SPORTS AUTHORITY OF INDIA
IT DIVISION

PHYSICAL SECURITY AND ACCESS CONTROL 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 Physical Security and Access Control Policy is to establish minimum security requirements for protecting **SAI** personnel, facilities, information assets, critical infrastructure, equipment, and supporting resources from unauthorized physical access, theft, damage, interference, disruption, or malicious activities.

This Policy aims to ensure that appropriate physical and environmental security controls are implemented to safeguard organizational assets and maintain business continuity.

---

2. SCOPE

This Policy applies to:

- All employees, consultants, contractors, interns, vendors, visitors, and third parties.
- All **SAI** offices, facilities, data centers, server rooms, communication rooms, storage locations, and operational areas.
- All information processing facilities, workstations, communication equipment, storage media, and other critical assets.
- All areas where **SAI** information is processed, stored, transmitted, or accessed.

---

3. OBJECTIVES

The objectives of this Policy are to:

- Prevent unauthorized physical access to organizational facilities.
- Protect information assets and critical infrastructure.
- Ensure controlled and monitored access to secure areas.
- Reduce risks arising from theft, vandalism, sabotage, and environmental threats.
- Establish accountability for physical access management.
- Support regulatory, legal, and information security compliance requirements.

---

4. 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 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.
- **SAI** Information Security Policies and Procedures.

---

5. TERMS AND ABBREVIATIONS

Term	Definition
Physical Security	Protection of facilities, personnel, and assets against physical threats
Secure Area	Area requiring controlled access mechanisms
Visitor	Any person not employed by **SAI**
Access Card	Physical credential used for facility access
CCTV	Closed Circuit Television
Critical Area	Facility area containing sensitive information or critical infrastructure

6. ROLES AND RESPONSIBILITIES

6.1 Management

Management shall:

- Ensure implementation of physical security controls.
- Allocate resources for physical security measures.
- Review physical security risks periodically.

6.2 Administration Department

The Administration Department shall:

- Maintain physical access control systems.
- Manage visitor access records.

- Monitor security guards and surveillance systems.
- Coordinate physical security reviews.

6.3 IT Division

The IT Division shall:

- Protect information processing facilities.
- Secure server rooms and network infrastructure.
- Support physical security controls for information assets.

6.4 Employees

Employees shall:

- Comply with physical security requirements.
- Protect access cards and keys.
- Report security weaknesses and incidents.
- Challenge unidentified persons where appropriate.

---

7. PHYSICAL SECURITY PRINCIPLES

SAI shall ensure:

- Physical access is restricted to authorized personnel.
- Critical facilities are adequately protected.
- Security measures are proportionate to identified risks.
- Physical security incidents are detected and responded to promptly.
- Physical security controls are reviewed periodically.

---

8. PHYSICAL SECURITY PERIMETERS

Appropriate security perimeters shall be established around facilities containing critical information assets.

Measures may include:

- Access-controlled entry points.
- Security barriers.
- Security guards.
- Fencing where applicable.
- CCTV monitoring.
- Visitor management controls.

Access points shall be limited and monitored.

---

9. SECURE AREA CONTROLS

Critical and secure areas shall include:

- Data Centers.
- Server Rooms.
- Network Operations Rooms.
- Security Operations Centers.
- Record Storage Facilities.
- Communication Equipment Rooms.

Access to secure areas shall:

- Require prior authorization.
- Be restricted to approved personnel.
- Be monitored and logged.
- Be reviewed periodically.

---

10. PHYSICAL ACCESS CONTROL

Physical access controls shall include:

- Access cards.
- Biometric controls where applicable.
- Visitor registration procedures.
- Security guards.
- Electronic access management systems.

Access rights shall:

- Be approved by authorized personnel.
- Follow the principle of least privilege.
- Be reviewed regularly.
- Be revoked immediately upon termination or transfer.

---

11. VISITOR MANAGEMENT

All visitors shall:

- Register at designated reception areas.
- Produce valid identification where required.
- Receive visitor passes.
- Be escorted in restricted areas.
- Return visitor badges before departure.

Visitor logs shall be retained and reviewed periodically.

---

12. CCTV AND SURVEILLANCE

Where implemented:

- CCTV systems shall monitor critical areas.
- Recording systems shall be protected from unauthorized access.
- Retention periods shall comply with organizational and legal requirements.
- Surveillance data shall only be accessed by authorized personnel.

Monitoring activities shall comply with applicable privacy requirements.

---

13. SERVER ROOM AND DATA CENTER SECURITY

Facilities housing critical systems shall implement:

- Restricted physical access.
- Environmental monitoring.
- Fire protection systems.
- Power backup arrangements.
- CCTV surveillance.
- Access logging mechanisms.

Only authorized personnel shall be granted access.

---

14. EQUIPMENT SECURITY

Organizational equipment shall be protected against:

- Theft.
- Unauthorized use.
- Damage.
- Environmental risks.

Equipment placement shall consider:

- Physical security requirements.
- Environmental conditions.
- Access restrictions.

---

15. CLEAR DESK AND CLEAR SCREEN REQUIREMENTS

Employees shall:

- Secure confidential information when unattended.
- Lock workstations when leaving work areas.
- Avoid leaving sensitive information exposed.
- Remove confidential material from desks after use.

Physical documents shall be stored securely.

---

16. PROTECTION AGAINST ENVIRONMENTAL THREATS

SAI shall implement safeguards against:

- Fire.
- Flooding.
- Electrical failures.
- Temperature fluctuations.
- Water leakage.
- Natural disasters.

Critical facilities shall maintain appropriate environmental controls.

---

17. REMOVAL OF ORGANIZATIONAL ASSETS

Assets shall not be removed from organizational premises without appropriate authorization.

Where removal is approved:

- Asset records shall be maintained.
- Custody shall be documented.
- Security controls shall remain applicable.

---

18. PHYSICAL SECURITY INCIDENT MANAGEMENT

The following events shall be treated as physical security incidents:

- Unauthorized entry.
- Forced access attempts.
- Theft of assets.
- Loss of access cards.
- Physical damage to infrastructure.
- Unauthorized photography or recording.
- Suspicious activity within facilities.

All incidents shall be reported immediately and investigated appropriately.

---

19. CONTRACTOR AND THIRD-PARTY ACCESS

Third-party personnel shall:

- Sign confidentiality agreements where applicable.
- Follow organizational security requirements.
- Be granted only authorized access.
- Be supervised where necessary.

Access rights shall be removed when services conclude.

---

20. BUSINESS CONTINUITY AND EMERGENCY MANAGEMENT

Physical security arrangements shall support:

- Business continuity objectives.
- Emergency response activities.
- Evacuation procedures.
- Critical facility recovery.

Emergency contact lists and evacuation plans shall be maintained.

21. COMPLIANCE AND MONITORING

Compliance shall be monitored through:

- Physical security inspections.
- CCTV reviews.
- Access log reviews.
- Internal audits.

- External audits.
- Risk assessments.

Security deficiencies shall be addressed promptly.

---

22. EXCEPTION MANAGEMENT

Any exception to this Policy shall:

- Be documented.
- Include valid business justification.
- Be risk assessed.
- Receive management approval.
- Include compensating controls.

---

23. POLICY REVIEW

This Policy shall be reviewed:

- Annually.
- Following major incidents.
- Following changes in facilities.
- Following audit findings.
- Following regulatory changes.

---

24. EFFECTIVE DATE

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

---

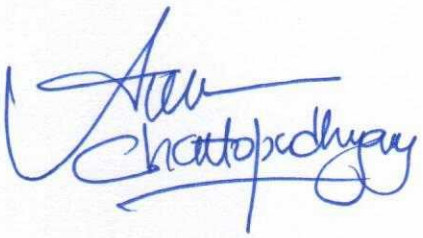
25. APPROVAL

This Physical Security and Access Control Policy is approved by the Competent Authority of **SAI** and shall be applicable throughout the organization.

---

26. 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. **ISO/IEC 27001 Annex A.7 - Physical and Environmental Security Controls**
   Link: https://www.iso.org
9. **National Building Code of India (NBC)**
   Link: https://www.services.bis.gov.in
10. **NIST SP 800-53 Physical and Environmental Protection Controls**
    Link: NIST Publications

***