



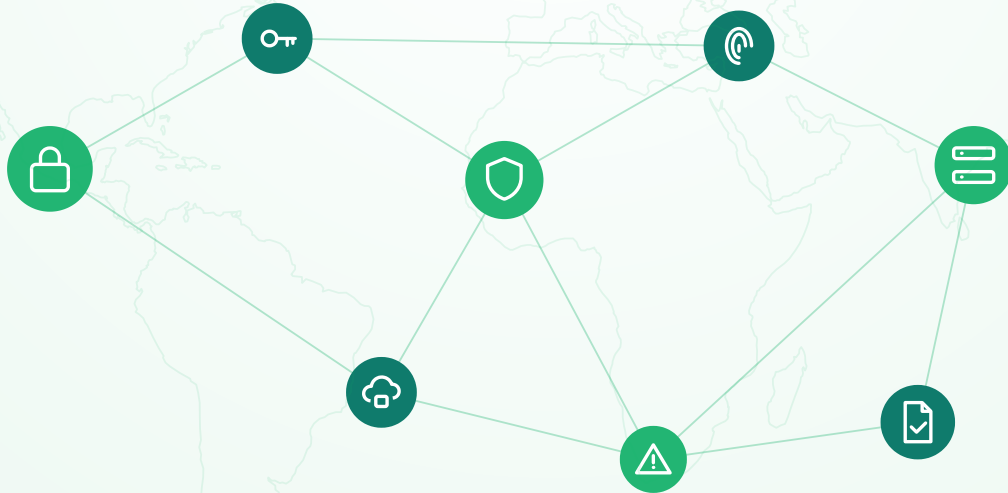
BHARAT WEB3
ASSOCIATION

CYBERSECURITY

Guidelines

FOR MEMBER EXCHANGES AND VIRTUAL ASSET SERVICE PROVIDERS

■ UPDATED AUGUST 2026



BHARAT WEB3 ASSOCIATION

Cybersecurity Guidelines

01 Introduction

The emergence of VDAs and blockchain technology has transformed various sectors, opening up fresh avenues for innovation and development. Yet, the distinct features of VDAs 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 comprehensive 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.

02 Scope

These guidelines are meant to apply to all BWA members. The guideline aims to provide a thorough resource for exchange management, security teams, compliance officers, and other stakeholders responsible for the secure functioning of an exchange. The primary focus areas of these cybersecurity guidelines (Phase I) are:

- a. Custody Technology and Operations
- b. Exchange Technology Infrastructure
- c. Exchange Operations
- d. Customer Data
- e. User (Customer & Employee) Awareness & Education

03 Objectives

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

04 Custody Technology and Operations

a. Scope

This section covers the systems, processes, and technologies utilized by BWA member exchanges to securely store, process, and manage digital assets, ensuring the safety of private keys, facilitating secure transactions, and complying with defined requirements.

b. **Security Technology:** The following key technologies must be designed, deployed, and integrated:

- | | |
|---------------------------------------|---|
| i. Secure Custody Storage Solutions | vi. Multi-Signature Wallets |
| ii. Encryption Technology | vii. Multi-Party Computation (MPC) |
| iii. Hardware Security Modules (HSMs) | viii. Secure Smart Contract |
| iv. Key Management Service | ix. Technology Integration with Partners (API Security) |
| v. Transaction Processing | |

c. **Key Policies:** The following key policies must be drafted, enforced, and regularly reviewed:

- i. Fund Diversification Policy
- ii. Key Management Policy
- iii. Fund Operation Policy - including implementation of velocity limits on withdrawals
- iv. Signer / Approver / Admin Quorum Policy - Strong, risk-commensurate identity verification for example, 2-factor authentication, video ID verification, etc.
- v. Privileged User Management - including 2-factor authentication, video ID verification, etc.
- vi. Device Security Policy for Crypto Fund Management
- vii. Cyber Insurance

d. **Security Testing:**

- i. Conduct at least an annual process audit and stress tests of custody technology and operations to ensure compliance with defined policies and standards.
- ii. Perform security testing after major changes or releases.
- iii. Engage external vendors for security testing at least on an annual basis.

e. **Best Practices:**

- | | |
|---|----------------------------------|
| i. NIST SP 800-90A | iv. NIST SP 800-57 Part 1 Rev. 5 |
| ii. Cryptocurrency Security Standard (CCSS) | v. ISO 27001:2022 |
| iii. Security Requirements for Cryptographic Modules (FIPS 140) | |

05 Exchange Technology Infrastructure

a. Scope

The scope includes the planning, implementation, and management of 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.

b. **Security Technology:** The following key technologies must be designed, deployed, and integrated:

- | | |
|---|--|
| i. System Hardening | xi. Secure Remote Access |
| ii. Web Application Firewall (WAF) | xii. Security Information and Event Management (SIEM) |
| iii. DDoS Protection | xiii. Audit Logging |
| iv. Vulnerability and Patch Management | xiv. Key Management Service |
| v. Network Segmentation | xv. Intrusion Detection and Prevention Systems (ID/PS) |
| vi. Identity and Access Management (IAM) | xvi. Backup Solution |
| vii. API Security (Gateway) | xvii. Mechanisms to detect malicious blockchain transactions |
| viii. Static Application Security Testing (SAST) Software | xviii. Local Device Security |
| ix. Dynamic Application Security Testing (DAST) Software | xix. Address Whitelisting |
| x. Authentication and Authorization | |

c. Key Policies: The following key policies must be drafted, enforced, and regularly reviewed:

- | | |
|---|---|
| i. Access Control Policy | vii. Vulnerability Management Policy |
| ii. Data Protection and Encryption Policy | viii. Application Security Policy |
| iii. Network Security Policy | ix. Third-Party Risk Management Policy
(including vendor onboarding/assessment policy) |
| iv. Incident Response Policy | x. Secure Development Lifecycle (SDLC) Policy |
| v. Cloud Security and Posture Management | |
| vi. Endpoint Detection and Response (EDR) | |

d. Security Testing:

- i. Conduct quarterly vulnerability testing and stress tests on the technology platform against defined policies and standards.
- ii. Perform security testing after major changes or releases.
- iii. Engage external vendors for security testing at least on an annual basis.

e. Best Practices:

- | | |
|--|---|
| i. ISO 27001:2022 | vi. OWASP Top 10 |
| ii. NIST Cybersecurity Framework (CSF) | vii. NIST Special Publication 800-57 |
| iii. CIS Benchmark | viii. Continuous Vulnerability Management |
| iv. NIST SP 800-123 | ix. OWASP Mobile Application Security |
| v. OWASP API Security Top 10 | |

06 Exchange Operations

a. 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.

b. **Security Technology:** The following key technologies must be designed, deployed, and integrated:

- | | |
|--------------------------------------|--|
| i. Transaction Monitoring Platform | vii. Email Security |
| ii. Threat Monitoring & Intelligence | viii. Privileged Access Workstation |
| iii. Digital Signatures | ix. Anti-Malware |
| iv. AML and KYC Platform | x. Secure Device (Mobile / Laptop) |
| v. Hardware Wallet | xi. Mobile Device Management |
| vi. Anti-Phishing | xii. Secure Access Service Edge (SASE) |

c. Key Policies: The following key policies must be drafted, enforced, and regularly reviewed:

- | | |
|--|---|
| i. Role-Based Access Control | ix. Security Education & Awareness |
| ii. User Access Review | x. Risk Management Framework |
| iii. Security Awareness and Education | xi. Incident Response Management |
| iv. Third-Party Risk Management Policy | xii. Remote Work and Telecommuting Policy |
| v. Mobile Device Management | xiii. Custody Providers Security |
| vi. Email Security Policy | xiv. Business Continuity Policy |
| vii. Acceptable Usage Policy | xv. User Monitoring and Logging Policy |
| viii. Password Policy | |

d. Security Testing:

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

e. Best Practices:

- | | |
|---|--|
| i. ISO 27001:2022 | vii. Security of Mobile Devices (NIST Special Publication 800-124) |
| ii. Digital Signature Standard (DSS) | viii. NIST Special Publication 800-37 – Risk Management Framework |
| iii. Privileged Access Workstation | ix. Computer Security Incident Handling (NIST SP 800-61 Rev. 2) |
| iv. Managing the Security of Mobile Devices | |
| v. CIS Controls – Least Privilege | |
| vi. Risk Management Framework (NIST Special Publication 800-37) | |

07 Customer Data Protection

a. 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 organisation. This includes ensuring the confidentiality, integrity, and availability of customer data while complying with defined policies and standards.

b. **Security Technology:** The following key technologies must be designed, deployed, and integrated:

- | | |
|--|---|
| i. Data Loss Prevention and Monitoring (DLP) | iv. Database Activity Monitoring (DAM) |
| ii. Data Encryption | v. Secure File Transfer |
| iii. Data Masking and Anonymisation | vi. Intrusion Detection and Prevention Systems (IDPS) |

c. **Key Policies:** The following key policies must be drafted, enforced, and regularly reviewed:

- | | |
|--|---------------------------------------|
| i. Data Loss Prevention (DLP) Policy | iv. Secure File Transfer Policy |
| ii. Data Masking and Anonymisation Policy | v. Data Protection and Privacy Policy |
| iii. Database Activity Monitoring (DAM) Policy | |

d. **Security Testing:**

- i. Conduct quarterly vulnerability testing and stress tests on the technology platform against defined policies and standards.
- ii. Perform security testing after major changes or releases.
- iii. Engage external vendors for security testing at least on an annual basis.

e. **Best Practices:**

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

08 User (Customer & Employee) Education & Awareness

a. Scope

The scope is to create, execute, and constantly improve programmes that educate all users within an organisation about cybersecurity risks and best practices. This includes frequent training sessions, awareness campaigns, and strategic communications aimed at keeping users up to date on possible risks, safe online behaviours, data protection regulations, and their roles in defending the organisation. 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 ensures that the organisation's security culture remains proactive and adaptable to changing threats.

b. **Security Technology:** The following key training programmes and practices must be thoughtfully designed and implemented:

- i. Security Training Modules (Role-Based Training)
 - 1. Engineering and Technology – Secure Development, DevSecOps
 - 2. Secure Fund Operations
 - 3. Signers and Approvers
- ii. Learning Management Systems (LMS)
- iii. Phishing Simulation Tools
- iv. Email Awareness Campaigns

c. Key Policies: The following key policies must be drafted, enforced, and regularly reviewed:

- | | |
|---------------------------------------|---|
| i. Security Awareness Training Policy | iii. Acceptable Use Policy (AUP) |
| ii. Phishing Simulation Policy | iv. Role-Based Security Training Policy |

d. Security Testing:

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

e. Best Practices:

- | | |
|---|---|
| i. SANS Institute Phishing Awareness | iv. NIST SP 800-115: Technical Guide to Information Security Testing and Assessment |
| ii. KnowBe4 Best Practices | |
| iii. NIST SP 800-50: Building an Information Technology Security Awareness and Training Programme | |

09 External Accreditation

For exchanges, external accreditation plays a crucial role in demonstrating adherence to industry standards and requirements. Below is a non-exhaustive recommendatory list of key external accreditations:

- a. ISO/IEC 27001:2022 – Information Security Management System (ISMS)
- b. ISO/IEC 27701:2019 – Privacy Information Management System (PIMS)
- c. Third-Party Penetration Testing
- d. CCSS C4 – CryptoCurrency Security Standard

References

1. Guidelines for the Protection of National Critical Information – https://nciipc.gov.in/documents/NCI_IPC_Guidelines_V2.pdf
2. NIST Cybersecurity Framework – <https://www.nist.gov/cyberframework>
3. RBI Cyber Security Guidelines <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0>
4. RBI Information Security Guidelines – <https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf>

