ACCESS MANAGEMENT POLICY

DOCUMENT CONTROL PAGE

Document ID	SCG/AMP/010/1.0
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

Our Access Control Policy serves as guidance for controlling access within [SecureCyberGates] Systems. Following [SecureCyberGates] Access Control Policy is important and helpful for everyone, not just the operations staff but also for security of our organization and customer data.

It is important to note that every situation may not be addressed in this Access Management Policy; if you are unsure how [SecureCyberGates] standards or values apply in a given situation, please ask questions and seek further guidance from the Security and IT team. Each and every one of us are responsible for ensuring that we follow these guidelines, and we will be held accountable for upholding our commitments to this Access Management Policy.

2) Roles &Responsibilities

Roles	Responsibilities
CISO	Overseeing the implementation and enforcement of this policy [Review and Approve Access Management Policy]
IT/Security Team	1. Responsible for ensuring Acess Management requirements are in place. 2. Responsible for enforcing these requirements.
BU Heads or Project Managers	Ensuring that employees under their supervision comply with this policy. [Review and Approve Access Management Policy]
Employees / Contractors	1. Read this Access Management Policy 2. Ask questions /Provide Feedbacks 3. Report possible or actual violations of this Policy.

3) Scope

This Policy applies to anyone who conducts business for or on behalf of [SecureCyberGates] including:

- All employees / Contractors.
- Management and company owners
- External business partners who act on [SecureCyberGates]'s behalf or in our interest as Third Party Representatives

4) Control of Access

Access control to information systems and services shall cover all stages of the user access life-cycle from granting and modifying user access to terminating access. Access to systems and IT assets shall be granted based on:

- Valid access authorization from the immediate supervisor or system owner.
- The concept of least privilege, allowing only authorized access for users (or processes acting on behalf of users), including privileged users, based on their job functions and intended system usage.
- Considering the separation of duties between individuals to prevent malicious activity without collusion and other attributes required by the organization or business function.
- Restricting user accounts from installing software on devices.[Non-Admin Access]
- Access to sensitive information such as personal information shall be restricted.
- Critical access such as privileged access, access to sensitive information shall be logged and access to these logs shall be restricted.
- Administration, system and generic accounts being strictly controlled and given based on authorization from designated personnel. [SecureCyberGates] shall authorize and monitor the use of guest/anonymous and temporary accounts.
- Temporary and inactive accounts that are no longer required and accounts of terminated or transferred users shall be deactivated promptly.
- Account access privileges (including service and generic accounts) shall be reviewed periodically.
- Access approval: [SecureCyberGates] shall follow a documented formal access approval process for granting or changing access privileges.
- Unnecessary services such as unused file sharing, web application modules or service functions must be disabled by the organization.

5) User Access Life Cycle

5.1) New User Registration

1. All New users using [SecureCyberGates] systems MUST be UNIQUELY[e.g. Unique Email address] Identified using any centrally managed Identity provider [e.g. Azure AD]

2. Group /Generic accounts/Service Accounts [e.g. Security@SecureCyberGates.com , info@SecureCyberGates.com] are prohibited unless explicitly approved and justified in accordance with the Shared Account Usage policy.

5.2) Approval Cycle

1. Access requests must be formally initiated by the user / Reporting Manager through a designated Access Request Form[Email Approval] or ticketing system.

2. For Admin access to Critical Systems there SHOULD be minimum 2 Approval Levels [e.g. L1 Approval from Manager , L2 Approval from Security Team / BU Head]
    1.
3. All request MUST follow a standard template with minimum fields as 1) User Role 2) Business Justification 3) How long access is needed [e.g. 2 Hours, 1 Month , 3 Months , Maximum 6 Months]

4. All Access requests [even Urgent Access request] MUST be Documented. No access will be granted without documented approval.

5.3) Access Provisioning

1. Once any Access request is Approved , IT team would provide access based on Role / Access request form.

2. IT team MUST ensure sufficient details are Documented e.g. Requested Date/Time , Approval Requested Date/Time , Date/Time when access is Provided , Which System access is provided to , How long access is granted , Is that a Normal user or a priveledge user? Is access Permanent or Temporary?]

3. For JIT [Just in Time] access / Temporary access , IT team MUST use Automated tools to disabled access after time is expired.

5.4) Access De-Provisioning

1. Whenever any Employee / Staff / Contractor Leaves [SecureCyberGates] their Reporting manager / HR team MUST notify to IT team.

2. If any Employee / Staff / Contractor MOVES to any other BU / Project , their current Reporting manager MUST inform IT team [If access to existing Project is required then proper justification needs to be obtained]

3. De-provisioning must occur within 24 hours of the triggering event.

4. All De-provisioning activities MUST be documented and tracked centrally.

5.5) Access Review

1. A formal access review MUST be done by SYSTEM OWNER at least QUARTERLY for CRITICAL Systems and every 6 months for all other Systems.

2. SYSTEM OWNER MUST share the results of this review to Security team retaining the results for MINIMUM 3 Years.

3. Any findings during review MUST be addressed, if any user contains excessive access to any system then it SHOULD be revoked within 15 Days [Notifying to the user]

4. Security team to ensure each applicable System have a SYSTEM OWNER.

5.6) Emergency Access

1. All emergency cases MUST be provided access ONLY after approval from CISO / Security Head with Proper Business Justification.

2. All emergency access request MUST be tracked and reviewed.

5.7) Dormant Account Management

1. Any user if found Inactive / unused for period of 45 consecutive days first SHOULD be alerted that their access would be Disabled and after 3 reminders on their business email, this account would be temporarily disabled.

2. Accounts inactive for more than 120 days shall be permanently deactivated and archived in accordance with the Retention Policy.

3. The IT team must review dormant accounts monthly and take appropriate clean-up actions.

6) Privileged User Access Management

1. Privileged access shall be granted only to users with job responsibilities that explicitly require such elevated rights.
2. All privileged access requests must follow a formal approval workflow via the designated access management system.
3. Privileged access would have MINIMUM 3 Levels of Approvals , First one from Application/System Owner , Second one from BU head / Project Manager and the Final from Security team.
4. All privileged accounts must be protected using MFA.

5. Privileged access must be revoked immediately upon role change, transfer, or termination.
6. All privileged accounts must be monitored.
7. User activity and Access of privileged accounts MUST be reviewed on MONTHLY basis.

7) Remote Access

1. Remote access are ALLOWED using Virtual Private Network [VPN] protected by MFA.
2. User Can directly CONNECT to VPN from Company managed Laptops / machines.
3. If user wants to CONNECT to VPN from personal Laptops / machines then they SHOULD first connect to a secure VDI and from inside that VDI they can connect to VPN.

8) Third Party Access

1. All third-party access (vendors, partners, consultants) must be governed by signed contractual agreements including confidentiality and acceptable use clauses.

2. Access would be granted after approval from respective unit.

3. Access MUST be revoked once Contract / Project is ended by Third party [Application / System Owner / HR / Security team Should be Notified]

9) Employee Training and Awareness

9.1) All [SecureCyberGates] employees SHOULD undergo training and assessment on this policy during their initial induction [Onboarding].

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

10) Compliance and Monitoring

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

10.2) 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].

10.3) 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 policy. These audits may include, but are not limited to:

- Reviewing Access Controls for System / Applications.
- Review Access Management Policy.

11) Escalation Matrix

11.1) 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]

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

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

12) Policy Exceptions

12.1) 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]]**

13) Policy Review and Updates

13.1) 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.

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

13.3) 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.

13.4) 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.

14) Conclusion

By implementing and adhering to this comprehensive Access Management 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://www.youtube.com/@SECURECYBERGATES
https://securecybergates.com/services
https://hackerone.com/crypto-khan
https://x.com/securecybergate
securecybergates@gmail.com

SECURE CYBER GATES