SPORTS AUTHORITY OF INDIA
IT DIVISION

INFORMATION SECURITY POLICY

Document No.: 01-01023(23)/1/2026-IT(HO)
Version: 1.0
Document Type: Internal Policy
Effective Date: 28.10.2026
Document Owner: IT Division, **Sports Authority of India**
Review Frequency: Annual

---

1. PURPOSE

The purpose of this Information Security Policy is to establish a comprehensive framework for protecting the confidentiality, integrity, and availability of information assets managed, processed, stored, transmitted, or accessed by **SAI**.

This Policy aims to:

- Protect organizational information assets against unauthorized access, disclosure, modification, damage, loss, theft, disruption, or destruction.
- Establish an Information Security Management Framework.
- Support business continuity and operational resilience.
- Ensure compliance with applicable legal, regulatory, contractual, and statutory requirements.
- Promote a security-conscious culture across the organization.

---

2. SCOPE

This Policy applies to:

- All employees, consultants, contractors, temporary staff, interns, vendors, and third-party service providers.
- All information assets, business processes, applications, databases, communication systems, cloud services, infrastructure, and facilities.
- All physical and electronic information owned, managed, processed, stored, or transmitted by **SAI**.
- All locations, offices, remote work environments, and cloud-hosted services.

---

3. OBJECTIVES

The objectives of this Policy are to:

- Safeguard information assets from cyber and physical threats.
- Ensure secure processing and handling of information.
- Maintain trust, reliability, and availability of business services.
- Define security responsibilities throughout the organization.
- Establish minimum security requirements and controls.
- Facilitate compliance with Government and regulatory requirements.

---

4. REFERENCE DOCUMENTS AND APPLICABLE REQUIREMENTS

4.1 This Policy shall be read in conjunction with:

- Information Technology Act, 2000.
- Digital Personal Data Protection Act, 2023.
- CERT-In Directions dated 28 April 2022.
- CERT-In Guidelines on Information Security Practices for Government Entities (CISG-2023-01).
- MeitY Information Security Guidelines.
- ISO/IEC 27001:2022.
- ISO/IEC 27002:2022.
- All approved **SAI** cybersecurity and information security policies.

4.2 Where SAI's activities involve Aadhaar authentication or a Sub-AUA/Sub-KUA arrangement, SAI shall identify and comply with the applicable requirements of the Aadhaar Act, rules and regulations framed thereunder, and directions, standards and specifications issued by UIDAI. The IT Division shall maintain appropriate records of applicable requirements and map the same to the relevant information security controls, systems and operational procedures. Any conflict between this Policy and an applicable statutory or regulatory requirement shall be resolved in favour of the applicable legal or regulatory requirement.

4.3 Where applicable under the UIDAI framework governing SAI's authentication arrangement, information security audits shall be conducted at the prescribed frequency and scope. Audit reports shall be submitted to UIDAI wherever required, and identified findings shall be recorded, assigned to responsible persons and tracked until remediation or formally approved risk treatment.

5 TERMS AND ABBREVIATIONS

Term	Definition
Information Asset	Any information, system, software, hardware, service, process, or resource with value to the organization
ISMS	Information Security Management System

CIA	Confidentiality, Integrity and Availability
DPO	Data Protection Officer
CERT-In	Indian Computer Emergency Response Team
User	Any authorized individual accessing organizational resources
Third Party	External entity providing products or services to **SAI**

6 INFORMATION SECURITY GOVERNANCE

SAI shall establish and maintain an Information Security Governance Framework to ensure:

- Protection of information assets.
- Risk-based decision making.
- Continuous improvement of security controls.
- Compliance with legal and contractual obligations.
- Security accountability at all organizational levels.

Information security shall be integrated into organizational governance and operational processes.

---

7 ROLES AND RESPONSIBILITIES

7.2 Management

Management shall:

7.2.1 Approve information security objectives.

7.2.2 Allocate necessary resources.

7.2.3 Ensure regulatory compliance.

7.2.4 Review information security performance.

7.3 IT Division

The IT Division shall:

7.3.1 Develop and maintain security policies.

7.3.2 Implement security controls.

7.3.3 Monitor cyber threats.

7.3.4 Conduct vulnerability assessments.

7.3.5 Coordinate incident management activities.

7.4 Information Asset Owners

Asset Owners shall:

7.4.1 Classify information assets.

7.4.2 Approve access rights.

7.4.3 Ensure protection of assigned assets.

7.4.4 Review access periodically.

7.5 Employees and Users

All personnel shall:

7.5.1 Comply with security policies.

7.5.2 Protect information assets.

7.5.3 Report security incidents.

7.5.4 Use organizational systems responsibly.

---

8 INFORMATION SECURITY PRINCIPLES

SAI shall ensure that information security controls support:

Confidentiality

Information shall be protected from unauthorized access and disclosure.

Integrity

Information shall remain accurate, complete, and protected against unauthorized modification.

Availability

Information and systems shall remain available when required for business operations.

Accountability

All actions affecting information assets shall be attributable to responsible individuals.

Risk-Based Security

Security measures shall be proportionate to identified risks.

9 INFORMATION ASSET MANAGEMENT

SAI shall:

- Maintain an inventory of information assets.
- Assign ownership of information assets.
- Classify information according to sensitivity.
- Implement protection controls based on classification.
- Review asset inventories periodically.

---

10 INFORMATION CLASSIFICATION

Information shall be classified as:

Classification	Description
Public	Authorized for public disclosure
Internal	Internal business information
Confidential	Sensitive business information
Restricted	Highly sensitive information requiring enhanced protection

Security controls shall be aligned with the classification level.

---

11 ACCESS CONTROL

Access to information shall:

- Follow least privilege principles.
- Be granted only upon authorization.
- Be reviewed periodically.
- Be revoked when no longer required.

Administrative and privileged access shall receive enhanced safeguards.

---

12 NETWORK SECURITY

Appropriate controls shall be implemented including:

- Firewalls.
- Network segmentation.
- IDS/IPS solutions.
- Secure remote access controls.

- Security monitoring mechanisms.
- Secure wireless controls.

13 ENDPOINT SECURITY

All endpoints shall:

- Use approved anti-malware solutions.
- Receive security updates.
- Follow hardening standards.
- Be continuously monitored.

Unauthorized devices shall not connect to organizational networks.

14 DATA PRIVACY AND DATA PROTECTION

Personal data shall:

- Be processed lawfully and fairly.
- Be protected against unauthorized disclosure.
- Be retained only as long as necessary.
- Be disposed of securely.
- Be handled according to applicable legal requirements.

15 CRYPTOGRAPHY AND ENCRYPTION

SAI shall implement encryption mechanisms appropriate to risk levels.

Encryption shall be considered for:

- Data at rest.
- Data in transit.
- Backup media.
- Portable devices.
- Sensitive business information.

16 VULNERABILITY AND PATCH MANAGEMENT

The organization shall:

- Conduct vulnerability assessments.
- Monitor security advisories.

- Deploy security patches.
- Address identified vulnerabilities based on risk.
- Maintain records of remediation activities.

---

17 INCIDENT MANAGEMENT

Security incidents shall:

- Be reported immediately.
- Be investigated appropriately.
- Be documented and tracked.
- Undergo corrective actions.
- Be managed according to the Incident Management Policy.

---

18 THIRD-PARTY SECURITY

Third parties shall:

- Comply with security requirements.
- Sign confidentiality agreements where applicable.
- Protect organizational information.
- Be subject to security assessments.

Appropriate contractual controls shall be established.

---

19 BUSINESS CONTINUITY AND DISASTER RECOVERY

Critical information assets shall be protected through:

- Backup procedures.
- Recovery arrangements.
- Business continuity planning.
- Periodic testing activities.

The organization shall maintain resilience against disruptions.

---

20 SECURITY MONITORING AND LOGGING

SAI shall implement:

- Security monitoring.

- Audit logging.
- Threat detection capabilities.
- Security event management.
- Continuous monitoring where appropriate.

Logs shall be protected against unauthorized modification.

---

21 SECURITY AWARENESS AND TRAINING

All personnel shall receive periodic awareness covering:

- Information security responsibilities.
- Cybersecurity threats.
- Phishing attacks.
- Data protection obligations.
- Incident reporting requirements.

Training records shall be maintained.

---

22 COMPLIANCE AND AUDIT

Compliance shall be monitored through:

- Internal audits.
- External audits.
- Compliance reviews.
- Risk assessments.
- Security assessments.

Violations may lead to disciplinary and contractual actions.

---

23 EXCEPTION MANAGEMENT

Policy exceptions shall:

- Be documented.
- Be risk assessed.
- Be approved by management.
- Include compensating controls.
- Be periodically reviewed.

---

24 POLICY REVIEW

This Policy shall be reviewed:

- Annually.
- Upon regulatory changes.
- Following significant incidents.
- Following audit findings.
- Following major technology changes.

25 EFFECTIVE DATE

This Policy becomes effective on 27.10.2026 by the approval by the Competent Authority.

26 APPROVAL

This Information Security Policy is approved by the Competent Authority of **SAI** and shall be applicable to all employees, contractors, consultants, vendors, and third parties.

27 REFERENCES

The following documents, standards, guidelines, and regulatory requirements were referred to while preparing this Policy:

1. **Information Technology Act, 2000**
   Link: https://www.meity.gov.in
2. **Digital Personal Data Protection Act, 2023**
   Link: https://www.meity.gov.in
3. **CERT-In Directions under Section 70B dated 28 April 2022**
   Link: https://www.cert-in.org.in/Directions70B.jsp
4. **CERT-In Guidelines on Information Security Practices for Government Entities (CISG-2023-01)**
   Link: https://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW02&refcode=CISG-2023-01
5. **MeitY Guidelines on Information Security Practices for Government Entities**
   Link: https://www.meity.gov.in
6. **ISO/IEC 27001:2022 Information Security Management Systems**
   Link: https://www.iso.org/isoiec-27001-information-security.html
7. **ISO/IEC 27002:2022 Information Security Controls**
   Link: https://www.iso.org/standard/75652.html
8. **NIST Cybersecurity Framework (CSF 2.0)**
   Link: NIST Cybersecurity Framework
9. **ISO/IEC 27005:2022 Information Security Risk Management**
   Link: https://www.iso.org/standard/80585.html

***