Safe Farming Policy

Projects and protocols often provide rewards to people using them. However, some malicious actors can take advantage of the hype to release contracts marketed as “yield farming” opportunities which in turn, can allow them to steal deposited assets.

As DeFi protocols become more and more complex, it is also hard for users to understand exactly which risks a particular strategy can bear.

This registry serves two main purposes:

- Verify that a yield farming strategy is legitimate as opposed to a fraudulent scheme that allows creators (or anyone else) to steal deposited assets.
- Verify that all the risks of a strategy are clearly disclosed.

Note that with the current speed of the yield farming ecosystem, it isn’t possible to be both up to date and completely safe. This registry tries to compromise between those two objectives by requiring a high deposit but with a short challenge period.

Guidelines:

➤ The name should briefly describe the yield farming opportunity. Submissions are not to be rejected on their name unless it is extremely misleading or extremely offensive.
Accept: SushiSwap farming.
➤ The image should be related to the strategy. It doesn’t need to be an official logo. Submissions are not to be rejected on their image unless it is extremely misleading or extremely offensive.
Accept: An image of a Sushi for SushiSwap.
➤ The strategy document should be a PDF composed of the following sections:

- **Overview:** A short introduction giving an overview of the strategy.
- **Required Assets:** The list of base assets required to execute the strategy. An asset is to be considered a base asset if there is no underlying correlated Ethereum-based asset it can be redeemed for through a smart contract.
- **Links:** Links to all frontends required to execute the strategy.
- **Strategy Description**: A detailed description of how to execute the strategy including screenshots of every step required (each transaction except those approving contracts for token transfers have to be included in a screenshot). If the strategy is submitted before the application goes live, it is acceptable for some screenshots to be missing or different than those of the live application.
- **Yield:** A short description of the yield produced by the strategy.
- **Risk Disclosure:** An exhaustive list and description of all non-negligible risks which could result in a loss of funds using the strategy. Risks can include:

  Smart contract risk (should probably always be mentioned), impermanent loss (in automated market makers), liquidation (in borrowing strategies), theft of assets by the smart contract owner, theft of liquidity pool due to unlimited printing of tokens, theft of assets due to malicious governance decisions.

- **Tipping address:** An Ethereum address to receive tips from people and entities finding the strategy useful. Kleros Cooperative vouches to give 10% of the yield it farms to the strategy submitter for a period of 3 months after it starts using a strategy. Other farmers are free to decide how much to tip.

➢ Strategies are not to be rejected due to small mistakes as long as the submission is still understandable and those mistakes are not likely to result in risks of fund loss.
Accept: The submission contains grammar mistakes and a link in a frontend is malformed leading to a 404 error. Grammar mistakes do not impede understanding of the strategy and it is still easy to find out the correct link.
Reject: An incorrect link leads to a copy of the main frontend sending user funds to hackers.

➢ Strategies are not to be rejected due to security or price concerns for the base assets or the reward asset. Risks of the base assets do not need to be explained in the Risk Disclosure section.
Accept: One of the base assets is YAM (despite it being buggy).

➢ Strategies using smart contracts with vulnerabilities likely to result in loss of funds should be rejected.
Accept: A vulnerability could be exploited by the anonymous smart contract owner to steal the funds but can only be used with a 2 days timelock (SushiSwap).
Reject: A vulnerability could be exploited by the anonymous smart contract owner to immediately steal the assets (SushiSwap contracts without timelock for the owner).

➢ Strategies with admin control allowing an administrator account which belongs to an anonymous individual to take the funds, without letting participants the time to exit the system, should be rejected.
Accept: The contract is made by a reputable project and the fact that an admin has the possibility to move the funds has been listed in the risk disclosure section.
Accept: The strategy uses a contract made by an anonymous team able to move the funds but requires a 2 days delay to do so. This risk was disclosed.
Reject: The strategy uses a contract made by an anonymous team able to move the funds.

➢ Strategies whose risk disclosure section lacks some risks should be rejected.
Reject: The strategy carries a liquidation risk during a blackswan event which hasn’t been listed.
Reject: The strategy requires users to provide liquidity to an automated market maker

pair. The risk of impermanent loss hasn't been listed.
Reject: The smart contract risk hasn't been listed.

➢ Strategies which are similar but use different assets can be listed in the same strategy submission. This list doesn't need to be exhaustive. When it is the case, the Required Assets section should list asset tuples which can be used and the remaining of the document can take one tuple as an example.
Ex: For the SushiSwap strategy, all usable liquidity pairs are listed in the Required Assets section. Then DAI-ETH is used as an example.