BHARAT WEB3
ASSOCIATION

CYBER SECURITY

Guidelines For Virtual Digital Asset Service Providers

Introduction

The emergence of crypto and blockchain technology has transformed various sectors, opening up fresh avenues for innovation and development. Yet, the distinct features of digital assets—such as their decentralized structure and dependence on cryptographic security—bring about new risks and challenges. Virtual Asset Service Providers, which serve as custodians of these assets, are particularly vulnerable to cyberattacks, fraud, and increasing regulatory oversight.

This document outlines a thorough set of cybersecurity guidelines to safeguard BWA members' integrity, availability, and confidentiality. These measures are essential for ensuring that these platforms operate securely and responsibly within the fast-changing landscape of Web3.

Scope

These guidelines are meant to apply to all BWA member exchanges (CEFI). The guideline aims to provide a thorough resource for exchange management, security teams, compliance officers, and other stakeholders involved in maintaining security and are responsible for the secure functioning of an exchange.

The primary focus areas of this cyber security guidelines as the first phase are to :

1. Custody technology and operations user
2. Exchange technology infrastructure
3. Exchange operations
4. Customer data
5. User (Customer & Employee) awareness & education

Objectives

- Ensure the safety and security of digital assets under the custody of the exchange.
- Adherence to existing regulatory guidelines and avoiding penalties or legal issues.
- Build and maintain trust with customers and investors by demonstrating a strong commitment to cybersecurity.
- Ensure effective operational procedures that support the overall security and compliance of the exchange.
- Ensure business continuity in case of cyber incidents with minimal disruption to operations.
- Educate users on security best practices to further enhance the protection of their digital assets and foster a culture of cybersecurity awareness.

01 Custody Technology and Operations

Scope

The systems, processes, and technologies utilized by BWA members exchange to securely store, process, and manage digital assets, ensuring the safety of private keys, facilitating securing transactions, and complying with defined requirements.

Security Technology

To achieve the required level of security in Custody Technology and Operations, it is imperative to design and implement a robust security stack tailored to the unique demands of virtual digital assets. The following key technologies must be meticulously designed, deployed, and integrated to protect core assets, ensure operational integrity, and mitigate cyber risks:

1. Secure Custody Storage Solutions
2. Encryption Technology
3. Hardware Security Modules (HSMs)
4. Key Management Service
5. Transaction Processing
6. Multi-Signature Wallets
7. Multi-Party Computation (MPC)
8. Secure Smart Contract
9. Technology Integration with Partners (API Security)

Key Policies

To safeguard the integrity, confidentiality, and availability of digital assets, it is crucial to establish and implement a comprehensive set of security policies tailored to the unique challenges of custody technology and operations. The following key policies must be meticulously drafted, enforced, and regularly reviewed to ensure robust security across all aspects of custody management including hot, warm and cold storage -

1. Fund Diversification Policy
2. Key Management Policy
3. Fund Operation Policy to include Implementing velocity limits on withdrawals
4. Signer / Approver / Admin Quorum Policy to include 2-factor authentication, video ID verification, etc.
5. Privileged User Management to include 2-factor authentication, video ID verification, etc.
6. Device Security Policy for Crypto Fund Management
7. Cyber Insurance

Security Testing

- Conduct quarterly process audits and stress tests of custody technology and operations to ensure compliance with the defined policies and standards.
- Perform security testing after major change or release.
- Engage external vendors for security testing on a bi-annual basis.

Best Practices

- NIST SP 800-90A
- Cryptocurrency Security Standard (CCSA)
- Security Requirements For Cryptographic Modules (FIPS 140)
- NIST SP 800-57 Part 1 Rev. 5
- ISO 27001:2022

02 Exchange technology infrastructure

Scope

The scope includes the planning, implementation, and management of the systems (hardware, software, application, data), networking, and cloud services that power the exchange platform. It also involves setting up security protocols, redundancy systems, and performance optimization strategies to ensure the exchange remains secure, available, and scalable. Additionally, this will encompass the integration of various systems and APIs, ensuring that all components work together seamlessly to facilitate secure, efficient, and compliant trading operations.

Security Technology

To achieve robust security within the exchange's technology infrastructure, it is crucial to create and implement a comprehensive technology stack that tackles the unique challenges faced by crypto exchanges. The following key technologies should be thoughtfully deployed and integrated to protect assets, uphold operational integrity, and reduce potential risks.

1. System Hardening
2. Web Application Firewall (WAF)
3. DDOS Protection
4. Vulnerability and patch management
5. Network Segmentation
6. Identity and Access Management (IAM)
7. API Security (Gateway)
8. Static Application Security Testing (SAST) Software
9. Dynamic Application Security Testing (DAST) Software
10. Authentication and Authorization
11. Secure Remote Access
12. Security information and event management (SIEM)
13. Auditing Logging
14. Key Management Service
15. Intrusion Detection and Prevention Systems (ID/PS)
16. Backup Solution
17. Mechanisms to detect malicious blockchain transactions
18. Local device Security
19. Address Whitelisting

Key Policies

To safeguard, it is crucial to create and put into practice a comprehensive set of security policies tailored to the unique challenges of exchange technology infrastructure. The following key policies must be meticulously designed, enforced, and regularly reviewed to guarantee complete security across all aspects of the exchange platform.

1. Access Control Policy
2. Data Protection and Encryption Policy
3. Network Security Policy
4. Incident Response Policy
5. Cloud Security and Posture Management
6. Endpoint Detection and Response (EDR)
7. Vulnerability Management Policy
8. Application Security Policy
9. Third-Party Risk Management Policy (including vendor onboarding/assessment policy)
10. Secure Development Lifecycle (SDLC) Policy

Security Testing

- Conduct quarterly vulnerability testing and stress tests on the technology platform with the defined policies and standards.
- Perform security testing after major change or release.
- Engage external vendors for security testing on a bi-annual basis.

Best Practices

- ISO 27001:2022
- NIST Cybersecurity Framework (CSF)
- CIS Benchmark
- NIST SP 800-123
- OWASP API Security Top 10
- OWASP Top 10
- NIST Special Publication 800-57
- Continuous Vulnerability Management
- OWASP Mobile Application Security

03 Exchange operations

Scope

The scope of exchange operations covers the comprehensive management and oversight of the exchange's daily trading activities, aimed at ensuring optimal efficiency and effectiveness. This includes the coordination of trading operations, clearing and settlement processes, banking rails, and managing customer onboarding. It also involves enforcing anti-money laundering (AML) and know-your-customer (KYC) policies, as well as business development and maintaining community relations to support the exchange's growth and engagement.

Security Technology

To achieve a strong level of security within the exchange's operation. The following key technologies should be thoughtfully deployed and integrated to protect assets, uphold operational integrity, and reduce potential risks.

1. Transaction Monitoring Platform
2. Threat Monitoring & Intelligence
3. Digital Signatures
4. AML and KYC Platform
5. Hardware Wallet
6. Anti-Phishing
7. Email Security
8. Privileged Access Workstation
9. Anti-Malware
10. Secure Device (Mobile / Laptop)
11. Mobile Device Management
12. Secure Access Service Edge (SASE)

Security Testing

- Implement and enforce mandatory security training (annual).
- Conduct quarterly user access reviews for critical applications and access to technology as per defined policies and standards.
- Engage external vendors for security testing on a bi-annual basis.

Key Policies

To safeguard the integrity, confidentiality, and accessibility of exchange operations, it is crucial to create and put into practice a comprehensive set of security policies to manage secure exchange operations.

1. Role-Based Access Control
2. User Access Review
3. Security Awareness and Education
4. Third-Party Risk Management Policy
5. Mobile Device Management
6. Email Security Policy
7. Acceptable Usage Policy
8. Password Policy
9. Security Education & Awareness
10. Risk Management Framework
11. Incident Response Management
12. Remote Work and Telecommuting Policy
13. Custody Providers Security
14. Business Continuity Policy
15. User Monitoring and Logging Policy

Best Practices

- ISO 27001:2022
- Digital Signature Standard (DSS)
- Privileged Access Workstation
- Managing the Security of Mobile Devices
- CIS Controls - Least Privilege
- Risk Management Framework (NIST Special Publication 800-37)
- Security of Mobile Devices (NIST Special Publication 800-124)
- NIST Special Publication 800-37 - Risk Management Framework
- Computer Security Incident Handling (NIST SP 800-61 Rev. 2)

04 Customer Data Protection

Scope

The scope of customer data protection encompasses the strategies, technologies, and processes involved in the collection, storage, processing, and protection of customer information within the organization. This includes ensuring the confidentiality, integrity, and availability of customer data while complying with defined policies and standards.

Security Technology

To achieve a high level of security within the management and protection of customer data, the following key technologies and practices should be thoughtfully deployed and integrated. These measures are essential for safeguarding data, ensuring operational integrity, and minimizing potential risks.

1. Data Loss Prevention and Monitoring (DLP)
2. Data Encryption
3. Data Masking and Anonymization
4. Database Activity Monitoring (DAM)
5. Secure File Transfer
6. Intrusion Detection and Prevention Systems (IDPS)

Key Policies

To safeguard the integrity, confidentiality, and accessibility of exchange operations, it is crucial to create and put into practice a comprehensive set of security policies to manage secure exchange operations.

1. Data Loss Prevention (DLP) Policy
2. Data Masking and Anonymization Policy
3. Database Activity Monitoring (DAM) Policy
4. Secure File Transfer Policy
5. Data Protection and Privacy Policy

Security Testing

- Conduct quarterly vulnerability testing and stress tests on the technology platform with the defined policies and standards.
- Perform security testing after major change or release.
- Engage external vendors for security testing on a bi-annual basis.

Best Practices

- ISO 27001:2022
- Key Management (NIST Special Publication 800-57)
- Protecting the Confidentiality of Personally Identifiable Information (PII) (NIST Special Publication 800-122)
- Digital Identity Guidelines (NIST Special Publication 800-63B)

05 User (Customer & Employee) Education & Awareness

Scope

The scope is to create, execute, and constantly improve programs that educate all users within an organization about cybersecurity risks and best practices. This includes different efforts such as frequent training sessions, awareness campaigns, and strategic communications aimed at keeping users up to date on possible risks, safe online behaviors, data protection regulations, and their roles in defending the organization. The scope also includes simulation-based security testing, such as phishing simulations and other real-world scenario exercises, to reinforce learning and assess the efficacy of awareness campaigns. This comprehensive strategy guarantees that the organization's security culture stays strong, proactive, and adaptable to changing threats.

Security Technology

To achieve a high level of security in user education and awareness, it is essential to thoughtfully design and implement key training programs and practices. These initiatives are crucial for empowering users with the knowledge and skills needed to safeguard the organization, maintain operational integrity, and minimize potential risks.

1. Security Training Modules (Role Based Training)
    a. Engineering and Technology - Secure Development, DevSecOps
    b. Secure Fund Operations
    c. Signers and Approvers
2. Learning Management Systems (LMS)
3. Phishing Simulation Tools
4. Email Awareness Campaigns

Key Policies

To safeguard the integrity, confidentiality, and accessibility of exchange operations, it is crucial to create and put into practice a comprehensive set of security policies to manage secure exchange operations.

1. Security Awareness Training Policy
2. Phishing Simulation Policy
3. Acceptable Use Policy (AUP)
4. Role-Based Security Training Policy

Security Testing

- Define and implement a security awareness program, following established policies and best practices.
- Perform additional phishing tests after significant updates to security protocols or changes in the threat landscape.

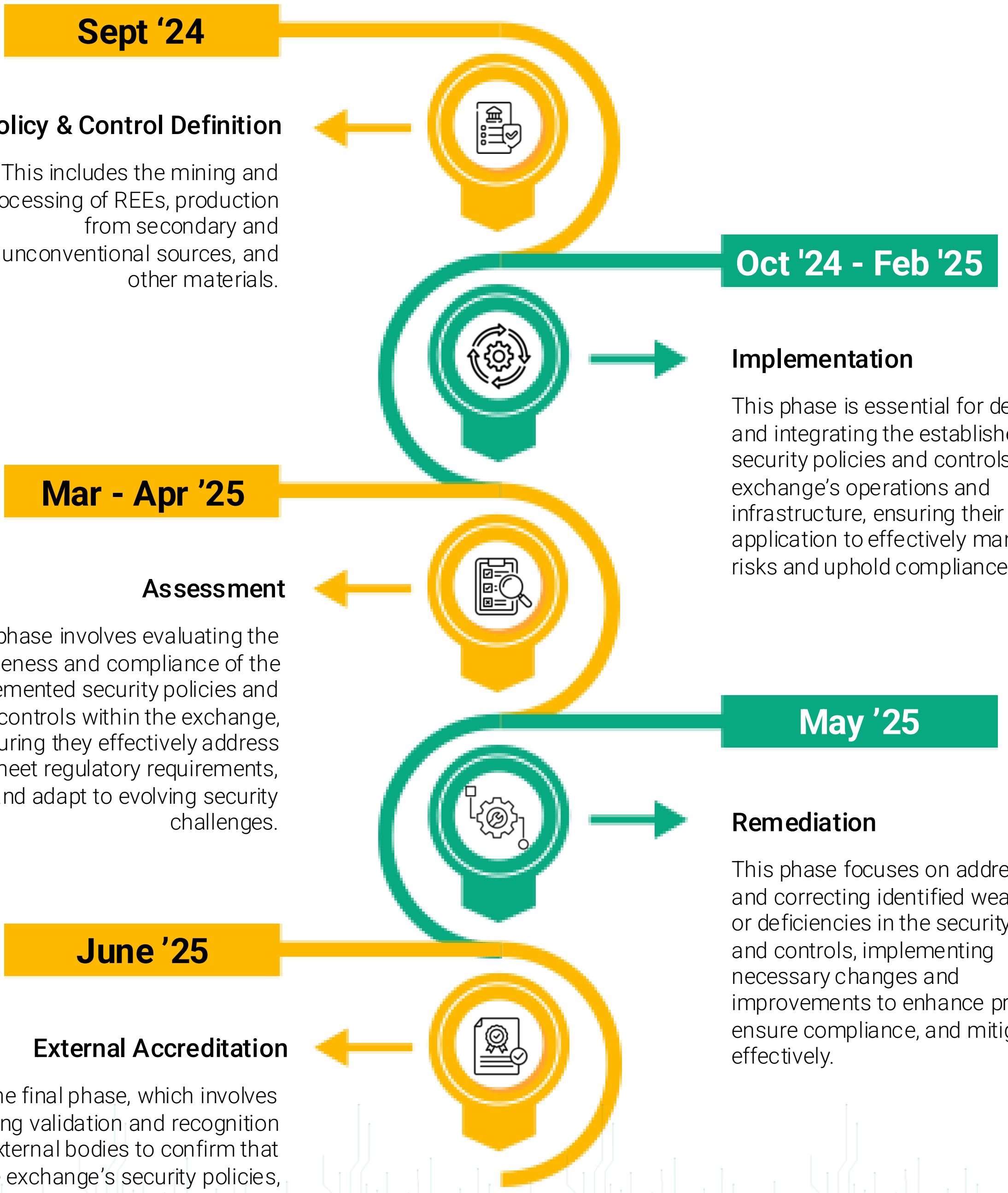
Best Practices

- SANS Institute Phishing Awareness
- KnowBe4 Best Practices
- NIST SP 800-50: Building an Information Technology Security Awareness and Training Program
- NIST SP 800-115: Technical Guide to Information Security Testing and Assessment

Timeline for Implementation

Taking a phased approach to implementation provides a clear and organized way to roll out new systems, processes, or policies. This method helps reduce risks, optimize resource management, and ensure that each phase effectively builds on the achievements of the previous one.

Below is a strategy that outlines a phased approach designed to facilitate a smooth and successful implementation not later than June 2025:



Sept ‘24

Policy & Control Definition

This includes the mining and processing of REEs, production from secondary and unconventional sources, and other materials.

Oct '24 - Feb '25

Implementation

This phase is essential for deploying and integrating the established security policies and controls into the exchange’s operations and infrastructure, ensuring their practical application to effectively manage risks and uphold compliance.

Mar - Apr ’25

Assessment

This phase involves evaluating the effectiveness and compliance of the implemented security policies and controls within the exchange, ensuring they effectively address risks, meet regulatory requirements, and adapt to evolving security challenges.

May ’25

Remediation

This phase focuses on addressing and correcting identified weaknesses or deficiencies in the security policies and controls, implementing necessary changes and improvements to enhance protection, ensure compliance, and mitigate risks effectively.

June ’25

External Accreditation

This is the final phase, which involves obtaining validation and recognition from external bodies to confirm that the exchange’s security policies, controls, and practices, thereby demonstrating credibility and adherence to best practices.

For exchanges, external accreditation plays a crucial role in demonstrating adherence to industry standards and requirements. Key external accreditations include:

1. ISO/IEC 27001:2022 - Information Security Management System (ISMS)
2. ISO/IEC 27701:2019 - Privacy Information Management System (PIMS)
3. Penetration Testing by 3rd Party
4. CCSS C4 (CryptoCurrency Security Standard)

Some references –

- Guidelines for the Protection of National Critical Information - https://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf
- NIST - Cyber security framework https://www.nist.gov/cyberframework
- RBI Cyber security guidelines https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0
- RBI Information security guidelines https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf