SPORTS AUTHORITY OF INDIA
IT DIVISION

CHANGE 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
Review Frequency: Annual

---

1. PURPOSE

The purpose of this Change Management Policy is to establish a structured, controlled, and documented process for managing changes to information systems, applications, databases, network infrastructure, cloud environments, business processes, and technology assets within **SAI**.

This Policy aims to:

- Minimize risks associated with unauthorized or poorly managed changes.
- Ensure that changes are planned, tested, reviewed, approved, implemented, and monitored appropriately.
- Maintain the confidentiality, integrity, and availability of information systems.
- Reduce service disruptions and operational risks.
- Support regulatory, contractual, and information security requirements.
- Ensure accountability and traceability of all changes.

---

2. SCOPE

This Policy applies to:

- All employees, consultants, contractors, service providers, and third parties involved in implementing or managing changes.
- All production, testing, staging, and development environments.
- All information systems, applications, databases, network devices, servers, cloud environments, and supporting infrastructure.
- Hardware, software, firmware, configuration, security, and business process changes.

---

3. OBJECTIVES

The objectives of this Policy are to:

- Ensure changes are evaluated and authorized before implementation.
- Minimize adverse impact on business operations.
- Improve stability and availability of systems and services.
- Establish accountability for change activities.
- Reduce security vulnerabilities arising from uncontrolled changes.
- Maintain proper documentation and audit trails.

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 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, Patch Management Policy, Incident Management Policy and Risk Management Policy.

5. DEFINITIONS AND ABBREVIATIONS

Term	Definition
Change	Addition, modification, removal, upgrade, or replacement of systems, services, infrastructure, configurations, or processes
Change Request (CR)	Formal request submitted for implementing a change
CAB	Change Advisory Board

Emergency Change	Change requiring immediate implementation to restore services or address critical risks
Standard Change	Low-risk, pre-approved change
Major Change	Significant change with potential business impact
Change Owner	Person responsible for managing and coordinating the change

6. ROLES AND RESPONSIBILITIES

6.1 Management

Management shall:

- Approve major changes where required.
- Ensure adequate resources are available.
- Review significant changes and related risks.

6.2 Change Advisory Board (CAB)

The CAB shall:

- Review change requests.
- Assess risks and impacts.
- Approve, reject, or defer changes.
- Ensure business and technical considerations are evaluated.

6.3 IT Division

The IT Division shall:

- Maintain change management procedures.
- Maintain change records.
- Conduct impact assessments.
- Verify successful implementation.
- Monitor change-related risks.

6.4 Change Owner

The Change Owner shall:

- Raise and document change requests.
- Coordinate testing and implementation.

- Ensure rollback procedures are available.
- Maintain implementation records.

6.5 Users and Stakeholders

Users shall:

- Participate in testing where required.
- Report issues related to implemented changes.
- Follow approved procedures.

7. CHANGE MANAGEMENT PRINCIPLES

SAI shall ensure that:

- All changes are formally documented.
- Risks are assessed before implementation.
- Appropriate approvals are obtained.
- Testing is performed prior to deployment.
- Rollback plans are available.
- Changes are auditable and traceable.
- Business disruptions are minimized.

---

8. CHANGE CLASSIFICATION

Changes shall be classified as follows:

8.1 Standard Changes

Pre-approved and low-risk changes that follow documented procedures.

Examples:

- Antivirus signature updates.
- Routine patch deployment.
- User account modifications.

8.2 Normal Changes

Changes requiring review, assessment, and approval prior to implementation.

Examples:

- Application modifications.
- Infrastructure upgrades.

- Security configuration changes.

8.3 Emergency Changes

Changes required to address:

- Security incidents.
- Critical vulnerabilities.
- Service outages.
- Regulatory requirements.

Emergency changes shall undergo post-implementation review.

---

9. CHANGE REQUEST PROCESS

All changes shall follow the documented Change Management Process:

Step 1 – Change Request Submission

A formal Change Request (CR) shall be submitted.

Step 2 – Change Assessment

Technical, business, security, and operational impacts shall be evaluated.

Step 3 – Risk Assessment

Associated risks shall be identified and documented.

Step 4 – Approval

Required approvals shall be obtained.

Step 5 – Testing

Changes shall be tested in a development or staging environment where feasible.

Step 6 – Implementation

Approved changes shall be deployed according to approved schedules.

Step 7 – Verification

Successful implementation shall be confirmed.

Step 8 – Closure

Change records shall be updated and formally closed.

---

10. CHANGE IMPACT ASSESSMENT

The assessment shall consider:

- Business impact.
- Security implications.
- Service availability.
- Regulatory impact.
- Dependency requirements.
- Resource requirements.
- Financial implications.

---

11. RISK ASSESSMENT REQUIREMENTS

Changes shall undergo risk assessment based on:

- Complexity.
- System criticality.
- Security impact.
- Data sensitivity.
- Recovery requirements.

High-risk changes shall require enhanced review and approval.

---

12. TESTING REQUIREMENTS

Changes shall be tested before implementation to:

- Validate functionality.
- Verify compatibility.
- Confirm security requirements.
- Minimize implementation

risks. Testing evidence shall be

retained.

---

13. CHANGE APPROVAL

Changes shall be approved by appropriate personnel based on:

- Change category.
- Business impact.
- Security impact.
- Risk level.

No production change shall proceed without authorization except approved emergency changes.

---

14. IMPLEMENTATION REQUIREMENTS

Implementation activities shall:

- Follow approved schedules.
- Minimize disruption.
- Maintain documentation.
- Ensure stakeholder communication.
- Follow change windows where applicable.

---

15. BACKOUT AND ROLLBACK PROCEDURES

All significant changes shall include:

- Rollback plans.
- Recovery procedures.
- Contingency actions.

Rollback capability shall be verified during testing where feasible.

---

16. EMERGENCY CHANGE MANAGEMENT

Emergency changes shall:

- Be justified and documented.
- Receive appropriate emergency approval.
- Be logged immediately.

- Undergo retrospective review.
- Be assessed for lessons learned.

---

17. SECURITY REQUIREMENTS FOR CHANGES

Changes impacting security controls shall be reviewed for:

- Access control implications.
- Privacy implications.
- Vulnerability exposure.
- Compliance obligations.
- Logging and monitoring requirements.

Security-related changes may require dedicated security review.

---

18. DOCUMENTATION AND RECORD KEEPING

The following records shall be maintained:

- Change Requests.
- Risk Assessments.
- Test Results.
- Approval Records.
- Implementation Reports.
- Rollback Activities.
- Change Closure Reports.

Records shall be retained according to organizational retention requirements.

---

19. POST-IMPLEMENTATION REVIEW

Significant changes shall undergo review to evaluate:

- Achievement of objectives.
- Operational impact.
- Security impact.
- Service performance.

- Lessons learned.

Corrective actions shall be implemented where necessary.

---

20. CHANGE FAILURE MANAGEMENT

Where changes result in incidents or failures:

- Root Cause Analysis (RCA) shall be conducted.
- Corrective actions shall be documented.
- Reoccurrence prevention measures shall be implemented.

---

21. THIRD-PARTY CHANGES

Changes performed by vendors, contractors, cloud providers, or third parties shall:

- Follow approved procedures.
- Be reviewed and authorized.
- Be monitored appropriately.
- Be documented.

---

22. COMPLIANCE AND MONITORING

Compliance shall be monitored through:

- Internal audits.
- External audits.
- Change reviews.
- CAB reviews.
- Compliance assessments.
- Security assessments.

Unauthorized changes shall be investigated.

---

23. EXCEPTION MANAGEMENT

Exceptions shall:

- Be documented.

- Include business justification.
- Be risk assessed.
- Receive approval from competent authority.
- Be periodically reviewed.

24. POLICY REVIEW

This Policy shall be reviewed:

- Annually.
- Following significant incidents.
- Following technology changes.
- Following audit observations.
- Following regulatory updates.

25. EFFECTIVE DATE

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

26. APPROVAL

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

27. 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**

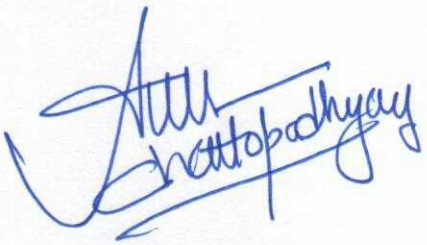
Entities (CISG-2023-01)
Link: https://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW02&refcode=CISG-2023-01

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. **NIST Cybersecurity Framework (CSF 2.0)**
   Link: NIST Cybersecurity Framework

9. **NIST SP 800-128 - Guide for Security-Focused Configuration Management**
   Link: NIST Publications

***