

[Template] Safe Harbor Adoption Checklist

[Outline](#)

[Steps and Instructions](#)

- [1. Initial Evaluation](#)
- [2. Define Scope and Terms](#)
- [3. Governance and Documentation](#)
 - [3.1 DAOs](#)
 - [3.2 Centrally Governed Protocols](#)
- [4. Finalization and Publication](#)
- [5. Communicate Adoption](#)

[Scope and Terms](#)

- [Protocol Information](#)
- [Assets under Scope](#)
- [Bounty Terms](#)
- [Identity Requirements](#)

Outline

Date Started:

Responsible Persons:

This Adoption Checklist is designed to walk you through the process of adopting the Whitehat Safe Harbor Agreement for your protocol. It assumes familiarity with the agreement. For more information on the agreement you can review the official GitHub [repository](#) or Skylock's [Safe Harbor Summary](#).

The following steps should be taken when adopting the Safe Harbor Agreement:

1. Initial Evaluation
2. Define Scope and Terms
3. Governance and Documentation
4. Finalization and Publishing

5. Communicate Adoption

Steps and Instructions

1. Initial Evaluation

- ☐ Completed initial evaluation of the Safe Harbor Agreement.

Instructions

- Review the [Safe Harbor Agreement](#).
- Understand the benefits and risks associated with the agreement.
- Decide whether to proceed.

Notes

2. Define Scope and Terms

- ☐ Scope and terms defined.

Instructions

- Define the scope and terms for your adoption of the agreement using the below [Scope and Terms](#).
- Refer to our [Blog Post](#) or the [official GitHub repository](#) for clarification.

Notes

3. Governance and Documentation

- ☐ Governance and documentation steps completed.

Instructions

- Follow the appropriate steps for your protocol's governance structure.

3.1 DAOs

- ☐ Created and published a DAO proposal.
 - Proposal URL / Transaction Hash:
 - Proposal Submission Date:
- ☐ DAO proposal approved.

Template

- Use the DAO proposal template as a starting point.
- Include all relevant information from the defined scopes and terms, and specific DAO information.

3.2 Centrally Governed Protocols

- ☐ Distribute this document to relevant parties for feedback.
 - Relevant parties have signed off:
 - Security Team.
 - Protocol Owner.

Notes

4. Finalization and Publication

- ☐ Finalization and publishing completed.

Instructions

- Download and complete the “*Whitehat Safe Harbor Agreement*” from the [official GitHub repository](#).
- Upload the full “*Whitehat Safe Harbor Agreement*” to IPFS (Agreement Fact Page).
- Upload “*Exhibit F - Adoption Form*” to a publicly accessible location (website, repository, or IPFS).
- Insert “*Exhibit D - User Adoption Procedures*” into the terms of service for all relevant web applications.
- Deploy an on-chain transaction from a governance address to the Safe Harbor Registry contract.

Notes

Link to completed “*Safe Whitehat Harbor Agreement*”:

Link to Completed “*Exhibit F - Adoption Form*”:

Link to “*Exhibit D - User Adoption Procedures*” in website ToS:

Link to on-chain governance registry transaction:

5. Communicate Adoption

- ☐ Communicated adoption of the Safe Harbor Agreement.

Instructions

- Officially and publicly announce the adoption of the Safe Harbor Agreement by your protocol.
- Update your protocol’s website with the adoption details.

Notes

Scope and Terms

Protocol Information

Protocol Name:

Asset Recovery Address:

Contact:

Name	Role	Contact Information

Assets under Scope

Chain(s)	Address	Type ¹ (Direct / Parent)

Bounty Terms

Bounty Percentage: %

Bounty Cap (USD): \$

Retainable²: {true, false}

¹ Direct assets are assets which themselves should be protected under the Safe Harbor Agreement. Parent assets are addresses for which all smart contracts deployed from the address should be protected under the agreement. For more details, view "safe-harbor, [1.Eligible Protocols, DAO Adoption Procedures, Chain\[\], Accounts\[\] scope.](#)"

² Whether the whitehat can retain their bounty or must return all funds to. If set to true, the whitehat will keep their bounty and return the rest to the asset recovery address. If set to false, the whitehat will send all funds back

Identity Verification³: {*“Anonymous”, “Pseudonymous”, “Named”*}

Diligence Requirements⁴:

to the asset recovery address and the bounty will be paid out at a later date. For more details view “safe-harbor, [1.Eligible Protocols, DAO Adoption Procedures, BountyTerms.](#)”

³ Whitehat identity verification requirements. If Anonymous, the whitehat will be subject to no KYC requirements. If Pseudonymous, the whitehat must provide a pseudonym. If Named, the whitehat must confirm their legal name. For more details view “safe-harbor, [1.Eligible Protocols, DAO Adoption Procedures, BountyTerms.](#)”

⁴ The diligence requirements placed on eligible whitehats. Only applicable for Named whitehats. For more details view “safe-harbor, [1.Eligible Protocols, DAO Adoption Procedures, BountyTerms.](#)”