Password Management Policy

Synthetic Users

Version: 1.2

Effective Date: January 2024

Last Updated: March 25, 2026

Document Owner: CTO — Artur Ventura

Review Frequency: Annually

Classification: Internal – Confidential

CRA Reference: 9.3.1, 9.3.3

Change History

Version	Date	Author	Changes
1.1	January 2024	CTO / Security Lead	Initial release
1.2	March 25, 2026	Artur Ventura, CTO	Added version metadata and last review date; expanded to explicitly cover password change frequency, strength requirements, password history, reset procedures, maximum failed login attempts, account lockout, and maximum idle session timeout; added AI/GenAI credential controls; added related documents. Per JPMC SCA CRA 9.3.1 and 9.3.3.

---

1. Purpose

To define requirements for the creation, management, and protection of passwords used to access Synthetic Users systems and data, ensuring account security and reducing the risk of unauthorized access.

2. Scope

This policy applies to all employees, contractors, and third-party users who access Synthetic Users systems, applications, and data, including environments such as AWS, Render, GitHub, Notion, Intercom, Google Workspace, and any AI/GenAI infrastructure credentials.

3. Policy Overview

Synthetic Users primarily uses **Single Sign-On (SSO)** integrated with **Multi-Factor Authentication (MFA)** to manage user access. Password use is limited to systems that do not support SSO. All non-SSO credentials are managed in a company-approved password manager.

4. Password Strength Requirements

All passwords — whether for SSO-fallback accounts, local system accounts, or service credentials — must meet the following minimum requirements:

Requirement	Standard
Minimum length	16 characters

Character composition	Must include at least one uppercase letter, one lowercase letter, one number, and one special character
Prohibited content	Must not contain the user's name, username, company name, or dictionary words
Prohibited patterns	Must not use sequential characters (e.g., 123, abc) or keyboard walks (e.g., qwerty)
Uniqueness	Must be unique — not reused across systems or accounts

5. Password Change Frequency

Account Type	Change Frequency
SSO-managed user accounts (application)	Passwords managed by IdP (Google Firebase); rotation triggered on suspected compromise or departure
SSO-managed employee accounts	Passwords managed by Google Workspace; rotation triggered on suspected compromise or departure
Non-SSO local accounts	Rotated every **12 months** at minimum
Service accounts and API keys	Rotated every **12 months** at minimum, or immediately upon personnel change
LLM provider API keys (AI/GenAI)	Rotated every **12 months** at minimum, or immediately upon suspected compromise or personnel departure
Shared / privileged credentials	Rotated **immediately after each use** and stored in the password manager

Passwords must also be changed immediately if there is any indication of compromise, unauthorized access, or upon report of a phishing attempt targeting the account holder.

6. Password History

- The last **12 passwords** must not be reused for any account.
- For SSO-managed application accounts, password history enforcement is handled by Google Firebase. For employee accounts, it is handled by Google Workspace.
- For non-SSO accounts, the password manager enforces uniqueness; reuse must be actively avoided.

7. Password Reset Procedures

- **Self-service reset:** Users may reset passwords via the IdP self-service portal. Identity is verified via MFA before any reset is permitted.
- **Admin-initiated reset:** IT administrators (or the CTO) may initiate a forced reset for any account. The reset link is delivered to the account holder's registered email.
- **Compromise-triggered reset:** If a password compromise is suspected or confirmed, the account holder must reset immediately. The Security Lead / CTO is notified within **1 hour** of the reset being initiated.
- **Offboarding reset:** All accounts are deprovisioned (not merely reset) upon employee departure. Shared credentials that the departing employee had access to are rotated immediately.

8. Maximum Failed Login Attempts and Account Lockout

Parameter	Policy Setting
Maximum failed login attempts	5 consecutive failed attempts
Account lockout trigger	Automatic lockout after 5 failed attempts

Lockout duration	30 minutes (auto-unlock) or until manually unlocked by an administrator
Lockout notification	User notified by email; administrator alerted after 3+ consecutive lockout events on the same account
Privileged account lockout	Privileged / admin accounts lock after **3** failed attempts and require administrator unlock

For SSO-managed application accounts, lockout is enforced at the Google Firebase level. For employee accounts, lockout is enforced at the Google Workspace level. For non-SSO accounts, the hosting platform or application enforces lockout settings.

---

9. Maximum Idle Session Timeout

Session Type	Timeout Setting
Web application sessions	30 minutes of inactivity
Administrative / privileged sessions	15 minutes of inactivity
Developer tool sessions (GitHub, AWS console)	60 minutes of inactivity or per-platform default, whichever is shorter
Mobile sessions	15 minutes of inactivity

Sessions must require re-authentication (including MFA) after timeout. "Remember me" functionality that bypasses MFA is prohibited.

---

10. Multi-Factor Authentication (MFA)

- MFA is **mandatory** for all accounts that support it.
- MFA must be enabled via a secure second factor: authenticator app (e.g., Google Authenticator, Authy) or hardware token (e.g., YubiKey).

- SMS-based MFA is permitted only where no stronger option is available, and must be approved by the CTO.
- MFA bypass codes must be stored securely in the password manager and rotated after use.

---

11. Password Storage and Sharing

- All non-SSO passwords must be stored in a **company-approved password manager** (1Password or Bitwarden).
- Passwords must **never be shared** verbally, written down, or transmitted in plain text (including email, Slack, or chat).
- Shared system accounts are prohibited unless technically required and approved by the CTO. Shared credentials must be stored in the password manager's shared vault, rotated after each use, and audited at each access rights review.

---

12. AI/GenAI Credential Controls

AI/GenAI infrastructure involves high-value credentials (LLM provider API keys, vector store access tokens, RAG pipeline service accounts) that are subject to the following specific controls:

- All AI/GenAI credentials are stored in a secrets manager — never in source code, configuration files, or environment variable files committed to version control.
- Access to retrieve AI/GenAI credentials is restricted to the CTO and authorized engineering personnel, per the Access Rights Review Policy.
- AI/GenAI credentials are rotated at least annually and immediately upon any personnel change affecting access.
- Any accidental exposure of an AI/GenAI credential (e.g., committed to a public repo) is treated as a security incident and reported per the Incident Response Plan.

---

13. Compromise and Incident Response

- Users must immediately report any suspected password compromise or unauthorized account activity to IT administration / the CTO.
- Compromised passwords must be changed immediately across all affected systems.
- The incident is documented and handled per the Incident Response Plan.

14. Enforcement and Review

- Violations of this policy may result in disciplinary action up to and including termination.
- This policy is reviewed **annually** and updated as needed to align with evolving security best practices and regulatory requirements.
- The last review was conducted on **March 25, 2026**.

15. Related Documents

- Access Rights Review Policy — Semi-annual review of credential access and privileged accounts
- Incident Response Plan — Credential compromise incident procedures
- User Awareness Training Program — Annual password hygiene and phishing awareness training
- Change Management Policy — Credential rotation as a change event for AI/GenAI systems
- Third-Party Risk Management Policy — LLM provider credential governance