U.S. DEPARTMENT of ENERGY | Office of Critical Minerals and Energy Innovation

Data Life Cycle: Livewire Data Platform

July 2026

Disclaimer

This work was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or any third party's use or the results of such use of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof or its contractors or subcontractors. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof, its contractors or subcontractors.

Authors

The authors of this report are:

Matthew Macduff, Pacific Northwest National Laboratory (PNNL)

Casey Quinn, Idaho National Laboratory (INL)

Chitra Sivaraman, PNNL

Lauren Spath Luhring, National Laboratory of the Rockies (NLR)

Table of Contents

1 Introduction 1
1.1 Purpose 1
1.2 Scope 1
1.3 Roles and Responsibilities 1
2 Phase 1: Data Acquisition and Collection 1
2.1 Data Sources 1
2.2 Ingestion Methods 2
2.3 Data Categorization 2
3 Phase 2: Data Processing and Transformation 2
3.1 Data Validation 2
4 Phase 3: Data Storage and Security 2
4.1 Storage Architecture 2
4.2 Security Measures 3
4.3 Backup and Disaster Recovery 3
5 Phase 4: Data Usage and Dissemination 3
5.1 Internal Analytics 3
5.2 Public/External Access 3
5.3 Data Auditing 3
6 Phase 5: Data Archiving 4
6.1 Archiving Triggers 4
6.2 Archive Storage 4
6.3 Retrieval Process 4
7 Phase 6: Data Destruction and Disposal 4
7.1 Retention Policies 4
7.2 Secure Deletion 4

1 Introduction

1.1 Purpose

This document is intended to define the end-to-end life cycle of data managed within the Livewire Data Platform (Livewire, https://livewire.energy.gov/), ensuring data integrity, security, availability, and compliance with U.S. Department of Energy (DOE) and other federal directives.

1.2 Scope

This document covers all datasets, APIs, user-generated content, and telemetry managed and disseminated by Livewire, from initial ingestion to final disposal or archiving.

1.3 Roles and Responsibilities

Management and operational execution data on Livewire are distributed across two primary organizational roles:

Role	Key Responsibilities
Data stewards/Livewire lead role	Typically, the principal investigator “owns” data in its original format and provides high-level metadata information, access constraints, and updates to data.
Data engineers/Livewire administrators	Responsible for infrastructure management, security controls, backup execution, data steward onboarding, metadata curation, compliance validation, and managing data release approvals.

2 Phase 1: Data Acquisition and Collection

2.1 Data Sources

Incoming data come from a variety of data streams. Primary sources of data in Livewire include projects funded by DOE’s Transportation Technologies Office and other data related to transportation that users may find useful. These sources such as :

- National labs (e.g., National Laboratory of the Rockies, Pacific Northwest National Laboratory, Idaho National Laboratory)
- External grid sensors and telemetry
- Third-party organizations (e.g., University of Michigan, U.S. Environmental Protection Agency)
- Internal DOE databases.

2.2 Ingestion Methods

Data can be included in Livewire the following ways:

- Manual file uploads via the secure user portal
- RESTful APIs (Representational State Transfer) for programmatic access
- Real-time streaming via Site Transfer Software
- Linking to an existing data repository.

Individuals who would like to upload or store their data on Livewire should reach out to the Livewire team at LivewireDevTeam@pnnl.gov or view the Livewire User Guide (https://livewire.energy.gov/publication/1931) for more information.

2.3 Data Categorization

Datasets on Livewire are tagged with keywords from Livewire's curated list to increase visibility through search. Keywords are visible on Livewire's project search page (https://livewire.energy.gov/project-search).

3 Phase 2: Data Processing and Transformation

3.1 Data Validation

Livewire's data pipeline, Diogenes (github.com/idaholab/diogenes), checks incoming data for completeness, accuracy, and proper formatting by implementing automated testing and monitoring to flag anomalies and write machine-readable low-level metadata. This platform-generated metadata often incorporate data dictionaries provided by data stewards and produces standard documentation in JSON and PDF format.

4 Phase 3: Data Storage and Security

4.1 Storage Architecture

Data are stored on Livewire as follows using Amazon Simple Storage Service (Amazon S3):

- Data versioning preserves all copies of data.
- Large datasets are migrated to "cold storage" after 30 days to manage cost.
- All data are mirrored to another region in cold storage.
- Data access is limited to platform services that enforce authorization for reading.
- New data are added by the platform after validating authorization and data standards.

4.2 Security Measures

Livewire adheres to strict federal security standards established by DOE and managed under an “authority to operate” at Pacific Northwest National Laboratory. This covers a broad range of controls including management, configurations, monitoring and access controls. Access controls include role-based access control, multi-factor authentication, and least privilege.

Livewire also allows data stewards to choose from three tiers of access control:

1. Tier 1/Open: Accessible to anyone who creates a Livewire account.

2. Tier 2/Privileged: Instantly accessible to users who authenticate using a .gov or .mil email address or with project lead (data steward) consent. The project page is viewable by all in Livewire’s catalog.

3. Tier 3/Restricted: Accessible only with project lead consent. Depending on the access restrictions mandated by the project, a PI may require that users sign a non-disclosure agreement and require that users log in with MFA.

4.3 Backup and Disaster Recovery

Livewire is backed up nightly to ensure recovery. The data are backed up via multi-region replication. In a disaster, all data could be warmed and retrieved from another region in less than 48 hours. All software is preserved in Git repositories to enable rebuilding all parts of the system.

5 Phase 4: Data Usage and Dissemination

5.1 Internal Analytics

Livewire measures usage and engagement on the metrics page (livewire.energy.gov/metrics), along with project-specific metrics displayed on each project’s page.

5.2 Public/External Access

After a user is logged in, open data on Livewire are available to external stakeholders and the public via API, download, or link to an external repository.

5.3 Data Auditing

Livewire tracks and logs all data access events to maintain a comprehensive audit trail, providing additional insight to usage and ensuring compliance with federal security directives. Livewire data files are inventoried with digital signatures to ensure the data remain unchanged.

6 Phase 5: Data Archiving

6.1 Archiving Triggers

Automated triggers manage moving data to different tiers of storage. All data stored on the platform are intended to be stored for an indefinite period per guidance from DOE. Large datasets are tagged with an alternate storage tier, and automated processes migrate the data within 30 days.

6.2 Archive Storage

Livewire utilizes low-cost, secure archival storage solutions such as Amazon S3 Glacier to minimize operational costs. All data are replicated to an alternate region and stored in Amazon S3 Glacier. All data stored on the system are considered archived for long-term storage. Some data are stored with external partners, and only a link to their resources is provided. Archive policies for external data are determined by the external provider.

6.3 Retrieval Process

All data stored on the system are fully available to any authorized user through the web portal. This allows for data search, discovery, and download.

7 Phase 6: Data Destruction and Disposal

7.1 Retention Policies

Livewire's data retention periods are aligned with the National Archives and Records Administration schedules for federal records.

7.2 Secure Deletion

Livewire encrypts all stored data. Users may delete their data before the retention period ends. Upon deletion, the contents are unusable and ultimately overwritten. Using Amazon S3 storage provides for robust storage security.

For more information, visit: energy.gov/

DOE/GO-102026-7135 • July 2026

U.S. DEPARTMENT of ENERGY

Office of Critical Minerals and Energy Innovation