



SECURITY AUDIT REPORT

SP

StakePoint Smart Contract Auditor

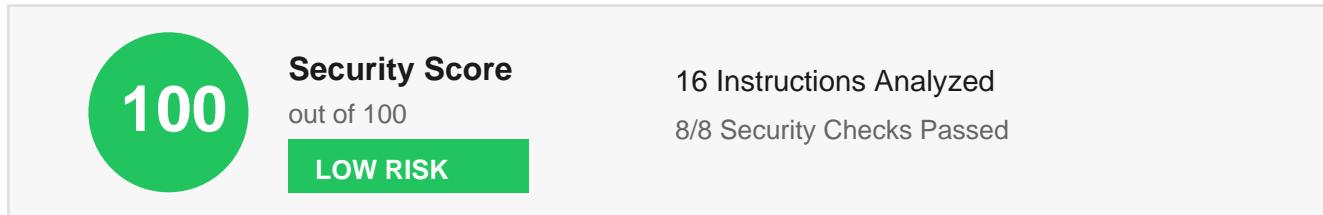
stakepoint.app

Generated: 12/11/2025, 3:38:04 PM

Program Information

Program Name: staking_program

Program ID: gLHaGJsZ6G7AXZxoDL9EsSWkRbKAWhFHi73gVfNXuzK



Executive Summary

Analyzed 16 instructions across the staking_program. Found 0 high-severity issues and 0 warnings. 8/8 security checks passed. The program follows most Solana security best practices.

Security Checks

● Signer Validation	PASS
16/16 instructions have signer checks	
● PDA Validation	PASS
PDA seeds and bumps are validated	
● Owner Checks	PASS
16/16 mutable instructions verify ownership	
● Initialization Guards	PASS
Has initialization instructions	
● Access Control	PASS
11 instructions require admin/authority	
● Emergency Pause	PASS
Has pause/unpause functionality	
● Error Handling	PASS
42 custom error types defined	
● Event Logging	PASS
14 events for audit trails	

Instructions Analysis

claim	11 accounts
Signer PDA Owner	
claim_reflections	8 accounts
Signer PDA Owner	
claim_unclaimed_tokens	7 accounts
Signer PDA Owner	
create_project	7 accounts
Signer PDA Owner	
deposit	12 accounts
Signer PDA Owner	
deposit_rewards	7 accounts
Signer PDA Owner	
emergency_unlock	2 accounts
Signer PDA Owner	
initialize	4 accounts
Signer PDA Owner	
initialize_pool	9 accounts
Signer PDA Owner	
pause_project	2 accounts
Signer PDA Owner	
refresh_reflections	4 accounts
Signer PDA Owner	
set_fees	2 accounts
Signer PDA Owner	
unpause_project	2 accounts
Signer PDA Owner	
update_fee_collector	2 accounts
Signer PDA Owner	

update_referrer

2 accounts

Signer

PDA

Owner

withdraw

12 accounts

Signer

PDA

Owner

Recommendations

- ! Consider a professional manual audit for production deployment

Disclaimer

This security audit report was automatically generated by StakePoint Smart Contract Auditor on 12/11/2025, 3:38:04 PM.

IMPORTANT: This automated analysis is provided for informational purposes only and should not be considered a comprehensive security audit. It analyzes publicly available IDL data and applies pattern-based checks for common vulnerabilities.

Limitations of this automated audit include:

- Cannot analyze actual program bytecode or implementation details
- Cannot detect logical vulnerabilities specific to business logic
- Cannot verify runtime behavior or edge cases
- Cannot assess cross-program invocation risks in full context
- May not detect all vulnerability patterns

For production deployments involving significant value, we strongly recommend engaging a professional security auditing firm to conduct a thorough manual review of your smart contract code.



StakePoint

Solana DeFi Platform

stakepoint.app

contact@stakepoint.app

Staking | Farming | Swaps | Tools