Cybersecurity Policy

Scope

This policy outlines Orbital’s approach to cybersecurity, leveraging Solana's security features, to protect our platform, users, and data. It covers the assets, systems, and processes integral to our platform, including networks, servers, applications, and user devices. The policy is applicable to all employees, contractors, partners, and users in the USA (and other countries in the future). It is effective immediately, although the platform will go live in December.

In-Scope Items

- **Assets**: Networks, serverless applications, user devices.
- **Systems**: Solana blockchain infrastructure, AWS services, Phantom wallet integration.
- **Processes**: Smart contract deployment, wallet security, incident response, legal compliance.
- **Data Types**: Wallet addresses, transaction data, certification/badge data.

Exclusions

- Personal devices used for non-work purposes.
- Financial data (until liquidity pools and token data are added).

Applicability

- **Audience**: Employees, contractors, partners, and users of Orbital.
- **Geographical Boundaries**: United States of America and Thailand.

Timeframe

- Effective Date: Immediately.
- Review Intervals: Semi-annually.

Policy Details

1. Understanding Solana’s Security Measures

- **Cryptographic Algorithms**: Solana employs SHA-256 and Ed25519 for transaction and identity security. These algorithms ensure data integrity and secure identity verification.

- **Consensus Algorithm**: Solana uses a Byzantine Fault Tolerant (BFT) consensus algorithm, enhancing network reliability and resistance to malicious attacks.
- **Security Audits**: Regular security audits are conducted to identify and mitigate potential vulnerabilities.

Why This Is Important: Utilizing strong cryptographic algorithms and a BFT consensus algorithm ensures the integrity and security of transactions on our platform. Regular security audits help maintain a high-security standard.

2. Smart Contract Security

- **Code Audits**: All smart contracts must undergo thorough code audits.
- **Standardized Practices**: Follow best practices in smart contract development.
- **Formal Verification**: Where possible, use formal verification to prove the correctness of smart contracts.

Why This Is Important: Ensuring smart contracts are secure and free from vulnerabilities (e.g., reentrancy, input validation, and authorization flaws) prevents exploits and enhances trust in our platform.

3. Wallet Security and Asset Management

- **Best Practices**:
    - Use hardware wallets (Ledger, Trezor) for long-term storage.
    - Enable two-factor authentication (2FA).
    - Regularly update wallet software.

Why This Is Important: Adopting these best practices protects users' assets from unauthorized access and phishing attacks.

4. Incident Response Plan

- **Roles**:
    1. **Incident Coordinator**: Ivan Dejesus (IT Manager) oversees the response, assesses situations, and guides technical actions, assisted by Samuel Johnson (Executive Director).
    2. **Communication Lead**: Isiah James (Creative Director) handles external communication with users, partners, and media.
- **Steps**:
    1. **Detection and Assessment**: Monitor logs and alerts, assess impact and severity.
    2. **Containment**: Isolate affected systems, revoke access tokens.
    3. **Eradication**: Identify the root cause, patch vulnerabilities.
    4. **Recovery**: Restore services, validate data integrity.
    5. **Lessons Learned**: Document the incident, conduct a post-incident review, update security practices.

Why This Is Important: A well-defined incident response plan ensures quick and effective handling of security breaches, minimizing damage and restoring normal operations promptly.

5. Legal/Compliance

- Follow the Florida Nonprofit Legal Compliance checklist for governance, advocacy, HR, and fundraising.
- Adhere to professional compliance guidelines provided by the Florida Department of Law Enforcement (FDLE).
- Ensure employee handbook compliance with state and federal laws.

Why This Is Important: Legal compliance ensures our operations are within the law, reducing the risk of legal repercussions.

User Education

- **Security Features**: Educate users about Solana's robust security measures (e.g., proof-of-history, BFT, SHA-256, Ed25519).
- **Safe Practices**:
  - Use hardware wallets.
  - Be cautious with software wallets due to phishing risks.
  - Regularly update wallet software.
  - Enable 2FA.
- **Asset Protection**:
  - Avoid phishing scams.
  - Never share private keys or seed phrases.
  - Double-check wallet addresses before transactions.
  - Be wary of suspicious links or emails.
  - Monitor account activity regularly.
  - Consider multisig wallets for added security.

Why This Is Important: Educating users on these practices helps them protect their assets and avoid common security pitfalls.

Regular Review and Adaptation

- Continuously assess and update the policy.
- Stay informed about Solana updates and emerging threats.
- Collaborate with security experts and the Solana community.

Why This Is Important: Regular reviews and updates ensure our policy remains effective against evolving threats and incorporates the latest security advancements.

Conclusion

A well-crafted cybersecurity policy balances innovation with security, ensuring a robust and trustworthy platform. By leveraging Solana's advanced security features and following best practices, Orbital aims to provide a secure environment for all users.