TRAC2 Progress Overview

Go to Document Checklist

Criteria Progress

TRAC2 Criteria	Approved	Comments
3.1 Governance & Organizational Viability		
3.1.1 Mission statement	✓	
3.1.2 Preservation strategic plan	✓	
3.1.2.1 Succession, contigency, escrow plans	✓	
3.1.2.2 Monitor environment for time to deploy succession,contingency, escrow	✓	
3.1.3 Collection policy	✓	
3.2 Organizational Structure & Staffing		
3.2.1 Identified duties and appointed staff	✓	
3.2.1.1 Identified and established duties	✓	
3.2.1.2 Appropriate number of staff	✓	
3.2.1.3 Professional development program	✓	
3.3 Procedural Accountability and Preservation Policy Framework		
3.3.1 Designated community	✓	
3.3.2 Preservation policies	✓	
3.3.2.1 Review and update presevation policies	✓	
3.3.3 Documented history of changes	✓	
3.3.4 Commit to transparency	✓	
3.3.5 Information integrity measurements	✓	
3.3.6 Self-assessment and external certification	✓	
3.4 Financial Sustainability		
3.4.1 Business planning processes	✓	
3.4.2 Financial transparency, compliance, and audits	✓	
3.4.3 Risk, benefit, investment, expenditure	✓	
3.5 Contracts, Licenses, & Liabilities		
3.5.1 Contracts or deposit agreements for content	✓	
3.5.1.1 Contracts or deposit agreements for preservation rights	✓	
3.5.1.2 Completeness of agreements with depositors	✓	
3.5.1.3 Policies about preservation responsibility	✓	
3.5.1.4 Policies about liability and rights challenges	✓	
3.5.2 Track and manage property rights/restrictions	✓	
4.1 Ingest - acquisition of content		
4.1.1 Identify content information and information properties	✓	
4.1.1.1 Procedures for identifying information properties that we will preserve	✓	
4.1.1.2 Record of content information and information properties that we will preserve	✓	
4.1.2 Specify content information at deposit	✓	
4.1.3 Recognition and parsing of SIPs	✓	
4.1.4 Verify the identity of the Producer	✓	

4.1.5 Verify SIPs for completeness and correctness	✓	
4.1.6 Obtain sufficient control over digital objects	✓	
4.1.7 Provide depositor with responses	✓	
4.1.8 Records of actions and processes related to acquisition	✓	
4.2 Ingest - creation of the AIP		
4.2.1 Associated definition for each AIP or class of AIPs	✓	
4.2.1.1 Identify which definition applies to which AIP	✓	
4.2.1.2 Definition of each AIP	✓	
4.2.2 Description of how AIPs are constructed from SIPs	✓	
4.2.3 Document final disposition of all SIPs	✓	
4.2.3.1 Procedures if a SIP is not incorporated or discarded	✓	
4.2.4 Convention that generates persistent, unique identifiers for AIPs	✓	
4.2.4.1 Uniquely identify each AIP	✓	
4.2.4.1.1 Have unique indentifiers	✓	
4.2.4.1.2 Assign and maintain persistent identifiers of the AIP and its components	✓	
4.2.4.1.3 Describe any processes for changes to identifiers	✓	
4.2.4.1.4 Provide a list of all identifiers and check for duplications	✓	
4.2.4.1.5 System of identifiers is adequate now and in the future	✓	
4.2.4.2 System of reliable linking/resolution services in order to find identified objects	✓	
4.2.5 Tool and resources to provide authoritative Representation Information for all objects	✓	
4.2.5.1 Tools or methods to identify the file types of all objects	✓	
4.2.5.2 Tools or methods to determine what Representation Information is necessary for understandability	✓	
4.2.5.3 Have access to the requisite Representation Information	✓	
4.2.5.4 Tools or methods to ensure that Representation Information is persistently associated with objects	✓	
4.2.6 Documented processes for acquiring PDI for associated Content Information	✓	
4.2.6.1 Documented processes for acquiring PDI	✓	
4.2.6.2 Execute documented processes for acquiring PDI	✓	
4.2.6.3 PDI is persistently associated with Content Information of AIP	✓	
4.2.7 Content Information is understandable for Designated Community at the time of AIP creation	✓	
4.2.7.1 Processes for testing understandability for Designated Community of the Content Information of AIPs	✓	
4.2.7.2 Execute testing process of Content Information of AIPs	✓	
4.2.7.3 Bring Content Information of AIP up to level of understandabililty if it fails testing	✓	
4.2.8 Verify each AIP for completeness and correctness	✓	
4.2.9 Independent mechanism for verifying the integrity of the content	✓	
4.2.10 Contemporaneous records of actions and administration processes relevant to AIP creation	✓	
4.3 Preservation Planning		
4.3.1 Documented preservation strategies relevant to its holdings	✓	
4.3.2 Mechanisms for monitoring its preservation environment	✓	
4.3.2.1 Mechanisms for monitoring and notification when Representation Information is inadequate for the Designated Community to understand the data holdings	✓	
4.3.3 Mechanisms to change preservation plans as a result of its monitoring activities	✓	
4.3.3.1 Mechanisms for creating, identifying or gathering any extra Representation Information required	✓	
4.3.4 Provide evidence of the effectiveness of its preservation activities	✓	
4.4 AIP Preservation		

4.4.1 Specifications for how the AIPs are stored down to the bit level	✓	
4.4.1.1 Preserve the Content Information of AIPs	✓	
4.4.1.2 Actively monitor the integrity of AIPs	✓	
4.4.2 Contemporaneous records of actions and administration processes that are relevant to storage and preservation of the AIPs	✓	
4.4.2.1 Procedures for all actions taken on AIPs	✓	
4.4.2.2 Demonstrate that any actions taken on AIPs were compliant with the specification of those actions	✓	
4.5 Information Management		
4.5.1 Specify minimum information requirements to enable the Designated Community to discover and identify material	✓	
4.5.2 Capture or create minimum descriptive information for each AIP	✓	
4.5.3 Create bi-directional linkages between each AIP and its descriptive information	✓	
4.5.3.1 Maintain the bi-directional associations between its AIPs and their descriptive information over time	✓	
4.6 Access Management		
4.6.1 Comply with Access Policies	✓	
4.6.1.1 Log and review all access management failures and anomalies	✓	
4.6.2 Follow policies and procedures that enable the dissemination of digital objects that are traceable to the originals	✓	
4.6.2.1 Record and act upon problem reports about errors in data and responses from users	✓	
5.1 Technical Infrastructure Risk Management		
5.1.1 Identify and manage the risks to its preservation operations and goals associated with system infrastructure	✓	
5.1.1.1 Employ technology watches or other technology monitoring notification systems	✓	
5.1.1.1.1 Hardware technologies appropriate to the services it provides to its designated communities	✓	
5.1.1.1.2 Procedures in place to monitor and receive notifications when hardware technology changes are needed	✓	
5.1.1.1.3 Procedures in place to evaluate when changes are needed to current hardware	✓	
5.1.1.1.4 Procedures, commitment and funding to replace hardware when evaluation indicates the need to do so	✓	
5.1.1.1.5 Software technologies appropriate to the services it provides to its designated communities	✓	
5.1.1.1.6 Procedures in place to monitor and receive notifications when software changes are needed	✓	
5.1.1.1.7 Procedures in place to evaluate when changes are needed to current software	✓	
5.1.1.1.8 Procedures, commitment and funding to replace software when evaluation indicates the need to do so	✓	
5.1.1.2 Adequate hardware and software support for backup functionality sufficient for preserving the repository content and tracking repository functions	✓	
5.1.1.3 Effective mechanisms to detect bit corruption or loss	✓	
5.1.1.3.1 Record and report to its administration all incidents of data corruption or loss, and steps shall be taken to repair/replace	✓	
5.1.1.4 Process to record and react to the availability of new security updates based on a risk-benefit assessment	✓	
5.1.1.5 Defined processes for storage media and/or hardware change (e.g., refreshing, migration)	✓	
5.1.1.6 Identified and documented critical processes that affect its ability to comply with its mandatory responsibilities	✓	
5.1.1.6.1 Documented change management process that identifies changes to critical processes that potentially affect the repository's ability to comply with its mandatory responsibilities	✓	
5.1.1.6.2 Process for testing and evaluating the effect of changes to the repository's critical processes	✓	
5.1.2 Manage the number and location of copies of all digital objects	✓	
5.1.2.1 Mechanisms in place to ensure any/multiple copies of digital objects are synchronized	✓	
5.2 Security Risk Management		
5.2.1 Maintain a systematic analysis of security risk factors associated with data, systems, personnel, and physical plant	✓	
5.2.2 Implemented controls to adequately address each of the defined security risks	✓	
5.2.3 Staff shall have delineated roles, responsibilities, and authorizations related to implementing changes	✓	
5.2.4 Suitable written disaster preparedness and recovery plan(s), including at least one off-site backup of all preserved information together with an offsite copy of the recovery plan(s)	✓	

Ongoing Discussions

Issue	Who's working on it?
~~Design template (letterhead, typefaces) for downloadable Documents~~	~~Steve, Karl~~
Future monitoring and reviewing schedule or calendaring. Discuss with Marie at CRL	Steve, Karl
~~Document version template~~	~~Aurianne, Karl, Steve~~
Risks associated with formats, where to talk about them?	Steve, Karl
List of formats?	Karl, Steve
Make file format language consistent	Karl
Make language, formatting consistent	All
"Understandability"	All