SPORTS AUTHORITY OF INDIA
IT DIVISION

PATCH 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 Patch Management Policy is to establish minimum requirements and responsibilities for the identification, assessment, testing, deployment, verification, and monitoring of security patches, updates, hotfixes, firmware updates, and service packs applicable to information systems, applications, databases, cloud environments, network devices, and endpoints operated or managed by **SAI**.

This Policy aims to reduce cybersecurity risks arising from known vulnerabilities, ensure timely remediation of security weaknesses, maintain system stability, and support compliance with applicable legal, regulatory, and security requirements.

---

2. SCOPE

This Policy shall apply to:

- All servers, workstations, laptops, network devices, databases, applications, security appliances, and cloud services owned, operated, managed, or used by **SAI**.
- All employees, contractors, consultants, service providers, and third parties responsible for managing or administering information systems.
- All operating systems, software applications, virtual environments, firmware, and cloud-hosted resources.

---

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).

4. DEFINITIONS AND ABBREVIATIONS

Term	Description
Patch	Software update intended to correct vulnerabilities, errors, or performance issues
Firmware	Embedded software controlling hardware devices
Vulnerability	Weakness that could be exploited by a threat actor
Critical Patch	Patch addressing vulnerabilities with severe risk or active exploitation
Change Management	Process for managing modifications to information systems

5. ROLES AND RESPONSIBILITIES

5.1 IT Division

The IT Division shall:

- Establish and maintain patch management procedures.
- Monitor vendor advisories and security notifications.
- Assess patch applicability and deployment priorities.
- Coordinate patch testing and deployment.
- Maintain patch deployment records.
- Monitor compliance and report patch status.

5.2 System Owners

System Owners shall:

- Ensure systems under their control are maintained and updated.
- Coordinate testing activities.
- Approve deployment schedules where required.

5.3 Users

Users shall:

- Cooperate during patch deployment activities.
- Not bypass or disable approved update mechanisms.

- Report system issues following patch deployment.

---

6. PATCH MANAGEMENT REQUIREMENTS

6.1 General Requirements

- **SAI** shall maintain a documented patch management process.
- Security patches shall be evaluated and deployed in a timely manner.
- Patch management activities shall be risk-based.
- Only supported software and platforms shall be used wherever feasible.

6.2 Patch Identification

The IT Division shall monitor:

- Vendor security bulletins.
- CERT-In advisories.
- MeitY advisories.
- Threat intelligence sources.
- Cloud provider security notifications.

6.3 Patch Classification

Patches shall be categorized as:

- Critical
- High
- Medium
- Low
- Feature Updates

---

7. VULNERABILITY ASSESSMENT AND PATCH PRIORITIZATION

All identified vulnerabilities shall be assessed based on:

- Severity rating.
- Exploitability.
- Exposure of the affected asset.
- Criticality of business functions.
- Availability of compensating controls.

Priority shall be assigned using a risk-based approach.

---

8. PATCH TESTING

Before deployment, patches shall, wherever feasible:

- Be validated in a testing or staging environment.
- Be assessed for compatibility.
- Be reviewed for operational impact.
- Have rollback procedures documented.

Emergency patch deployment may bypass standard testing where immediate remediation is required.

---

9. PATCH DEPLOYMENT REQUIREMENTS

The following timelines shall be targeted:

Severity	Deployment Timeline
Critical	Within 15 days
High	Within 30 days
Medium	Within 60 days
Low	Within 90 days

Where compliance with timelines is not feasible, justification and risk acceptance shall be documented.

---

10. OPERATING SYSTEM PATCH MANAGEMENT

- Operating systems shall be maintained at supported versions.
- Security updates shall be reviewed regularly.
- End-of-life systems shall be upgraded, isolated, or formally risk accepted.

---

11. APPLICATION PATCH MANAGEMENT

- Security updates for applications shall be evaluated upon availability.
- Internet-facing applications shall receive priority attention.
- Secure development teams shall address identified vulnerabilities promptly.

---

12. NETWORK DEVICE AND SECURITY APPLIANCE PATCHING

The following devices shall be included:

- Firewalls
- Routers
- Switches
- VPN Appliances
- Web Application Firewalls
- IDS/IPS Systems
- Load Balancers

Firmware updates shall be reviewed and applied where appropriate.

---

13. CLOUD SERVICE PATCH MANAGEMENT

Where cloud services are used:

- Responsibilities shall be clearly defined under the shared responsibility model.
- Customer-managed resources shall remain updated.
- Security configurations shall be reviewed periodically.

---

14. EMERGENCY PATCH MANAGEMENT

Emergency patching may be initiated when:

- Active exploitation is identified.
- Critical vulnerabilities are announced.
- CERT-In advisories require urgent action.
- Significant business risk exists.

Emergency changes shall be recorded and reviewed after implementation.

---

15. PATCH VERIFICATION

Following deployment:

- Successful installation shall be verified.
- Vulnerability remediation shall be confirmed.
- System functionality shall be validated.
- Relevant records shall be maintained.

Verification may include vulnerability scanning and compliance reviews.

---

16. PATCH EXCEPTIONS

Any deviation from this Policy shall:

- Be documented.
- Be risk assessed.
- Receive management approval.
- Be protected through compensating controls.
- Be reviewed periodically.

---

17. COMPLIANCE AND MONITORING

Compliance shall be monitored through:

- Vulnerability assessments.
- Security audits.
- Compliance reviews.
- Configuration reviews.
- Technical monitoring activities.

Non-compliance may result in corrective actions.

---

18. POLICY REVIEW

This Policy shall be reviewed:

- At least annually.
- Following significant cybersecurity incidents.
- Following changes in legal or regulatory requirements.
- Following major technology changes.

---

19. 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.

---

20. APPROVAL

This Patch Management Policy is approved by the Competent Authority of **SAI** and shall be implemented across all applicable systems and environments.

---

21. REFERENCES

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

1. **CERT-In Guidelines on Information Security Practices for Government Entities (CISG-2023-01)**
   Link: CERT-In Government Entity Guidelines
2. **CERT-In Directions under Section 70B dated 28 April 2022**
   Link: CERT-In Directions
3. **Information Technology Act, 2000**
   Link: Ministry of Electronics and Information Technology
4. **Digital Personal Data Protection Act, 2023**
   Link: DPDP Act Information
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

***