Digital Preservation Policy Review Checklist

Standard

- [ ] **Mission/Purpose**
  Defines why the document exists, what it will address, and by what authority you are doing it.
  States related documentation (e.g., digital preservation plan, lower-level specific policies)
- [ ] **Audience/Designated Community**
  Indicates to whom the documented is directed (internal and/or external audiences).
- [ ] **Updates**
  How often will you commit to reviewing the policy and making updates? Once a year, once every # years?
- [ ] **Objectives/**
  What is your institution committed to having the repository do? What will it not do?
  What aspects of the curation cycle will the repository be responsible for? Access, as well as preservation?
  Will the repository normalize files; will it preserve the original bitstream; will it create dissemination derivatives (DIPs)? If the repository is responsible for access, what will be the level of service. Will items be available immediately upon request? If not,
- [ ] **Authority to Access/Request**
  Will the repository be open to any and all requesters? Or are only certain authorized entities allowed?List out these entiries by job function or role, not by name.
- [ ] **Scope**
  Define what content your repository will have (e.g., born digital and/or digitized; government records and/or private materials; permanent records and/or records with retentions 10+ years).
  Define what you will do with material you do not accept.
- [ ] **Responsibilites**
  Define responsibilities at a high level but do not go into detail--authentication, virus checking, fixity checking, dispersed copies.Do not list specific methods or technical to accomlish.
  Define roles and responsibilities via job title of different positions that interact with the respository; do not use personal
- [ ] **Compliance with OAIS/ISO 16363**
  Define if your repository will conform to OAIS or ISO 16363, or to what degree it will attempt to conform (e.g., NC said it would try to comply recognizing that many issues are out of our control. Kansas points out that they will get an external
- [ ] **Collaborators and Partners**
  Define stakeholders in ensuring the viablity of the repository; acknowledge who will contribute to the repository and who can
- [ ] **Transfer/Acceptance of Content**
  Acknowledge if the repository will require content to be submitted in a certain format (SIP); define what you will do if you receive content that does not conform. Define how you will handle if content is removed from the repository (e.g. legal) and
- [ ] **Restrictions/Redactions**
  Indicate whether the repository will manage the identification, control, and auditing of restricted records (e.g., confidential records). Avoid specifying technology that will be used to accomplish these activities.

Optional

- [ ] **Physical facilities**
  Temperature, access, compliance with IT Architecture
- [ ] **Personnel**
  Background checks.
- [ ] **Uniform Electronic Transaction Act (UETA)**
  Compliance with UETA if your state has adopted it