodes may also be asked to develop custom code for use by the other Nodes in the Federation. When necessary, DPN would pay the development costs for code used by other Nodes.

Services provided to Depositors beyond the standard DPN archive service would be negotiated directly between the Node and the Depositor. These services may include format migration or transformation, access, metadata enhancement,or other value-added service provided by the Node.

SOFTWARE ENVIRONMENT

- DPN code resides in Github (https://github.com/dpn-admin)
- Nodes deploy and instantiate the DPN-Server Rails environment
  - A copy of the registry, resides in a relational database in a secure node environment
  - Synchronization events occur to provide transactional consistency in the DPN federation
- Nodes will run a client service, such as https://github.com/dpn-admin/dpn-client to access/perform services
- All access to the registry is via the API endpoints
- Any code changes or enhancements are deposited in the DPN Github repository for reuse
- Nodes will comply with the DPN Communication Architecture

OPERATIONS

- DPN nodes operate as a trusted community
  - Firewall rules are in place to allow API and Transfer access between nodes
  - Nodes will exhibit good network behavior with peers
    - port scanning is prohibited
    - nodes will practice bandwidth stewardship
- DPN production environments will coordinate installation/upgrade of DPN Server components on a timely basis
- All DPN Nodes run parallel production and pre-production environments
  - each instance has
    - auth tokens documented
    - firewall whitelists for peer nodes
    - separate transfer areas are accessible to peer nodes
  - pre-production environments
    - used for end to end testing and validation of code releases
    - experimentation with non-production evaluation of the infrastructure

DPN RESPONSIBILITIES AND/OR REQUIREMENTS

- Upon receiving notice of Content requiring Replication from an Ingestion Node, DPN will facilitate the distribution of the Content to its Replication Nodes for purposes of maintaining the copies of the Content in backed-up, Dark Storage.
- DPN will track deposits made into DPN by the Service Provider, including but not limited to: (a) checking the Content against a distributed registry; and (b) maintaining an auditable record of actions taken on Content during transmission, Storage, maintenance and Restoration sufficient to demonstrate the provenance and authenticity of replicated Content.
- DPN will assist Service Provider with capacity management based on Depositor forecasts; demand for replication services to be forecast one year in advance with quarterly review/updates.
- DPN will report to each of Service Provider's Depositors regarding the Ingestion and Replication of each Depositor's Content and its accounts. Each year during the Term, DPN will report to the Depositor: (a) when the Depositor's Content was deposited; (b) where the Depositor's Content currently resides; and (c) when the Depositor's Content was last checked.
- DPN will specify and assist with identification, packaging, transmission, Fixity Checks, preservation strategies, Replication, and Restoration of Content.
- DPN will assist Service Provider with capacity management based on Depositor forecasts; demand for replication services to be forecast one year in advance with quarterly reviews and updates.
- DPN will process any request from a Depositor requesting Restoration services and enter into a Restoration Service Agreement with such Depositor. In the event Service Provider receives a Restoration request from a Depositor, Service Provider will promptly forward such request to DPN. Upon receiving a request by DPN, Service Provider will provide Restoration services to a Depositor within a reasonable amount of time.
- DPN will notify Service Provider of any known breach of, or challenge to, the Network potentially affecting the Service Provider.
- DPN will provide timely payment for Services rendered by Service Provider.
- DPN will provide reasonable availability of DPN representative(s) when resolving a Service related incident or request.

NODE RESPONSIBILITIES AND/OR REQUIREMENTS *(Service Provider)*

- Service Provider will employ generally accepted industry practices to protect its computer networks and the Network, restricted areas of services and any databases used in the DPN services context, and operate in a secure manner to protect the integrity of the processing, transport, and Storage of Content that it holds.
- Service Provider will, in consultation with DPN, provide staff to support DPN services provided under this Agreement. DPN may reimburse Service Provider.
- Service Provider will notify DPN within twenty-four (24) hours of any loss of connection to the Network lasting more than forty-eight (48) hours or any failure of the connection to perform as expected for a high performance advanced network connection which failure lasts more than forty-eight (48) hours.
- Service Provider will notify DPN within twenty-four (24) hours of discovery of any known or suspected breach of or challenge to the Network or any Network Service security directly affecting DPN content, or any known or suspected unauthorized use of a Service Provider's facilities to access the DPN infrastructure.
- Service Provider will review and agree or collaboratively amend the technical specifications by DPN for identification, packaging, Replication, Fixity Checks, reporting, and Restoration.
- Service Provider will not overwrite, replace, or update Content without written and confirmed consent from DPN.

SERVICES

- DPN Transfer/Syncing application
  - Service Provider makes content available to other DPN Replication Nodes by programmatic calls to the DPN software.
  - Service Provider updates the DPN registry based on the status of the replication requests.
- Fixity Checks
  - Service Provider accesses the content objects via programmatic means and uses an agreed upon algorithm to verify the integrity of the content copy.
  - Service Provider updates the DPN registry based on the status of the fixity operation.
- Preservation Strategies
  - Service provider maintains a preservation environment which implements the Open Archival Information System Reference Model.
- Restoration
  - Service Provider recovers Content from DPN Nodes
  - Service Provider receives a request for Restoration from a Depositor.
  - Service Provider retrieves the identified object from its storage and makes provisions to deliver, or make accessible, to the Depositor.

SERVICE MANAGEMENT

- Service Availability. Coverage parameters specific to the Ingestion Node Service(s) are as follows:
  - Support for Service Provider: DPN will provide telephone and email support to Service Provider during "Normal Business Hours".
  - Support for Depositor: DPN will provide telephone support to Depositors within two (2) business days.
  - Service Provider will respond to Ingestion Node Service related incidents and/or requests for Restoration submitted by Depositors within the following time frames:
    - Service Provider will acknowledge request within eight (8) hours during Normal Business Hours.
    - Service Provider will communicate with the Depositor about the Services available to provide to assist with Restoration.
    - Service Provider will provide to DPN, within ten (10) working days, a plan and timeline for Restoration of Content to be returned to Depositor.

INGESTION NODE RESPONSIBILITIES AND/OR REQUIREMENTS

- Service Provider agrees to provide to Depositors:
  - Ingest Content from Depositors for purposes of preserving each Depositor's Content in Dark Storage for twenty (20) years from the date the Depositor is invoiced.
  - Before Ingesting Content of a Depositor, Service Provider must verify Depositor has entered into a Deposit Agreement with DPN. The Service Provider may add an addendum to the Deposit Agreement for each Depositor setting forth the Service Provider's reasonable service management levels.
  - Service Provider will permit each Depositor to deposit its Content at any time during effective period of the Depositor's Deposit Agreement.
  - Service Provider will Ingest Depositors' Content into the Network using DPN's BagIt specification.

REPLICATION NODE SERVICE PROVIDER RESPONSIBILITIES AND REQUIREMENTS

- Service Provider agrees to provide to Depositors the services described below:
  - Upon receiving notice from DPN of Content requiring Replication, Replication Node will make a copy of the Content to preserve in Dark Storage.
  - Service Provider will receive content from Ingestion Nodes up to the agreed number of terabytes.
  - Service Provider will accept Content from other Replication Nodes as requested by DPN.
  - Service Provider agrees to the following responsibilities and/or requirements:
    - Service Provider will obtain DPN's pre-approval regarding infrastructure purchasing costs and lead times necessary to bring new infrastructure online.
    - Service Provider will perform bit auditing and Fixity Checks on each copy of Depositors' Content no less than once every twenty-four (24) months per Content copy and will use reasonable efforts to replace corruption, errors and data loss of any of the Content by requesting an uncorrupted copy from another Replication Node in the Network.