Summary

This post outlines version 1.0 of a set of applicable controls for increasing DAO security (aka, the DAO Security Standard

). This is a collaborative work, led by DAOstar, eth.limo, and Tally, funded by the Ethereum Foundation, and supported by several members of the Security Alliance (SEAL).

Motivation

DAO security is a multi-faceted concept. Because of their decentralized nature, security measures vary across DAOs. This specification (DAOIP-8) aims to establish a minimum viable security standard among DAOs. Our intention is to ensure that at least the controls defined in this guide are standard practice in all organizations, irrespective of their scale. In writing this, we have considered data transparency, decentralized ownership, proposal safety, vendor management, defense against governance attacks, physical security, code upgrades, and other angles. While the absence of some of these (for example, a physical security policy for delegates) can lead to a critical security incident, others (for example, data transparency) may not have an immediate side effect. Even so, it may lead to second-order effects (e.g., low data transparency → loss of quality contributors → governance takeover). Hence, all DAOs are recommended to make their best effort to follow the controls outlined below.

Please note that this guide is a work in progress. It should not be taken as the gold standard when it comes to DAO security, but rather as the minimum. Several sections (for example, vendor management policy

, or incident response

) need to be polished to fit the design of your DAO. Security practices in web2 organizations are generally more mature than in web3 organizations like DAOs. Therefore, many of the templates and inspiration documents referenced have web2 origins. We urge DAOs to modify them considering their unique properties.

Controls below are categorized into:

1. [MANDATORY]

: includes measures that are critical to ensuring DAO security.

1. [RECOMMENDED]

: includes measures that may not have an immediate effect, but have second-order security effects.

We recommend following both categories of controls to ensure maximum security in your DAO.

The second section is for protocol DAOs

, i.e., DAOs that control an on-chain protocol, like Arbitrum DAO. All DAOs, whether or not they are a protocol DAO

, are advised to consider the controls detailed in the first section.

We are posting this version first in Arbitrum DAO — one of the most active DAOs in terms of governance participation — to gauge community sentiment and solicit feedback. We urge you, as a delegate and a participant in the DAO ecosystem, to provide your feedback on the standard. This work has the potential to drive the security policy of DAOs in the coming years and could lead to an L2Beat-type website tracking the state of security in DAOs. Your feedback is important.

Specification

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119.

DAO Controls

Control

Description

Data transparency

1. [MANDATORY]

The DAO should publish an up to date governance document

, outlining the steps and stakeholders involved in governance.

Data transparency is critical to an organization's security. The governance document should clearly define the person(s) responsible for its upkeep, along with a channel to reach out to them if information is incorrect or outdated.

Along with key details on governance design, and operational rules, the governance document SHOULD

include information on all privileged roles

(details on who can do what). For example, can anyone create a new proposal, can proposals be vetoed, are proposal execution autonomous, etc?

1. [RECOMMENDED]

The DAO should maintain a repository of all DAO-related artifacts.

DAO-related artifacts include (but are not limited to) grant programs; list of all smart contracts; list of functional committees, councils and multisigs; trusted service providers; and financial reporting. We recommend using the EIP-4824 standard to facilitate this, as it allows decentralized control of data by the DAO.

Ownership of digital assets

[MANDATORY]

The DAO should release a public list of digital assets it owns and controls. The list could include ENS names and other naming services, dApps, frontends, etc.

Self defense, incident response, and vulnerability management

1. [MANDATORY]

The DAO must publish a self-defense and emergency management plan.

It is important to have an incident response plan, including details of what constitutes an emergency/incident. Note that the intention here is to prompt the creation of a plan - no critical details of the incident response plan need to be public. A template is available here (not Web3/DAO specific).

1. [RECOMMENDED]

The DAO should publish a vulnerability management plan. Sampletemplate (not Web3/DAO specific).

Vendor/service provider management Policy

1. [MANDATORY]

The DAO should publish a list of vendors/service providers it relies upon.

1. [RECOMMENDED]

The DAO should publish a vendor management policy. Inspiration here.

Vendors include all 3rd party service providers that provide a good or service to the DAO, including software services that are not paid by the DAO, but used for operations, governance or other avenues

.

Proposal safety

[RECOMMENDED]

It is recommended to:

- Use a timelock before upgrading protocols that hold funds.
- Simulate proposals before executing them.
- Perform automated checks on proposals for common attacks.

Physical security policy

[MANDATORY]

The DAO should publish a physical security policy, and provide training to combat wrench attacks.

While enforcing this is difficult, the DAO is recommended to focus on educational content that describes measures to be taken by key delegates, multisig signers, members of the foundation, and other important stakeholders to ensure security while traveling to conferences and other events. Inspiration taken from here.

Community management

[MANDATORY]

The DAO should follow secure community management processes, to secure community accounts on Twitter, Discord, Telegram, and other applications. Template here.

Compliance

[MANDATORY]

The DAO must keep a record of its compliance efforts, including policies, procedures, and audit results. It should make its best efforts to comply with the regulatory frameworks applicable to its areas of incorporation.

Note that regardless of DAO jurisdiction or its regulatory standing, assets such as websites, frontends, forums, etc. can be subject to various data privacy laws. It is recommended to make a concerted effort to adhere to regulatory obligations to prevent future burdens or headaches such as “DSARs” and “Right to be forgotten” requests.

Protocol Controls

The following set of controls are authored for protocol DAOs, i.e DAOs that control an on-chain protocol. All DAOs, irrespective of whether they are a protocol DAO, are advised to follow the controls detailed in the previous section.

Control

Description

Data transparency

1. [MANDATORY]

Code that the DAO governs should be available somewhere publicly, even if it is not open source.

1. [RECOMMENDED]

All DAO related smart contracts including protocol, token, governance and treasury related smart contracts, should be verified on block explorers, if the provision exists.

1. [RECOMMENDED]

There should be publicly accessible documentation on the protocol components, along with flow diagrams, design choices, dependencies and a record of critical privileged roles.

Code security

[MANDATORY]

Protocol code MUST

be audited, and a comprehensive report detailing vulnerabilities and suggested improvements should be publicly available for the latest protocol version.

Proposal safety

[RECOMMENDED]

It is recommended to:

- Use a timelock before upgrading protocols that hold funds.
- Perform automated tests on code commits.

Bug bounty program

1. [RECOMMENDED]

The DAO is recommended to operate a bug bounty program, should it handle user funds.

1. [RECOMMENDED]

The DAO is recommended to execute a white hatSafe Harbor agreement if the provision exists.

Key management

[MANDATORY]

Use isolated and purpose specific hardware wallets for multisig key holders and delegates.

Operational security policy for key entities

[RECOMMENDED]

The DAO should require entities, including its foundation, founding company, or service providers with a long-term service agreement, to publish and adhere to an operational security policy.

Inspiration for the policy is here. As above, the intention is to prompt operational security for all stakeholders and not to publish critical information publicly.

Subdomains for contracts and dApps

[RECOMMENDED]

It is recommended to provide all contracts with ENS names. dApps should enforce ENS subdomain versioning schemas (v1, v2, etc) as mentioned here.

This is a best practice for future management of organizational units when delegating responsibilities to working groups or other sub-organizations within the DAO. Additionally this provision helps ensure that versioning remains immutable and easy to understand.

How to Contribute

Community members are urged to engage in this thread. We will take critical feedback to improve the specification. Additionally, you can also submit a direct PR by following the instructions in the DAOIP-8 on GitHub.