SPORTS AUTHORITY OF INDIA
IT DIVISION

INCIDENT 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 Incident Management Policy is to establish a structured and consistent approach for identifying, reporting, assessing, responding to, managing, recovering from, and reporting information security incidents that may affect the confidentiality, integrity, or availability of **SAI** information assets, systems, applications, networks, services, or data.

This Policy aims to minimize operational disruption, reduce security risks, preserve evidence, ensure timely response to cyber incidents, and support compliance with applicable Government of India regulatory and cybersecurity requirements.

---

2. SCOPE

This Policy shall apply to:

- All employees, contractual staff, interns, consultants, vendors, service providers, and authorized users.
- All information systems, applications, servers, databases, cloud environments, endpoints, and network infrastructure owned, operated, or managed by **SAI**.
- All cyber security incidents, information security incidents, data breaches, privacy incidents, and technology-related disruptions affecting **SAI**.

---

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 27035: Information Security Incident Management.
- NIST Cybersecurity Framework (CSF 2.0).
- **SAI** Information Security Policies and Procedures.

Where legal or regulatory requirements impose stricter obligations, such requirements shall prevail.

---

4. DEFINITIONS AND ABBREVIATIONS

Term	Description
Incident	Any event that compromises or may compromise information security
Cyber Security Incident	Incident affecting information systems, networks, applications, or digital services
Data Breach	Unauthorized access, disclosure, alteration, destruction, or loss of information
CERT-In	Indian Computer Emergency Response Team
IOC	Indicator of Compromise
CSIRT	Cyber Security Incident Response Team
Root Cause Analysis	Process used to determine the underlying cause of an incident

5. ROLES AND RESPONSIBILITIES

5.1 IT Division

The IT Division shall:

- Maintain incident management processes.
- Coordinate incident response activities.
- Investigate security incidents.
- Maintain incident records.
- Liaise with management and regulatory authorities where required.
- Conduct lessons learned reviews.

5.2 Department Heads

Department Heads shall:

- Report incidents affecting their business units.
- Support investigations.

- Assist in implementation of corrective actions.

5.3 Employees and Users

All users shall:

- Immediately report suspected incidents.
- Cooperate during investigations.
- Follow incident response instructions.
- Preserve relevant information and evidence.

5.4 Third Parties

Third parties shall:

- Promptly notify **SAI** of incidents affecting **SAI** information assets.
- Support investigations and remediation activities.
- Preserve evidence where required.

---

6. INCIDENT MANAGEMENT PRINCIPLES

SAI shall ensure that:

- All incidents are reported and managed consistently.
- Incident response activities are risk-based.
- Appropriate evidence is preserved.
- Business operations are restored promptly.
- Regulatory reporting requirements are fulfilled.
- Lessons learned are incorporated into security improvements.

---

7. INCIDENT IDENTIFICATION

Potential incidents may be identified through:

- Security monitoring tools.
- Security Information and Event Management (SIEM).
- Antivirus and Endpoint Detection and Response (EDR) solutions.
- Vulnerability assessments.
- User reports.
- Vendor notifications.
- Third-party threat intelligence feeds.
- CERT-In advisories.

8. INCIDENT REPORTING

All users shall immediately report:

- Malware infections.
- Ransomware attacks.
- Phishing attacks.
- Unauthorized access attempts.
- Data breaches.
- Lost or stolen devices.
- Website defacement.
- Denial-of-Service (DoS) attacks.
- Privilege misuse.
- Unauthorized disclosure of information.
- Any suspicious activity affecting **SAI** systems.

Reports shall be submitted through designated reporting channels established by **SAI**.

9. INCIDENT CLASSIFICATION

Incidents shall be classified based on severity and impact.

Severity	Description
Critical	Severe impact on critical business operations or sensitive information
High	Significant impact requiring urgent action
Medium	Moderate operational impact
Low	Limited impact with minimal operational disruption

Classification shall consider:

- Impact on confidentiality.
- Impact on integrity.
- Impact on availability.
- Regulatory implications.
- Financial implications.
- Reputational impact.

10. INCIDENT RESPONSE PROCESS

The incident management process shall include:

10.1 Detection and Reporting

Identification and reporting of incidents.

10.2 Assessment and Triage

Evaluation of severity, impact, and priority.

10.3 Containment

Actions to limit the spread and impact of the incident.

10.4 Investigation

Determination of root cause, affected assets, attack vectors, and impact.

10.5 Eradication

Removal of malicious code, unauthorized access, vulnerabilities, or threats.

10.6 Recovery

Restoration of affected services and systems.

10.7 Closure

Documentation and formal closure after validation.

---

11. EVIDENCE PRESERVATION

During incident investigations:

- Relevant logs shall be preserved.
- System images may be collected where required.
- Evidence shall be protected against alteration.
- Chain-of-custody records shall be maintained where necessary.
- Digital forensic procedures shall be followed when applicable.

---

12. CYBER SECURITY INCIDENT NOTIFICATION

Where required:

- Incidents shall be reported to management.
- Regulatory reporting obligations shall be fulfilled.
- CERT-In reporting requirements shall be complied with.
- Relevant stakeholders shall be informed on a need-to-know basis.

13. COMMUNICATION MANAGEMENT

During significant incidents:

- Internal communication shall be coordinated.
- External communication shall be authorized.
- Media interactions shall be managed through authorized personnel.
- Incident information shall be protected from unauthorized disclosure.

14. DATA BREACH MANAGEMENT

In the event of a data breach:

- Immediate containment actions shall be initiated.
- Impact assessment shall be performed.
- Affected information shall be identified.
- Root cause shall be determined.
- Corrective and preventive actions shall be implemented.
- Applicable legal notification obligations shall be assessed.

15. ROOT CAUSE ANALYSIS

For significant incidents, **SAI** shall conduct:

- Detailed investigation.
- Root cause analysis.
- Impact determination.
- Corrective action planning.
- Preventive action planning.

16. CORRECTIVE AND PREVENTIVE ACTIONS

Appropriate actions may include:

- Security control enhancements.
- Patch deployment.
- Configuration changes.
- User awareness activities.

- Process improvements.
- Technology improvements.

---

17. INCIDENT RECORDS AND DOCUMENTATION

The IT Division shall maintain records including:

- Incident description.
- Detection date and time.
- Classification.
- Investigation details.
- Actions taken.
- Closure details.
- Lessons learned.

---

18. TRAINING AND AWARENESS

SAI shall conduct awareness activities covering:

- Incident identification.
- Phishing reporting.
- Cyber security threats.
- Reporting procedures.
- Evidence handling requirements.

---

19. COMPLIANCE AND MONITORING

The effectiveness of this Policy shall be monitored through:

- Security reviews.
- Incident trend analysis.
- Internal audits.
- External assessments.
- Tabletop exercises.
- Compliance reviews.

Non-compliance may result in disciplinary or contractual action.

---

20. POLICY REVIEW

This Policy shall be reviewed:

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

---

21. EFFECTIVE DATE

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

---

22. APPROVAL

This Incident Management Policy is approved by the Competent Authority of **SAI** and shall be implemented across the organization.

---

23. 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 27035 Information Security Incident Management**
   Link: https://www.iso.org

***