Bullionix Smart Contract Security Concerns

There are always security concerns that need to be accounted for when dealing with smart contracts; especially if those contracts hold funds for users and allow anyone to interact with them. This document contains an outline of the potential foreseen security concerns that could happen and how to deal with them.

Premise:
Any user who has DGX can claim ownership of a Bullionix NFT by sending their DGX to our contract to back the NFT with DGX. This NFT would have ownership of DGX so if its sold or traded, the new owner can claim the previously staked DGX for themselves at any point.

Potential Risk Areas and Corresponding Solutions:

Owner Functions and 'god power' abuse
Limit functionality for admin, only to do what is needed, without access to change user/address amounts or balances. No code written that can be exploited by malicious actors.

Withdrawing/burning the NFT to reclaim the DGX associated with it
Just need to confirm that there are no overflow issues with the balances and proper standards are upheld. Security audit will prevent this from being an issue.

Loss of funds due to miscalculations
Safe math and open source code review.

Injection of bad data
Limit the data coming into the contract from the user, and confirm anything and everything via requires and reverts. Minimum viable input.

Compromised accounts
Hardware wallet accounts as admin and owner.