# Security Working Group

| Description |
| --- |
| As a goal, we would like to guide realization of an security in energy system that is interoperable, by standardizing the meaning of secure data exchange and guide secure implementation of open source projects developing exchange (interfaces) based on these security standards. We focus on the business side of security as common understanding, trust and transparency of data used and data privacy is a fundamental part of the energy system of the future, regardless of geography. |

## Purpose

The purpose of the Security WG is to have a center of gravity for discussions and thought leadership within the energy sector on software security, which will create the standard approach from software security as the industry evolves and the use of open source continues to grow. This will provide market education on pressing topics such as the software supply chain, which will ensure that solutions can be developed in a secure and safe manner. The group intends to work cross-functionally across LFE, but also bring in and leverage expertise from other groups such as CNCF.

# Goals/Non-Goals

Goals

- Bring member's organization's best practices internally on software security into a vendor-neutral public discussion.
- Capture the industry challenges in software security, especially those coming to light with the energy transition.
- Succinctly define software security as it applies to the industry.
- Coaching and guidance to hosted LFE projects on software security best practices and recommendations on resources for projects.

Non-goals

- Not leveraging existing software security standards or collaborating with other software security efforts. (i.e. reinventing the wheel).

# Deliverables

- Framework for security in open source projects in LFE (work to be done by postdoc).
- Training and education resources for use by projects and members.
- Resources for projects to pass the security requirements outlined in the CII Best Practices badge.

# Next Steps

**Phase 1**

- Collect resources on this Wiki page
  - Definition & Challenges
  - Best Practices
- Join the mailing list to become actively involved: https://lists.lfenergy.org/g/security

Phase 2

- Deliverables
  - 1) Describe the problem
  - 2) Describe the LFE solution derived from similar efforts

Phase 3

- Implementation (select test project, develop training material)

# Suggested Material

- https://github.com/cncf/tag-security
- https://github.com/cncf/tag-security/blob/main/security-whitepaper/cloud-native-security-whitepaper.md
- https://www.nist.gov/cyberframework
- https://www.tfir.io/is-open-source-ready-for-bidens-executive-order-for-cybersecurity/
- Security Data architecture support as a topic