SPORTS AUTHORITY OF INDIA
IT DIVISION

PASSWORD 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 Password Policy is to establish minimum requirements for the creation, use, protection, storage and management of passwords used to access the information systems, applications, networks, devices and digital services of the **Sports Authority of India (SAI)**.

The Policy is intended to minimise the risk of unauthorised access, credential compromise, data breach and misuse of **SAI** information assets and to establish secure authentication practices across **SAI**.

---

2. SCOPE

This Policy shall apply to:

i. all officers, employees, contractual personnel, consultants, interns, volunteers, vendors, service providers and other authorised users having access to **SAI**'s information systems or information assets;
ii. all password-based user, application, network, database, system, privileged, administrative and service accounts;
iii. all information systems, applications, servers, databases, network devices, endpoints, cloud services and other IT assets owned, operated, managed or authorised by **SAI**; and
iv. third-party or outsourced systems where **SAI** credentials are used or where such systems provide access to **SAI** information or services, subject to applicable contractual arrangements.

---

3. REFERENCE DOCUMENTS AND APPLICABLE REQUIREMENTS

This Policy shall be read in conjunction with applicable Government of India laws, rules, directions, guidelines, standards and policies, including:

1. **Information Technology Act, 2000**, as amended from time to time;
2. **Directions issued by the Indian Computer Emergency Response Team (CERT-In) under Section 70B of the Information Technology Act, 2000, dated 28.04.2022**, relating to information security practices, procedures, prevention, response and reporting of cyber incidents;

3. **CERT-In Guidelines on Information Security Practices for Government Entities (CISG-2023-01), dated 29.06.2023**;
4. **CERT-In Advisory CIAD-2022-0026 – Password Management and Security, dated 18.10.2022**;
5. applicable **Ministry of Electronics and Information Technology (MeitY) Guidelines on Information Security Practices for Government Entities**;
6. applicable Government of India cyber-security policies, advisories, directions and instructions issued from time to time; and
7. other applicable **SAI** information-security policies, procedures and instructions.

In case of any conflict between this Policy and a statutory provision or mandatory Government of India requirement, the applicable statutory provision or Government requirement shall prevail.

---

4. DEFINITIONS AND ABBREVIATIONS

Term/Abbreviation	Description
SAI	**Sports Authority of India**
IT Division	Information Technology Division, **Sports Authority of India**
MFA	Multi-Factor Authentication
PAM	Privileged Access Management
User Account	An account assigned to an individual for accessing an information system or service
Privileged Account	An account having elevated administrative, system, security or configuration privileges
Service Account	An account used by an application, service, system or automated process
Password	A secret authentication credential used to verify the identity of a user or account
Password History	A system-maintained record used to prevent reuse of previously used passwords

5. ROLES AND RESPONSIBILITIES

5.1 IT Division

The IT Division shall:

i. establish and maintain technical controls for implementation of this Policy;
ii. prescribe appropriate password and authentication controls for **SAI**'s information systems;
iii. ensure implementation of appropriate controls for privileged and administrative accounts;
iv. provide guidance and awareness to users regarding secure password practices;
v. coordinate with system/application owners, vendors and service providers for implementation of appropriate password controls;
vi. monitor compliance with this Policy, wherever technically feasible;
vii. maintain records relating to approved exceptions to this Policy; and
viii. review and update this Policy periodically in accordance with applicable Government of India requirements and emerging cyber-security threats.

5.2 System/Application Owners

System and Application Owners shall:

i. ensure implementation of applicable password and authentication controls in their respective systems;
ii. ensure that default and temporary passwords are appropriately changed;
iii. ensure appropriate management of privileged and service accounts; and
iv. coordinate with the IT Division in case of suspected credential compromise or other security incidents.

5.3 Users

All users shall:

i. maintain the confidentiality of their passwords;
ii. use only their authorised accounts;
iii. not share passwords with any person;
iv. immediately report suspected compromise, disclosure or unauthorised use of credentials; and
v. comply with this Policy and other applicable **SAI** information-security requirements.

---

6. PASSWORD REQUIREMENTS

6.1 General Requirements

All password-based authentication mechanisms shall, wherever technically feasible, comply with the following minimum requirements:

i. Passwords for standard user accounts shall have a minimum length of **10 characters**.
ii. Passwords shall contain an appropriate combination of uppercase letters, lowercase letters, numbers and special characters, wherever supported by the concerned system.
iii. Passwords shall not contain easily identifiable information relating to the user, including username, name, employee number, date of birth, telephone number, family member details or other publicly available personal information.
iv. Passwords shall not be commonly used, easily guessable, predictable, compromised or based on simple patterns.
v. Passwords shall not be reused across different **SAI** accounts or between **SAI** accounts and personal/non-official services.
vi. Passwords shall not be based on sequential numbers, repeated characters, keyboard patterns or other easily predictable patterns.
vii. Where technically supported, systems shall maintain password history and prevent reuse of the previous **twelve (12) passwords**.

---

7. PASSWORD CHANGE AND EXPIRY

i. Passwords for standard **SAI** network/user accounts shall be changed at least once every **120 days**.
ii. A password shall be changed immediately where compromise, suspected compromise, unauthorised disclosure or unauthorised use is detected or suspected.
iii. Temporary passwords issued for initial account creation or password reset shall be changed at first login or within the period prescribed by the concerned system.
iv. System-enforced password expiry shall be implemented wherever technically feasible.

v. Where an alternative authentication mechanism is implemented in place of password-based authentication, it shall comply with applicable Government of India security requirements and shall be approved by the IT Division, wherever such approval is required.

---

8. MULTI-FACTOR AUTHENTICATION

i. Multi-Factor Authentication (MFA) shall be enabled **wherever available and technically supported**, particularly for privileged/administrative accounts, remote access and critical applications or systems.
ii. MFA shall be implemented for critical **SAI** applications and services based on the sensitivity and risk associated with the system.
iii. Users shall not share MFA credentials, authentication codes, tokens or other authentication factors.
iv. Users shall immediately report unexpected MFA requests or authentication prompts that they did not initiate.

---

9. PRIVILEGED AND ADMINISTRATIVE ACCOUNTS

i. Privileged and administrative accounts shall have passwords of at least **12 characters**, or a higher length where technically supported.
ii. Privileged passwords shall comply with strong complexity requirements, including a suitable combination of uppercase letters, lowercase letters, numbers and special characters.
iii. Privileged accounts shall, wherever feasible, be separate from normal user accounts.
iv. Administrative accounts shall not be used for routine activities such as general internet browsing, email or other ordinary user activities.
v. Access to privileged accounts shall be restricted to authorised personnel based on the principle of least privilege.
vi. Privileged credentials shall not be shared except where technically unavoidable and specifically authorised.
vii. Wherever technically feasible, privileged credentials should be managed through an organisation-approved **Password Vault or Privileged Access Management (PAM)** solution.
viii. Privileged accounts shall be periodically reviewed to ensure that access remains authorised and necessary.

---

10. SERVICE AND APPLICATION ACCOUNTS

i. Service and application accounts shall be created only where operationally necessary.
ii. Service account credentials shall not be used for interactive user login unless specifically authorised.
iii. Service account credentials shall be securely stored and access shall be restricted to authorised personnel or authorised processes.
iv. Service account passwords shall be changed periodically or whenever there is a suspected compromise, change in authorised personnel, system modification or other security event, as applicable.
v. Inactive or unnecessary service accounts shall be disabled or removed.

vi. Where technically feasible, service account credentials shall be managed through an approved password-vault/PAM mechanism.

---

11. DEFAULT AND TEMPORARY PASSWORDS

i. Default passwords supplied with hardware, software, applications, network devices or other IT equipment shall be changed before deployment or first operational use.
ii. Temporary passwords shall be unique and shall not be reused.
iii. Vendor-supplied credentials shall not be retained beyond the period for which they are operationally required.
iv. Third-party/vendor access shall be authorised, restricted to the minimum required period and disabled when no longer required.

---

12. PASSWORD STORAGE AND PROTECTION

i. Passwords shall **not be stored in plaintext**.
ii. Passwords shall not be stored in a manner that permits recovery or retrieval in readable/plaintext form by administrators or unauthorised persons.
iii. Passwords shall be stored using an approved **strong, salted, one-way cryptographic hashing mechanism** appropriate to the technology and security requirements of the system.
iv. Password hashes and associated authentication information shall be protected against unauthorised access, disclosure and modification.
v. Passwords shall not be embedded in source code, configuration files, automated login scripts or application files in plaintext.
vi. Where authentication is managed by a third-party service provider, appropriate contractual and technical controls shall be established to ensure secure password handling.

---

13. PASSWORD CONFIDENTIALITY

i. Passwords shall be treated as confidential authentication information.
ii. Passwords shall not be shared with colleagues, supervisors, vendors, family members or any other person.
iii. Passwords shall not be communicated through email, SMS, instant messaging, telephone or any other unsecured communication channel.
iv. Users shall not disclose or provide hints regarding the composition or format of their passwords.
v. Passwords shall not be written on desks, notice boards, sticky notes, plain paper or other unsecured material.
vi. Passwords shall not be stored in browsers or unprotected documents.
vii. Users shall not store **SAI** passwords in personal password-management applications or other unauthorised third-party services.
viii. Where a password-management solution is required, only an **IT Division-approved password manager/password vault** shall be used.

---

14. FAILED LOGIN ATTEMPTS

Where technically supported, **SAI** systems shall implement appropriate controls against repeated unsuccessful authentication attempts, including account lockout, login throttling, progressive delays or equivalent security mechanisms.

The threshold and duration for such controls may be determined based on the criticality, architecture and risk profile of the concerned system.

---

15. PASSWORD RESET

i. Password-reset requests shall be subject to appropriate identity verification.
ii. Temporary/reset credentials shall not be communicated through insecure channels.
iii. Password-reset mechanisms shall incorporate appropriate controls to prevent unauthorised password resets.
iv. Temporary reset passwords shall be changed upon successful authentication.
v. Helpdesk or support personnel shall not request users to disclose their existing passwords.

---

16. COMPROMISED PASSWORDS

Where a password is suspected to have been compromised, disclosed, stolen or misused:

i. the concerned password shall be changed immediately;
ii. the user shall report the matter to the IT Division/helpdesk or designated information-security function;
iii. the concerned account may be temporarily disabled or subjected to additional security controls, wherever necessary;
iv. relevant authentication and system logs may be reviewed to identify unauthorised activity; and
v. the incident shall be handled in accordance with applicable **SAI** cyber-security incident management procedures and applicable CERT-In requirements.

---

17. NON-EXPIRING PASSWORDS

Non-expiring passwords shall not ordinarily be permitted for normal user accounts.

Where a non-expiring password is technically required for a service, application, system or emergency account:

i. the requirement shall be documented;
ii. the account shall be approved by the IT Division or designated competent authority;
iii. appropriate compensating security controls shall be implemented;
iv. access shall be restricted and monitored; and
v. the credential shall be changed whenever technically feasible and immediately upon suspected compromise.

---

18. SECURITY AWARENESS

The IT Division shall undertake appropriate information-security awareness activities to educate users regarding:

i. creation and protection of strong passwords;
ii. password reuse and credential-theft risks;
iii. phishing and social-engineering attacks;
iv. secure use of MFA;
v. safe use of password-management solutions; and
vi. reporting of suspected credential compromise.

---

19. EXCEPTIONS

Any exception to this Policy shall be permitted only where there is a documented technical, operational or business requirement.

Such exception shall:

i. be documented with adequate justification;
ii. be assessed for associated security risks;
iii. be approved by the competent authority designated by **SAI**/IT Division; and
iv. include appropriate compensating security controls wherever necessary.

Approved exceptions shall be periodically reviewed and shall not be treated as permanent deviations unless specifically approved.

---

20. COMPLIANCE AND MONITORING

The IT Division shall monitor compliance with this Policy through appropriate technical controls, system reviews, security assessments, audits, vulnerability assessments and other monitoring mechanisms, as considered appropriate.

System and application owners shall provide necessary support for implementation and verification of the prescribed controls.

Non-compliance may result in restriction, suspension or withdrawal of system access and may be dealt with in accordance with applicable **SAI** rules, service conditions, contractual provisions and Government of India requirements.

---

21. POLICY REVIEW

This Policy shall be reviewed at least once every year and earlier, wherever required, in case of:

i. changes in applicable Government of India laws, rules, directions or guidelines;
ii. changes in CERT-In or MeitY cyber-security requirements;
iii. significant changes in **SAI**'s IT infrastructure, applications or authentication mechanisms;

iv. major cyber-security incidents or emerging cyber threats;
v. findings/recommendations arising from security audits or assessments; or
vi. introduction of new authentication or identity-management technologies.

---

22. 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.

---

23. APPROVAL

This Password Policy is approved by the Competent Authority of the **Sports Authority of India** and shall be implemented across applicable **SAI** information systems and services.

The important current references are:

1. **CERT-In Guidelines on Information Security Practices for Government Entities, dated 29.06.2023 (CISG-2023-01)** — these establish a baseline of cyber-security controls for Central Government organisations and associated government entities. They specifically require, among other things, password changes at least every 120 days, MFA wherever available, no password reuse across services, and no storage of passwords in browsers or unprotected documents. (CERT-In) CERT-In – Guidelines on Information Security Practices for Government Entities
2. **CERT-In Advisory CIAD-2022-0026 – Password Management and Security, dated 18.10.2022** — specifically covers strong passwords, MFA, secure password handling, protection of password hashes and use of password-vault solutions. (CERT-In)
   CERT-In – Password Management and Security Advisory
3. **CERT-In Directions under Section 70B of the Information Technology Act, 2000, dated 28.04.2022** — these remain an important overarching cyber-security requirement concerning information-security practices, prevention, response and reporting of cyber incidents. (CERT-In) CERT-In – Directions under Section 70B
4. MeitY's Government Entity Guidelines also contain the same practical password controls, including **120-day password change, MFA, prohibition on password reuse and prohibition on saving passwords in browsers/unprotected documents**. (MeitY)
5. CERT-In's current website continues to list the 29.06.2023 Government Entity Guidelines as an active guideline, and CERT-In conducted a Government Entity Guidelines workshop in March 2026, so I would use these as the principal current reference for **SAI**'s policy. (CERT-In)

***

Atanu Chattopadhyay