SECURE CYBER GATES

PASSWORD POLICY

SECURE CYBER GATES

DOCUMENT CONTROL PAGE

Document ID	SCG/PP/009/1.0
Security Classification	Confidential
Date Issued	30-Jul-2025
Version	1.0
Project Name	NA
Author	AJ KHAN

VERSION HISTORY / CHANGE HISTORY

Version	Date Issued	Issued to	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

REVIEWERS

Version	Review Date	Reviewed By	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

APPROVERS

Version	Date Approved	Approved By	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

DISTRIBUTION LIST

Date	Name / Distribution List	Comments
30-Jul-2025	Customer_DL_ABC	Published to Customer ABC

DOCUMENT CONTROL PAGE

RELATED DOCUMENTS

DOC_ID	DOC Version#	DOC Link	Comments
SCG/BASEINS/005/1.0			Base Template Instructions
SCG/PXF/008/1.0			Policy Exception Form
SCG/BLP/036/1.0			List of Blacklisted passwords.
SCG/S2RAS/113/1.0			SOC2 Asset Scope

CONFIDENTIALITY STATEMENT

This document is the exclusive property of [SecureCyberGates]. This document contains proprietary and confidential information. Duplication, Redistribution, or use, in whole or in part, in any form, requires consent of [SecureCyberGates].

[SecureCyberGates] may share this document with auditors under non-disclosure agreements [NDA] to demonstrate Security Audit requirement compliance.

Contents

1) Objective

Passwords are a critical first line of defense for protecting [SecureCyberGates]'s information assets and systems from unauthorized access, which could lead to data breaches, intellectual property theft, and other damaging security incidents. As such, it is imperative that all [SecureCyberGates]employees, contractors, vendors, and anyone with access to [SecureCyberGates]'s networks and systems follow rigorous password security practices. This policy establishes the standards and requirements for creating, using, protecting, and managing passwords across the organization. The primary objective is to maintain strong and secure passwords to protect information assets from unauthorized access. This Policy applies to all [SecureCyberGates](sometimes also referred to as the "Company/Organization") employees and contract employees.

The purpose of this policy is to provide clear guidelines and requirements for passwords to ensure the confidentiality, integrity, and availability of [SecureCyberGates]'s sensitive data and critical systems. By adhering to robust password security practices, [SecureCyberGates] aims to mitigate the risk of unauthorized access, data breaches, and other security incidents that could result in financial losses, reputational damage, and legal liabilities.

2) Roles &Responsibilities

Roles	Responsibilities
CISO	Accountable - Overseeing the implementation and enforcement of this policy [Review and Approve Password Policy]
DPO [Data Privacy Officer]	Responsible for creating ,updating, and maintaining this policy.
IT/Security Team	1. Responsible for ensuring password protection requirements are in place 2. Responsible for enforcing these password requirements
BU Heads or Project Managers	Ensuring that employees under their supervision comply with this policy. [Review and Approve PasswordPolicy]
Employees / Contractors	1. Read this Password Policy 2. Ask questions /Provide Feedbacks 3. Report possible or actual violations of this Password Policy.

3) Scope

This policy applies to all individuals, including employees, contractors, vendors, and third-party users, who have been granted access to any [SecureCyberGates]system, network, application, database, or data repository that requires a password for authentication and authorization purposes. This policy covers all types of passwords, passphrases, and other authentication credentials used within [SecureCyberGates]'s computing environments.

4) Password Construction Requirements

4.1) Password Length and Complexity

- Passwords should include a combination of uppercase and lowercase letters, numbers, and special characters.
  Uppercase letters (A-Z)
  Lowercase letters (a-z)
  Numbers (0-9)
  Special characters (e.g., !, @, #, $, %, ^, &, *, (,), -, +, =)

- The minimum password length should be at least **08** characters [[SecureCyberGates] Internal network]
- The minimum password length should be at least **12** characters [Public Facing / Internet facing Assets]

4.2) Prohibited Passwords

The following types of passwords are explicitly prohibited due to their inherent weakness and susceptibility to guessing or cracking:

- Words found in dictionaries (English or foreign languages)
- Common names, phrases, or patterns (e.g., “admin”, “password” "SecureCyberGate123," dates, sequential numbers)
- Personal information (e.g., names, birthdays, addresses, phone numbers, usernames)
- Permutations or minor variations of the above (e.g., "password123," "SecureCyberGate2025," "JohnDoe123")
- Passwords obtained from previous data breaches or known compromised credential lists.

[SecureCyberGates]Maintains a central tracker for blacklisted password , Please refer document ID “SCG/BLP/036/1.0” for list of Blacklisted passwords.

4.3) Passphrases

The use of passphrases (long, memorable phrases) is **strongly encouraged** as an alternative to traditional passwords. Passphrases should be **easy to remember** yet difficult to guess, and they must meet the length and complexity requirements outlined in section

Examples of strong passphrases include "SecureCyberGateCyberCompany@2005" and "YouCannotGuessThisPassword#777”

4.4) MFA Requirements

MFA must be enabled for any and all systems that provide the option for Multi-Factor Authentication (MFA).

MFA typically involves the use of two or more authentication factors from the following categories:

Something you know: This is typically a password or PIN.
Something you have: This can include a smartphone, hardware token, or smart card.
Something you are: This refers to biometric factors such as fingerprint, facial recognition, or iris scan.

4.4.1) MFA for Public-Facing Systems

Our systems can be accessed via multi-step authentication using two levels of credentials. The first level of authentication is that for all work done on sensitive data, one needs to be logged in to the [SecureCyberGates]corporate network either via VPN [2FA enabled] or via the WLAN/LAN at the [SecureCyberGates]office location (secured by biometric access). After this the second level of verification is via user id – passwords at the application login screens[Enabling MFA as per requirements]. Every CRITICAL **Public-Facing System** MUST have MFA enabled.

4.4.2) MFA for VPN Solutions

Connecting to our [SecureCyberGates]network when outside the office is goes through an extra layer of defense. Apart from keying in the credentials for VPN remote connectivity, employees also receive a randomly generated rotating token number on the VPN provider’s authorized mobile application. The employee has to enter this token to validate their connection request to the corporate network. VPN MUST have MFA enabled.

4.4.3) MFA for Cloud Environments

Multi-factor authentication can be configured with the cloud provider’s service. The first factor is the prompt for username and password. The second factor authentication is that the user is prompted to enter a time-based verification code from a registered device. Every Cloud Subscription MUSThave MFA enabled.

4.4.4) MFA for Privileged Access

For access to critical systems, sensitive data, and administrative controls, MFA is going to be enforced using cloud service for cloud environment or using TPIN or authenticator

solutions for privileged access to application.

- MFA will be implemented for all sensitive systems and applications.
- Users will be required to provide additional factors, such as a one-time password or biometric verification, in addition to their password.
- MFA will be enforced for remote access to sensitive systems, especially when users connect from untrusted networks or locations.

Policy Exceptions

- Exceptions to MFA requirements will be granted on a case-by-case basis, with proper authorization and justification. Kindly refer Policy Exception section for more details.

5) Password Protection Standards

5.1) End-User Responsibilities

All [SecureCyberGates]employees, contractors, and authorized users must adhere to the following password protection standards:

- Never share passwords with anyone, including co-workers, superiors, family members, or [SecureCyberGates]IT staff, under any circumstances.
- Never write down or store passwords in plain text, except in approved and secure password managers .
- Never use the "Remember Password" feature in applications, as this practice can expose passwords to unauthorized access.
- Change passwords immediately if there is any suspicion or evidence of compromise, such as unauthorized access attempts or suspected phishing attacks.
- Use unique passwords for [SecureCyberGates] accounts and systems. Do not reuse passwords across multiple accounts or services, whether within [SecureCyberGates]or externally.
- Ensure passwords are not visible or accessible to others when entering them, such as by shielding the keyboard or screen from view.
- Users will not be allowed to reuse any of the 5 most recent passwords.The system will maintain a password history to enforce this requirement.
- All passwords entered are not displayed, regardless of whether on screen, in job or in database. A salted Hash is created of the passwords using SHA-512
- Passwords must not appear in any audit trails or logs.

5.2) IT Team / Project Team Responsibilities

[SecureCyberGates]IT and Project team must adhere to the following password protection standards:

- Never request or accept passwords from end-users, whether verbally, in writing, or through any other means.
- Store passwords using strong, approved encryption methods that meet industry best practices.
- Implement technical controls to prevent password guessing and brute-force attacks, such as account lockouts after a limited number of failed attempts, IP address blocking, and CAPTCHA challenges.
- Enable multi-factor authentication (MFA) wherever possible, especially for privileged accounts and remote access scenarios, to provide an additional layer of security beyond passwords alone.
- Regularly review and rotate any system-level or service account passwords to limit the potential impact of compromised credentials.

5.3) Use of Password Managers

[SecureCyberGates]strongly recommends the use of secure password managers [e.g. LastPass, 1Password, or KeePass,] to generate, store, and manage passwords for all accounts and systems. Password managers should be configured with strong master passwords and, where applicable, additional factors such as biometrics or hardware tokens.[SecureCyberGates] Security team MUST do a proper due diligence before selecting any secure password managers.

6) Password Reset, Expiration & Account Lockout

6.1) Mandatory Password Resets

Password resets are mandatory in the following situations:

- When there is evidence or reasonable suspicion that a password has been compromised, such as through a data breach, successful phishing attack, or unauthorized access attempt.
- When an employee, contractor, or third-party user with access to [SecureCyberGates]systems leave the organization or has their access revoked.
- If a password has not been changed in 6 months or more, to limit the potential exposure time of compromised credentials.

6.2) Periodic Password Expiration

[SecureCyberGates]does not enforce periodic password expiration (e.g., every 90 days) for end-user accounts, unless mandated by specific regulatory or contractual obligations. This approach is based on current industry best practices and research suggesting that forced password changes at arbitrary intervals can lead to insecure behaviours such as using predictable patterns or writing down passwords.

However, system-level and service account passwords must be rotated on a regular basis, with the frequency determined by the criticality and risk profile of the associated systems

and services.

- Passwords will expire every 90 days; this may change on Client's requirement.
- Users will be prompted to change their passwords upon expiration.

6.3) Account Lockout

- Accounts will be locked after 5 failed login attempts.
- Accounts dormant for 90 days will be deactivated
- Employees need to contact IT Team for unlocking of account

7) System and Application Development Standards

7.1) Application and System Requirements

All applications and systems developed or acquired by [SecureCyberGates]must adhere to the following password security requirements:

- Support authentication of individual users, not groups or shared accounts.
- Never store passwords in plain text or reversible formats, even temporarily during transmission or processing.
- Implement strong, salted key derivation functions (e.g., SHA-256/SHA-512, AES) for password hashing and storage.
- Provide role-based access controls and follow the principle of least privilege when granting access to users.
- Support secure authentication protocols, wherever possible.
- Integrate with [SecureCyberGates]'s centralized password blacklist to prevent the use of commonly used, expected, or compromised passwords

7.2) Centralized Password Blacklist

[SecureCyberGates]shall maintain a centralized password blacklist that includes:

- Common and frequently used passwords (e.g., "password," "123456," "qwerty")
- Permutations and variations of words like Password, [SecureCyberGates]'s name, locations, products, and other relevant terms
- Passwords obtained from previous data breaches or known compromised credential lists
- Personally identifiable information, such as names, dates of birth, and phone numbers

This blacklist must be integrated into all [SecureCyberGates]applications and systems during the authentication process to prevent the use of weak or compromised passwords. Please refer document ID "SCG/BLP/036/1.0" for list of Blacklisted passwords.

7.3) Account Lockout

The Account Management procedures ensure that user accounts are created, modified, and disabled in a secure and controlled manner. This includes account provisioning, deprovisioning, and access control.

Account Creation

- User accounts will be created based on job roles and responsibilities.
- Account creation requires approval from the appropriate authority.

Account Modification

- Accounts may be modified to adjust access rights or update user information.
- Any modifications must be authorized and documented.

Account Disabling and Termination

- Accounts of employees who leave the [SecureCyberGates]or contractors whose contracts have ended will be promptly disabled.
- The termination process will include revoking all access privileges.

Account Recertification

- User account access will undergo periodic recertification to ensure access rights are still necessary and appropriate.
- Recertification will be conducted at least annually.

Logging and Monitoring

- All account management activities, including account creation, modification, and disabling, will be logged.
- Account management logs will be regularly reviewed for any unauthorized or suspicious activities.

8) Employee Training and Awareness

8.1) All [SecureCyberGates] employees SHOULD undergo training and assessmenton this policy during their initial induction [Onboarding].

8.2) Security team to conduct periodic trainings **ATLEAST ONCE** a year.

9) Compliance and Monitoring

9.1) Compliance with this policy is **MANDATORY**. Employees violating this policy will be subject to disciplinary action up to and including termination.

9.2) Third-party users, contractors, and vendors who **FAIL**to comply with this policy may have their access to [SecureCyberGates]systems , Application and networks revoked or suspended until compliance is achieved. Repeated or severe violations may result in the termination of their contracts or business relationships with [SecureCyberGates].

9.3) Periodic Audits and Assessments : [SecureCyberGates]'s IT department, in collaboration with the Information Security team, will conduct periodic audits and assessments to evaluate compliance with this password security policy. These audits may include, but are not limited to:

- Reviewing password construction and complexity for a sample of user accounts across different systems and applications.
- Assessing the effectiveness of technical controls, such as password blacklisting, account lockouts, and multi-factor authentication.
- Evaluating the secure storage and transmission of passwords within applications and databases.
- Evaluating the procedures and processes for password resets, expiration, and management.

10) Escalation Matrix

10.1) In case of any policy violations issues, the following escalation structure shall be followed to ensure timely resolution and appropriate accountability:

Level	Role	Contact
Level 1	Team Lead /Reporting Manager	First-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]
Level 2	Group Manager / Senior Managers	Second-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]
Level 3	CISO	Final-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]

10.2) Employee SHOULD provide sufficient evidences and details , Clear description of the issue.

10.3) Security team to define issue severity and proper SLA for issue resolution as per severity.

11) Policy Exceptions

11.1) There may be requirements where Employee needs policy exception for legitimate reasons, In such cases, employee should follow POLICY EXCEPTIONS template and

approval process. **[Kindly refer Policy exception form [Document ID SCG/PXF/008/1.0]]**

12) Policy Review and Updates

12.1) This policy shall be periodically reviewed **[Atleast Once in a YEAR]**and updated to ensure its effectiveness, relevance, and alignment with [SecureCyberGates]objectives,legal requirements and industry best practices.

12.2) Feedback from employees, stakeholders, and external audits shall be solicited and considered for continuous improvement of the policy and associated procedures.

12.3) Regular audits and inspections shall be conducted to assess compliance with this policy and associated procedures, with non-conformances addressed through corrective actions and preventive measures.

12.4) Any updates or revisions to this policy will be communicated to all employees and relevant stakeholders through appropriate channels. Employees are responsible for familiarizing themselves with the latest version of the policy and adhering to its requirements.

13) Conclusion

By implementing and adhering to this comprehensive password security policy, [SecureCyberGates]aims to protect its sensitive information, intellectual property, and critical systems from unauthorized access and data breaches. This policy aligns with industry best practices and incorporates robust requirements for password construction, protection, management, and system development standards.

SECURE CYBER GATES

THANKYOU!
FOR CYBER-SECURITY RELATED UPDATES, KINDLY FOLLOW BELOW PAGES...

https://www.linkedin.com/in/aj57/
https://www.linkedin.com/company/securecybergates
https://securecybergates.com/services
https://www.youtube.com/@SECURECYBERGATES
https://hackerone.com/crypto-khan
https://x.com/securecybergate
securecybergates@gmail.com

SECURE CYBER GATES