SPORTS AUTHORITY OF INDIA
IT DIVISION

DATA PRIVACY AND DATA PROTECTION 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 Data Privacy and Data Protection Policy is to establish a comprehensive framework for the lawful collection, processing, storage, transmission, sharing, retention, protection, and disposal of personal data and sensitive information handled by **SAI**.

This Policy aims to:

- Protect the privacy rights of individuals.
- Ensure compliance with applicable legal, regulatory, and contractual obligations.
- Safeguard personal information from unauthorized access, disclosure, alteration, loss, or destruction.
- Define roles and responsibilities for data privacy and protection.
- Promote privacy-by-design principles across business processes and information systems.
- Ensure responsible and accountable data processing practices.

---

2. SCOPE

This Policy shall apply to:

- All employees, contractual personnel, interns, consultants, service providers, vendors, and third parties handling information on behalf of **SAI**.
- All personal data, sensitive personal data, business information, and other regulated information processed by **SAI**.
- All systems, applications, databases, cloud environments, storage media, and communication channels used for data processing.
- Physical and electronic records maintained by **SAI**.

---

3. OBJECTIVES

The objectives of this Policy are to:

- Ensure lawful and transparent processing of personal data.
- Protect confidentiality, integrity, and availability of information.
- Implement appropriate technical and organizational safeguards.
- Minimize privacy and cybersecurity risks.
- Protect the rights of data principals.
- Promote accountability and compliance throughout the organization.

4. REFERENCE DOCUMENTS AND APPLICABLE REQUIREMENTS

This Policy shall be read in conjunction with:

- Digital Personal Data Protection Act (DPDP Act), 2023.
- Information Technology Act, 2000.
- CERT-In Directions under Section 70B dated 28 April 2022.
- CERT-In Guidelines on Information Security Practices for Government Entities (CISG-2023-01).
- MeitY Guidelines on Information Security Practices.
- ISO/IEC 27001:2022.
- ISO/IEC 27701:2019 Privacy Information Management System.
- ISO/IEC 27002:2022.

In case of conflict, applicable legal and regulatory requirements shall prevail.

5. DEFINITIONS AND ABBREVIATIONS

Term	Definition
Personal Data	Any information relating to an identified or identifiable individual
Sensitive Data	Information requiring enhanced protection due to business, legal, or privacy implications
Data Principal	Individual to whom personal data relates
Data Fiduciary	Entity determining the purpose and means of processing personal data
Processing	Any operation performed on personal data

DPO	Data Protection Officer
Data Breach	Unauthorized access, disclosure, loss, destruction, or alteration of information
Consent	Free, specific, informed, and unambiguous agreement of the data principal

6. ROLES AND RESPONSIBILITIES

6.1 Management

Management shall:

- Provide support for privacy and data protection activities.
- Ensure sufficient resources are available.
- Review compliance status periodically.

6.2 Data Protection Officer (DPO)

The DPO shall:

- Monitor compliance with this Policy.
- Provide guidance on privacy obligations.
- Coordinate privacy impact assessments.
- Monitor data breach reporting activities.
- Conduct privacy awareness initiatives.

6.3 IT Division

The IT Division shall:

- Implement technical security controls.
- Ensure protection of personal data.
- Monitor system security.
- Support investigations and incident response activities.

6.4 Employees and Users

All personnel shall:

- Handle personal data responsibly.
- Follow approved security procedures.
- Report privacy incidents immediately.
- Maintain confidentiality of information.

7. DATA PRIVACY PRINCIPLES

SAI shall ensure that all personal data is processed in accordance with the following principles:

7.1 Lawfulness, Fairness and Transparency

Personal data shall be collected and processed lawfully, fairly, and transparently. Individuals shall be informed regarding the purpose of collection, usage, sharing arrangements, retention requirements, and applicable privacy rights.

7.2 Purpose Limitation

Personal data shall only be collected for specific, explicit, and legitimate purposes. Data shall not be used for purposes incompatible with the original collection objective unless legally permitted.

7.3 Data Minimization

Only the minimum amount of personal data necessary to achieve the intended purpose shall be collected, processed, stored, or shared.

7.4 Accuracy and Data Quality

Reasonable measures shall be implemented to ensure that personal data remains accurate, complete, relevant, and up to date. Inaccurate or obsolete data shall be corrected or removed where appropriate.

7.5 Storage Limitation

Personal data shall not be retained longer than necessary. Retention periods shall be based on legal, regulatory, contractual, operational, and business requirements.

7.6 Integrity and Confidentiality

Appropriate technical and organizational measures shall be implemented to protect personal data against unauthorized access, disclosure, alteration, destruction, theft, or loss.

7.7 Accountability

Departments handling personal data shall be responsible for demonstrating compliance with applicable privacy obligations and organizational requirements.

7.8 Privacy by Design and Privacy by Default

Privacy requirements shall be integrated into the design, development, implementation, and operation of systems, applications, and business processes. By default, only necessary personal data shall be processed.

---

8. DATA COLLECTION AND PROCESSING

- Personal data shall be collected only for legitimate and authorized purposes.
- Data collection shall be limited to information necessary for identified purposes.
- Appropriate privacy notices shall be provided.

- Processing activities shall comply with applicable laws and approved procedures.
- Sensitive processing activities may be subject to additional controls.

---

9. CONSENT MANAGEMENT

Where consent is required:

- Consent shall be obtained using clear and understandable language.
- Consent records shall be maintained.
- Data principals shall be able to withdraw consent where legally permissible.
- Withdrawal mechanisms shall be documented and communicated.

---

10. DATA CLASSIFICATION

Information shall be classified as:

- Public
- Internal
- Confidential
- Restricted

Appropriate protection controls shall be applied based on classification levels.

---

11. ACCESS CONTROL REQUIREMENTS

Access to personal data shall:

- Follow the principle of least privilege.
- Be granted on a need-to-know basis.
- Be approved by authorized personnel.
- Be periodically reviewed.
- Be revoked when no longer required.

Privileged access shall be subject to enhanced controls.

---

12. ENCRYPTION AND DATA SECURITY

SAI shall implement appropriate controls including:

- Encryption of sensitive information in transit and at rest where applicable.

- Multi-factor authentication for critical systems.
- Secure password management.
- Security monitoring and logging.
- Malware protection measures.
- Backup and recovery arrangements.
- Network security controls.

13. DATA SHARING AND THIRD-PARTY PROCESSING

Where personal data is shared:

- Appropriate agreements shall be executed.
- Third parties shall implement adequate security controls.
- Data sharing shall be limited to authorized purposes.
- Privacy and confidentiality obligations shall be documented.
- Third-party compliance may be assessed periodically.

14. DATA RETENTION

14.1 SAI shall:

- Establish and maintain retention schedules.
- Retain information only for required periods.
- Review retained data periodically.
- Ensure legal and regulatory retention obligations are met.

14.2 Where Aadhaar numbers, Virtual IDs (VID), authentication-related information or other Aadhaar-linked information are processed in connection with SAI's activities, such information shall be collected, accessed, used, transmitted, stored and disposed of strictly in accordance with applicable UIDAI requirements and law.

SAI shall not retain Aadhaar numbers, VID or authentication-related information where such retention is prohibited under the applicable legal or regulatory framework. Where retention or storage of Aadhaar numbers is permitted and an Aadhaar Data Vault or other prescribed safeguard is required, SAI shall ensure implementation of the applicable storage, access-control and security requirements. Where prescribed, Aadhaar numbers maintained in other systems shall be replaced with appropriate reference keys.

15. DATA DISPOSAL

Data disposal activities shall ensure:

- Secure deletion of electronic information.

- Secure destruction of physical records.
- Prevention of unauthorized recovery.
- Documentation of disposal activities where appropriate.

---

16. PRIVACY IMPACT ASSESSMENT

Privacy Impact Assessments (PIAs) shall be conducted where appropriate, including:

- New systems processing personal data.
- Major technology changes.
- Large-scale processing activities.
- Introduction of new data collection methods.

---

17. DATA BREACH MANAGEMENT

All actual or suspected privacy incidents shall:

- Be reported immediately.
- Be investigated appropriately.
- Be documented and tracked.
- Have corrective and preventive actions implemented.
- Be escalated in accordance with organizational procedures.

Where required, regulatory notification obligations shall be fulfilled.

---

18. INDIVIDUAL RIGHTS MANAGEMENT

Subject to applicable legal and regulatory requirements, **SAI** shall establish mechanisms supporting:

- Access requests.
- Correction requests.
- Data update requests.
- Consent withdrawal requests.
- Redressal mechanisms.

All requests shall be handled through approved processes.

---

19. TRAINING AND AWARENESS

SAI shall conduct periodic awareness activities covering:

- Data privacy obligations.
- Personal data protection requirements.
- Data breach reporting procedures.
- Secure handling of information.
- Regulatory obligations.

Training records shall be maintained.

20. COMPLIANCE AND MONITORING

Compliance with this Policy shall be monitored through:

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

Non-compliance may result in disciplinary, contractual, or legal actions.

21. EXCEPTION MANAGEMENT

Any exception to this Policy shall:

- Be formally documented.
- Include business justification.
- Be risk assessed.
- Receive appropriate approval.
- Include compensating controls where necessary.

22. POLICY REVIEW

This Policy shall be reviewed:

- At least annually.
- Following regulatory changes.
- Following significant incidents.
- Following technology changes.
- Following audit recommendations.

23. EFFECTIVE DATE

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

24. APPROVAL

This Data Privacy and Data Protection Policy is approved by the Competent Authority of **SAI** and shall be implemented across the organization.

---

25. REFERENCES

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

1. **Digital Personal Data Protection Act, 2023 (DPDP Act)**
   - Link: https://www.meity.gov.in
2. **Information Technology Act, 2000**
   - 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. **ISO/IEC 27701:2019 Privacy Information Management System**
   - Link: https://www.iso.org/standard/71670.html

***