SPORTS AUTHORITY OF INDIA
IT DIVISION

THIRD PARTY 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 Third-Party Information Security Policy is to establish minimum information security requirements and controls for managing risks arising from third-party relationships involving access to, processing of, storage of, transmission of, or management of **SAI** information assets, information systems, applications, networks, cloud services, and supporting infrastructure.

This Policy is intended to ensure that third-party engagements do not introduce unacceptable information security, privacy, operational, regulatory, legal, or cyber security risks to **SAI**.

---

2. SCOPE

This Policy shall apply to:

- All vendors, suppliers, contractors, consultants, service providers, managed service providers, cloud service providers, system integrators, outsourcing partners, and other third parties engaged by **SAI**.
- Third parties having physical or logical access to **SAI** information assets, facilities, systems, networks, applications, databases, or cloud environments.
- All information shared, processed, stored, transmitted, or managed on behalf of **SAI**.
- All contracts, service agreements, procurement arrangements, and outsourcing engagements involving information processing activities.

---

3. REFERENCE DOCUMENTS AND APPLICABLE REQUIREMENTS

This Policy shall be read in conjunction with applicable laws, regulations, and standards, including:

- Information Technology Act, 2000 and amendments thereto.
- Digital Personal Data Protection Act, 2023.
- CERT-In Directions under Section 70B of the Information Technology Act, 2000 dated 28.04.2022.

- CERT-In Guidelines on Information Security Practices for Government Entities (CISG-2023-01).
- MeitY Information Security Guidelines for Government Entities.
- ISO/IEC 27001:2022.
- ISO/IEC 27002:2022.
- Applicable Government of India cyber security advisories, notifications, and guidelines.
- **SAI** Information Security Policy and related procedures.

In case of conflict between this Policy and statutory requirements, applicable legal and regulatory requirements shall prevail.

---

4. DEFINITIONS AND ABBREVIATIONS

Term	Description
SAI	Organization/Company
Third Party	Any external entity providing products or services to **SAI**
MSP	Managed Service Provider
CSP	Cloud Service Provider
NDA	Non-Disclosure Agreement
SLA	Service Level Agreement
DPA	Data Processing Agreement
Personal Data	Information relating to an identified or identifiable individual
Information Asset	Information, systems, software, hardware, networks, and related resources owned or managed by **SAI**

5. ROLES AND RESPONSIBILITIES

5.1 IT Division

The IT Division shall:

- Establish and maintain third-party security requirements.
- Conduct or coordinate security assessments.
- Review cybersecurity risks associated with third parties.
- Monitor compliance with this Policy.
- Maintain records of security reviews and exceptions.
- Coordinate incident response activities involving third parties.

5.2 Procurement Department

The Procurement Department shall:

- Ensure security requirements are incorporated into procurement processes.
- Coordinate contractual obligations with vendors.
- Ensure completion of due diligence activities before onboarding.

5.3 Business Owners

Business Owners shall:

- Identify security requirements associated with outsourced services.
- Ensure third-party access remains justified and approved.
- Periodically review vendor relationships and associated risks.

5.4 Third Parties

Third parties shall:

- Comply with contractual security obligations.
- Protect **SAI** information against unauthorized access, disclosure, modification, or destruction.
- Promptly report security incidents involving **SAI** information.
- Support security assessments and compliance reviews.

---

6. THIRD PARTY RISK ASSESSMENT

Prior to onboarding any third party, **SAI** shall conduct an appropriate risk assessment considering:

- Nature and criticality of services provided.
- Type and sensitivity of information involved.
- Access to systems, applications, and infrastructure.
- Regulatory and compliance obligations.
- Cyber security maturity of the third party.
- Geographic location and hosting arrangements.
- Previous security incidents and compliance history.

The depth of assessment shall be proportionate to the associated risk.

---

7. THIRD PARTY DUE DILIGENCE

Prior to engagement, due diligence activities shall include, where applicable:

- Verification of legal and business status.
- Review of information security controls.
- Assessment of privacy and data protection practices.
- Review of certifications such as ISO 27001.
- Security questionnaire and supporting evidence review.
- Assessment of incident response capabilities.
- Review of business continuity and disaster recovery arrangements.

---

8. INFORMATION SECURITY REQUIREMENTS

Third parties shall implement appropriate controls to protect **SAI** information, including:

- Access control mechanisms.
- Strong authentication controls.
- Secure configuration of systems.
- Vulnerability management processes.
- Malware protection controls.
- Security monitoring mechanisms.
- Network security controls.
- Backup and recovery arrangements.
- Secure software development practices, where applicable.

---

9. ACCESS CONTROL REQUIREMENTS

- Third-party access shall be approved on a business need-to-know basis.
- Access shall be restricted to the minimum level required.
- User accounts shall be individually assigned and attributable.
- Shared accounts shall be avoided wherever possible.
- Privileged access shall be strictly controlled and monitored.
- Remote access shall be authorized and secured.
- Access rights shall be reviewed periodically.
- Third-party access shall be revoked immediately upon termination of services or no longer being required.

10. DATA PROTECTION AND PRIVACY

Third parties processing personal data on behalf of **SAI** shall:

- Process data only for authorized and agreed purposes.
- Comply with the Digital Personal Data Protection Act, 2023 and applicable legal requirements.
- Implement appropriate technical and organizational safeguards.
- Ensure confidentiality of personal and sensitive information.
- Restrict disclosure of information to unauthorized parties.
- Securely delete or return information upon contract termination.
- Notify **SAI** of any actual or suspected personal data breach without undue delay.

---

11. CLOUD SERVICE PROVIDERS

Where services are hosted in cloud environments:

- Cloud providers shall implement industry-recognized security controls.
- Data residency requirements shall be evaluated and documented.
- Encryption shall be implemented for sensitive data where applicable.
- Security logs shall be maintained and protected.
- Access management controls shall be appropriately configured.
- Security incidents shall be promptly reported to **SAI**.

---

12. CONTRACTUAL SECURITY REQUIREMENTS

All applicable agreements shall include, where appropriate:

- Confidentiality obligations.
- Data protection and privacy requirements.
- Information security requirements.
- Right to audit clauses.
- Incident notification requirements.
- Subcontractor management obligations.
- Data retention and disposal requirements.
- Business continuity requirements.
- Termination and exit provisions.
- Regulatory compliance obligations.

- Where a third party is engaged in providing services, infrastructure or support relating to SAI's Aadhaar authentication arrangement, the relevant contract or security schedule shall, as applicable, incorporate the UIDAI-related information security, confidentiality, access restriction, incident reporting, audit cooperation, data retention and secure deletion requirements applicable to that engagement.
- SAI shall assess the security risks associated with such third parties before engagement and periodically thereafter, as appropriate to the risk and applicable requirements. Third-party access to Aadhaar-related information and systems shall be restricted to authorised purposes and revoked when no longer required.

13. SECURITY MONITORING AND COMPLIANCE

SAI reserves the right to:

- Review compliance with contractual security obligations.
- Request evidence of security control implementation.
- Conduct security assessments and audits where contractually permitted.
- Monitor security performance of critical third parties.
- Require remediation of identified security weaknesses.

---

14. INFORMATION SECURITY INCIDENT MANAGEMENT

Third parties shall:

- Report actual or suspected security incidents affecting **SAI** information immediately.
- Cooperate with **SAI** during investigations.
- Preserve relevant logs and evidence.
- Support containment, eradication, and recovery activities.
- Implement corrective and preventive actions as necessary.

Incidents shall be managed in accordance with applicable **SAI** incident management procedures and CERT-In requirements.

---

15. THIRD PARTY OFFBOARDING

Upon termination of services:

- Access rights shall be revoked.
- Credentials shall be disabled or removed.
- Organization information shall be returned or securely destroyed.
- Assets shall be recovered where applicable.
- Confidentiality obligations shall continue beyond contract termination where

applicable.

- Evidence of data deletion may be requested.

---

16. EXCEPTIONS

Any exception to this Policy shall:

- Be documented with proper justification.
- Be risk assessed.
- Be approved by the competent authority.
- Include compensating controls where necessary.
- Be reviewed periodically.

---

17. COMPLIANCE AND MONITORING

The IT Division shall monitor compliance through:

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

Non-compliance may result in contractual actions, suspension of access, service restrictions, or termination of services.

---

18. POLICY REVIEW

This Policy shall be reviewed at least annually and whenever required due to:

- Changes in applicable laws or regulations.
- Updated CERT-In or MeitY requirements.
- Significant cyber security incidents.
- Major organizational changes.
- Findings from audits or assessments.
- Emerging cyber security threats.

---

19. EFFECTIVE DATE

This Policy becomes effective on 27.10.2026 by the approval by the Competent Authority and shall remain in force until amended, superseded, or withdrawn.

---

20. APPROVAL

This Third-Party Information Security Policy is approved by the Competent Authority of **SAI** and shall be implemented across all applicable third-party engagements.

---

21. REFERENCES

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

Information Technology Act, 2000

- Reference: Government of India - Ministry of Electronics & Information Technology

Digital Personal Data Protection Act, 2023

- Reference: Digital Personal Data Protection Act, 2023

CERT-In Directions under Section 70B dated 28 April 2022

- Reference: CERT-In Directions

CERT-In Guidelines on Information Security Practices for Government Entities (CISG-2023-01)

- Reference: CERT-In Government Entity Guidelines

MeitY Guidelines on Information Security Practices for Government Entities

- Reference: MeitY Information Security Guidelines

ISO/IEC 27001:2022 Information Security Management Systems

- Reference: https://www.iso.org/isoiec-27001-information-security.html

ISO/IEC 27002:2022 Information Security Controls

- Reference: https://www.iso.org/standard/75652.html

NIST Cybersecurity Framework (CSF 2.0)

- Reference: NIST Cybersecurity Framework

***

Chattopadhyay