SPORTS AUTHORITY OF INDIA

IT DIVISION

NETWORK SECURITY 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 Network Security Policy is to establish minimum security requirements for the protection, management, monitoring, operation, and secure use of **SAI** network infrastructure. This Policy aims to safeguard network resources from unauthorized access, cyber threats, data leakage, disruption of services, and other security risks that may compromise the confidentiality, integrity, and availability of organizational information assets.

This Policy also establishes network security controls to support compliance with applicable legal, regulatory, contractual, and cybersecurity requirements.

---

2. SCOPE

This Policy shall apply to:

- All network infrastructure owned, leased, managed, or operated by **SAI**.
- All employees, contractual personnel, consultants, vendors, service providers, and authorized users utilizing **SAI** network resources.
- Internal and external networks.
- Data centers and cloud-hosted network environments.
- Routers, switches, firewalls, wireless infrastructure, VPN infrastructure, proxies, IDS/IPS systems, load balancers, and other networking devices.
- Third-party connectivity to **SAI** networks.

---

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 issued 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 obligations establish stricter requirements, such requirements shall prevail.

---

4. DEFINITIONS AND ABBREVIATIONS

Term	Description
LAN	Local Area Network
WAN	Wide Area Network
VPN	Virtual Private Network
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
DMZ	Demilitarized Zone
Firewall	Network device used to monitor and control network traffic

Network Asset	Any device, service or infrastructure component connected to the network
Network Segmentation	Logical or physical separation of network zones

5. ROLES AND RESPONSIBILITIES

5.1 IT Division

The IT Division shall:

- Establish and maintain network security controls.
- Implement security monitoring mechanisms.
- Manage network infrastructure securely.
- Periodically assess network risks.
- Maintain network security documentation.

- Review firewall and network security configurations.
- Coordinate incident response activities involving network infrastructure.

5.2 Network Administrators

Network Administrators shall:

- Configure and maintain network devices securely.
- Apply firmware and security updates (n-1).
- Monitor network activity.
- Maintain backup configurations.
- Investigate security alerts affecting network infrastructure.

5.3 Users

Users shall:

- Use network resources only for authorized business purposes.
- Comply with organizational security requirements.
- Report suspicious activities or network security incidents immediately.
- Not connect unauthorized devices to **SAI** networks.

---

6. NETWORK SECURITY PRINCIPLES

SAI shall ensure that:

- Access to network resources is authorized and controlled.
- Network infrastructure is protected against cyber threats.
- Security monitoring is implemented.
- Network traffic is appropriately managed.
- Critical systems are adequately segregated.
- Security incidents are promptly detected and addressed.

---

7. NETWORK SEGMENTATION

- Network segmentation shall be implemented based on business and security requirements.
- Critical systems shall be separated from general user networks wherever feasible.
- Sensitive information processing environments shall be isolated appropriately.
- DMZ architecture shall be used for public-facing services where required.
- Administrative networks shall be segregated from user networks.

Periodic reviews shall be conducted to ensure segmentation effectiveness.

8. FIREWALL SECURITY MANAGEMENT

Firewalls shall be implemented to control network traffic.

The following requirements shall apply:

- Firewall rules shall be formally approved.
- Default-deny principles shall be implemented wherever feasible.
- Unnecessary ports, services, and protocols shall be restricted.
- Firewall rule reviews shall be conducted periodically.
- Configuration backups shall be maintained.
- Administrative access shall be restricted to authorized personnel.

9. NETWORK ACCESS CONTROL

- Access to network resources shall follow the principle of least privilege.
- Network access shall be granted based on authorized business requirements.
- User authentication mechanisms shall be employed.
- Privileged access shall be subject to enhanced controls.
- Access rights shall be reviewed periodically.
- Dormant, inactive, or unnecessary access permissions shall be removed.

10. REMOTE ACCESS SECURITY

Remote access to **SAI** systems shall:

- Be approved by authorized personnel (AD, IT Division).
- Utilize secure communication channels.
- Use VPN technology or equivalent security controls.
- Implement Multi-Factor Authentication (MFA) wherever technically feasible.
- Be monitored and logged.

Unauthorized remote access shall be prohibited.

11. WIRELESS NETWORK SECURITY

Wireless networks shall:

- Use strong encryption mechanisms.
- Require authentication before granting access.
- Restrict unauthorized wireless devices.
- Separate guest wireless networks from internal corporate networks.
- Periodically review wireless security configurations.

Default manufacturer settings shall not be retained unless justified.

---

12. NETWORK DEVICE SECURITY

The following security controls shall be implemented:

- Secure configuration of routers, switches, firewalls, VPN gateways, IDS/IPS systems, and related infrastructure.
- Removal or disabling of unnecessary services.
- Timely application of firmware and security updates.
- Restriction of administrative interfaces.
- Configuration backup management.
- Security hardening measures.

---

13. INTRUSION DETECTION AND MONITORING

SAI shall implement monitoring mechanisms appropriate to the risk environment.

Such controls may include:

- Security Information and Event Management (SIEM).
- Intrusion Detection Systems (IDS).
- Intrusion Prevention Systems (IPS).
- Network traffic analysis.
- Security logging and alerting mechanisms.

Security alerts shall be investigated as appropriate.

---

14. NETWORK LOGGING AND MONITORING

Network security logs shall be generated, retained, and protected.

Logs may include:

- Authentication events.
- Administrative activities.

- Firewall activity.
- VPN usage.
- Security alerts.
- Configuration changes.

Log retention periods shall comply with applicable legal and regulatory requirements.

---

15. INTERNET AND EMAIL TRAFFIC SECURITY

The organization shall implement appropriate controls to:

- Restrict access to malicious websites.
- Detect malicious traffic.
- Prevent unauthorized data transfer.
- Reduce phishing and malware risks.
- Monitor internet gateway activity.

Filtering and monitoring technologies may be utilized as appropriate.

---

16. CLOUD NETWORK SECURITY

Where cloud environments are utilized:

- Network security controls shall be implemented in accordance with risk assessments.
- Security groups, virtual firewalls, and network controls shall be properly configured.
- Cloud connectivity shall be secured.
- Network logs shall be maintained and monitored.
- Responsibilities shall be clearly defined under the shared responsibility model.

---

17. THIRD-PARTY NETWORK CONNECTIVITY

Third-party network connections shall:

- Be formally approved.
- Be subject to security assessment.
- Be limited to business requirements.
- Be monitored and periodically reviewed.
- Be removed when no longer required.

Appropriate contractual security controls shall be established where applicable.

---

18. NETWORK VULNERABILITY MANAGEMENT

The IT Division shall:

- Conduct periodic vulnerability assessments.
- Review identified weaknesses.
- Implement risk-based remediation.
- Apply security patches and updates in accordance with the Patch Management Policy.
- Monitor exposure to emerging cyber threats.

---

19. NETWORK SECURITY INCIDENT MANAGEMENT

Any network-related security incident shall be managed in accordance with the Incident Management Policy.

Incidents may include:

- Unauthorized access attempts.
- Denial-of-Service attacks.
- Malware propagation.
- Network compromise.
- Suspicious traffic activity.
- Security control failures.

Appropriate containment, investigation, recovery, and reporting procedures shall be followed.

---

20. BUSINESS CONTINUITY AND RESILIENCE

Network infrastructure supporting critical services shall:

- Maintain redundancy where appropriate.
- Support business continuity objectives.
- Maintain backup configurations.
- Be included within disaster recovery arrangements.
- Be periodically tested.

---

21. EXCEPTIONS

Any exception to this Policy shall:

- Be documented.

- Include adequate business justification.
- Be reviewed through risk assessment.
- Be approved by the competent authority.
- Include compensating controls where required.

Approved exceptions shall be reviewed periodically.

---

22. COMPLIANCE AND MONITORING

Compliance with this Policy shall be monitored through:

- Security assessments.
- Vulnerability assessments.
- Internal audits.
- External audits.
- Network security reviews.
- Configuration reviews.
- Penetration testing activities.

Non-compliance may result in corrective actions, access restrictions, disciplinary measures, or contractual actions where applicable.

---

23. POLICY REVIEW

This Policy shall be reviewed:

- At least annually.
- Following significant cyber security incidents.
- Following regulatory updates.
- Following major infrastructure modifications.
- Following audit recommendations.
- Following changes in technology or threat landscape.

---

24. EFFECTIVE DATE

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

---

25. APPROVAL

This Network Security Policy is approved by the Competent Authority of **SAI** and shall be implemented across all applicable network infrastructure and services.

26. 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 800-41 Rev.1 - Guidelines on Firewalls and Firewall Policy**
   Link: NIST Publications

***

Chattopadhyay