Project Name: Date:

Section C: Digital Sustainability Plans

Module C4: Permissions & Data Integrity

Overview
The activities discussed in this module focus on protecting and maintaining the integrity of your work over time, from the platform level down to the bit level. The permissions section asks you to assess which team members have read, write, and delete authorizations for each technology used. The data integrity section details actions that will help project members ensure that the files they are preserving remain, if desired, fixed or unchanged.
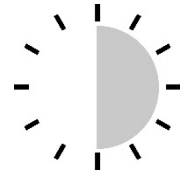
Activity: Group-Based Consensus Building
30-45 min

As a group (if appropriate), read through the sustainability levels offered by this module and then determine:

- How high a priority this area is for your project;
- Your current level of sustainability practices;
- Your desired level of sustainability practices (as a goal to be achieved within the next *three years*);
- The resources and actions that will be required to meet your desired level.

Your current level may be a "Level 0" for these areas, and that is absolutely fine. It may even be the case that your *desired* level for a given area is "Level 0." Keep in mind that very few projects need to be at Level 4, and that this is not necessarily the central goal. Depending upon the specific traits, objectives, and resources of your project, it is likely that you will have different desired levels of effort across many of the sustainability areas presented by the Socio-Technical Sustainability Roadmap. Please focus on choosing your levels of sustainability mindfully and in harmony with your project's resources and desired longevity.

Form: Apr-18

Project Name: Date:

Module C4: Permissions & Data Integrity

	Level 1	Level 2	Level 3	Level 4
Permissions	Identify which project members have login credentials to accounts and services used Identify which project members have read, write, move, and delete authorization to individual files	Restrict authorizations to only necessary team members Document access restrictions for services and files	Maintain logs of who performs what actions on files, including deletions and preservation actions	Perform routine audits of activity logs

What is your desired level? Why?

0   1   2   3   4

How high a priority is reaching your desired level in this area? Why?

Low   Medium   High

What is your current level? Why?

0   1   2   3   4

What resources and actions are required to reach your desired level?

Project Name: Date:

Module C4: Permissions & Data Integrity

	Level 1	Level 2	Level 3	Level 4
Data Integrity	Identify which project members have login credentials to accounts and services used Identify which project members have read, write, move, and delete authorization to individual files	Be able to replace/ repair corrupted data Create fixity information for stable project files	Check fixity of stable content at fixed intervals	Check fixity of stable content in response to specific events or activities

What is your desired level? Why?

0   1   2   3   4

How high a priority is reaching your desired level in this area? Why?

Low   Medium   High

What is your current level? Why?

0   1   2   3   4

What resources and actions are required to reach your desired level?