SPORTS AUTHORITY OF INDIA

IT DIVISION

ASSET MANAGEMENT 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 Asset Management Policy is to establish minimum requirements for the identification, ownership, classification, acquisition, use, protection, maintenance, tracking, transfer, disposal, and management of information assets throughout their lifecycle.

This Policy aims to ensure that information assets supporting the operations of **SAI** are appropriately identified, protected, monitored, and managed against loss, theft, misuse, unauthorized access, disclosure, damage, or destruction.

---

2. SCOPE

This Policy shall apply to:

- All employees, contractual personnel, consultants, interns, vendors, service providers, and authorized users having access to **SAI** assets.
- All information assets owned, leased, managed, operated, or used by **SAI**.
- Physical and logical assets including hardware, software, applications, databases, cloud resources, network infrastructure, storage media, and information maintained by **SAI**.
- Third-party assets used for processing, storing, or transmitting **SAI** information.

---

3. REFERENCE DOCUMENTS AND APPLICABLE REQUIREMENTS

This Policy shall be read in conjunction with:

- Information Technology Act, 2000.
- Digital Personal Data Protection Act, 2023.
- 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 for Government Entities.

- ISO/IEC 27001:2022.
- ISO/IEC 27002:2022.
- NIST Cybersecurity Framework (CSF 2.0).
- **SAI** Information Security Policies and Procedures.

Where statutory or regulatory requirements impose stricter controls, those requirements shall prevail.

---

4. DEFINITIONS AND ABBREVIATIONS

Term	Description
Asset	Anything that has value to **SAI** and supports organizational operations
Information Asset	Information, software, hardware, services, people, and facilities supporting business operations
Asset Owner	Individual responsible for asset classification, protection, and usage approval
Asset Custodian	Individual or department responsible for day-to-day asset management
Asset Inventory	Authorized record of organizational assets
Media	Physical or electronic storage devices used for storing information
End-of-Life (EOL)	Point at which a product is no longer supported by the manufacturer

5. ROLES AND RESPONSIBILITIES

5.1 IT Division

The IT Division shall:

- Establish and maintain asset management processes.
- Maintain a comprehensive asset inventory.
- Implement controls for asset protection.
- Track the asset lifecycle.
- Conduct periodic asset reviews and audits.
- Ensure secure disposal of information assets.

5.2 Asset Owners

Asset Owners shall:

- Classify assets based on business and security requirements.

- Approve access and usage requirements.
- Ensure assets are protected appropriately.
- Review asset inventories periodically.

5.3 Asset Custodians

Asset Custodians shall:

- Maintain asset records.
- Monitor asset status and usage.
- Report lost, stolen, damaged, or compromised assets.
- Ensure assets remain protected in accordance with organizational requirements.

5.4 Users

All users shall:

- Use assets only for authorized business purposes.
- Protect assigned assets from misuse or loss.
- Report asset-related incidents immediately.
- Return organizational assets upon termination or transfer.

---

6. ASSET MANAGEMENT PRINCIPLES

SAI shall ensure that:

- All information assets are identified and inventoried.
- Asset ownership is formally assigned.
- Assets are protected according to their classification.
- Asset risks are regularly assessed.
- Asset lifecycle activities are documented and monitored.
- Asset disposal is performed securely.

---

7. ASSET INVENTORY MANAGEMENT

A comprehensive inventory of information assets shall be maintained.

The inventory shall include:

- Asset identifier.
- Asset type.
- Asset owner.
- Asset custodian.

- Asset location.
- Classification level.
- Asset status.
- Purchase and warranty details where applicable.

Asset inventories shall be reviewed periodically to ensure accuracy and completeness.

---

8. ASSET OWNERSHIP

All information assets shall have a designated owner responsible for:

- Asset classification.
- Security requirements.
- Access authorization.
- Risk management.
- Asset review and validation.

Ownership shall remain documented throughout the asset lifecycle.

---

9. ASSET CLASSIFICATION

Assets shall be classified based on business value, sensitivity, legal requirements, and operational importance.

The following classifications may be adopted:

- Public
- Internal
- Confidential
- Restricted

Appropriate security controls shall be implemented according to classification levels.

---

10. ACCEPTABLE USE OF ASSETS

Organizational assets shall be used only for authorized business purposes.

Users shall not:

- Install unauthorized software.
- Modify asset configurations without authorization.
- Use assets for unlawful activities.
- Circumvent security controls.

- Share assets without approval.

Usage shall comply with organizational policies and applicable laws.

---

11. INFORMATION HANDLING REQUIREMENTS

Information assets shall be handled according to their classification.

Security controls may include:

- Access restrictions.
- Encryption.
- Secure storage.
- Secure transmission.
- Retention controls.
- Monitoring mechanisms.

Sensitive information shall receive enhanced protection.

---

12. ASSET PROTECTION REQUIREMENTS

Appropriate safeguards shall be implemented to protect assets against:

- Unauthorized access.
- Theft.
- Damage.
- Loss.
- Tampering.
- Malware attacks.
- Environmental threats.

Security controls shall be commensurate with business and security risks.

---

13. MOBILE AND PORTABLE ASSETS

Portable assets including laptops, tablets, smartphones, removable storage devices, and other mobile equipment shall:

- Be protected against theft and loss.
- Use encryption where appropriate.
- Be password protected.

- Remain under user control and supervision.
- Be reported immediately if lost, stolen, or compromised.

---

14. SOFTWARE ASSET MANAGEMENT

SAI shall maintain controls over software assets, including:

- Licensing compliance.
- Approved software inventories.
- Software version management.
- Removal of unauthorized software.
- Regular software reviews.

Only authorized and licensed software shall be installed on organizational systems.

---

15. CLOUD ASSET MANAGEMENT

Where cloud services are utilized:

- Cloud assets shall be inventoried.
- Ownership shall be assigned.
- Security responsibilities shall be documented.
- Appropriate security controls shall be implemented.
- Cloud resources shall be reviewed periodically.

---

16. ASSET TRANSFER AND MOVEMENT

Any movement or transfer of assets shall:

- Be authorized.
- Be documented.
- Maintain asset accountability.
- Preserve confidentiality and integrity of information.

Asset records shall be updated accordingly.

---

17. ASSET RETURN PROCEDURES

Employees, contractors, consultants, and third parties shall return all organizational assets:

- Upon termination of employment.

- Upon completion of contractual engagements.
- Upon transfer of responsibilities.
- Upon request by authorized management.

Asset return shall be documented and verified.

---

18. ASSET DISPOSAL AND DECOMMISSIONING

Assets shall be securely disposed of when:

- No longer required.
- Replaced.
- Decommissioned.
- Reaching end-of-life.

Before disposal:

- Information shall be securely erased.
- Storage media shall be sanitized.
- Sensitive information shall be destroyed appropriately.
- Asset records shall be updated.

Disposal activities shall be documented.

---

19. LOSS, THEFT AND DAMAGE REPORTING

Users shall immediately report:

- Lost assets.
- Stolen assets.
- Damaged assets.
- Compromised assets.
- Unauthorized asset access.

Appropriate investigation and remediation activities shall be initiated.

---

20. ASSET REVIEW AND AUDIT

Periodic reviews shall be conducted to:

- Verify asset ownership.
- Validate inventory accuracy.

- Identify unauthorized assets.
- Assess security controls.
- Ensure compliance with this Policy.

Asset audits may be conducted periodically by authorized personnel.

---

21. BUSINESS CONTINUITY AND RECOVERY

Critical assets shall be identified and protected to support:

- Business continuity requirements.
- Disaster recovery planning.
- System restoration activities.
- Continuity of critical services.

Appropriate backup and recovery arrangements shall be maintained.

---

22. EXCEPTIONS

Any exception to this Policy shall:

- Be documented.
- Include appropriate justification.
- Be risk assessed.
- Be approved by the competent authority.
- Include compensating controls where necessary.

Approved exceptions shall be reviewed periodically.

---

23. COMPLIANCE AND MONITORING

Compliance with this Policy shall be monitored through:

- Asset reviews.
- Asset inventories.
- Internal audits.
- External audits.
- Risk assessments.
- Compliance assessments.

Non-compliance may result in disciplinary action, access restrictions, or contractual action where applicable.

---

24. POLICY REVIEW

This Policy shall be reviewed:

- At least annually.
- Following significant organizational changes.
- Following major security incidents.
- Following changes in applicable regulations.
- Following audit recommendations.
- Following technology changes.

---

25. EFFECTIVE DATE

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

---

26. APPROVAL

This Asset Management Policy is approved by the Competent Authority of **SAI** and shall be implemented across all organizational assets.

---

27. REFERENCES

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

1. **Information Technology Act, 2000**
   Link: MeitY Official Website
2. **Digital Personal Data Protection Act, 2023**
   Link: DPDP Act Information
3. **CERT-In Directions under Section 70B dated 28 April 2022**
   Link: CERT-In Directions
4. **CERT-In Guidelines on Information Security Practices for Government Entities (CISG-2023-01)**
   Link: CERT-In Government Entity Guidelines
5. **MeitY Guidelines on Information Security Practices for Government Entities**
   Link: MeitY Official Website
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. **NIST SP 800-53 Security and Privacy Controls**
   Link: NIST SP 800-53

10. **ISO/IEC 55001 Asset Management Systems**
    Link: https://www.iso.org/standard/55088.html

***