SECURE CYBER GATES

ACCEPTABLE USAGE POLICY

SECURE CYBER GATES

DOCUMENT CONTROL PAGE

Document ID	SCG/AUP/013/1.0
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/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 Acceptable Use Policy serves as guidance for Rules of Behaviour that apply to the use of [SecureCyberGates] provided IT resources. Following our Acceptable Use Policy is important and helpful for everyone, not just the operations and research staff, but also for maintaining the confidentiality, integrity and availability of [SecureCyberGates]systems and data.

This Acceptable Use Policy establishes the standards that promote fairness in ensuring that Data and system use complies with [SecureCyberGates] policies and standards.

This Policy applies to anyone employed by or conducting business for [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

It is important to note that every situation may not be addressed in this Acceptable Use Policy; if you are unsure how [SecureCyberGates] standards or values apply in a given situation, please ask questions and seek further guidance from HR team , IT or Security 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 Acceptable Use Policy.

2) Roles &Responsibilities

Roles	Responsibilities
CISO / Security Team	Review and Audit Acceptable Use Policy.
HR Team	Overseeing the implementation and enforcement of this policy.Create, Manage, Monitor, Maintain, Audit Acceptable Use Policy.
BU Heads or Project Managers	Ensuring that employees under their supervision comply with this policy. [Review Acceptable Use Policy]
Employees / Contractors	1. Read this Acceptable Use Policy 2. Ask questions / Provide Feedbacks 3. Report possible or actual violations of this Acceptable Use Policy.

3) Scope

This policy applies to all individuals accessing or operating any IT resources owned, licensed or managed by [SecureCyberGates] This includes but is not limited to:

- Computer systems, servers, networks and network equipment
- Mobile devices such as smartphones, tablets, and laptops
- Software applications and databases
- Cloud services, storage, and collaboration platforms
- Email, messaging, and unified communications systems
- Internet connectivity and web services
- Physical technology infrastructure, equipment and facilities

The requirements cover the use of [SecureCyberGates] IT resources from any location, including on-premises at [SecureCyberGates] offices, data centres, and facilities as well as remote access from off-site.

4) Rules of Behaviour (Acceptable & Unacceptable Use)

4.1) General Usage

- Only authorized users with a valid business need may access [SecureCyberGates] systems and data
- User accounts, passwords and other credentials must not be shared with anyone
- Only [SecureCyberGates] approved and issued devices are permitted to access corporate systems
- Personal devices must go through IT's onboarding process before accessing [SecureCyberGates] resources
- [SecureCyberGates] IT assets are for approved business purposes only. Personal use should be limited.
- Users must respect intellectual property rights, licensing terms and copyright laws
- These Rules of Behaviour apply to the use of [SecureCyberGates] provided IT resources, regardless of the geographic location
- Data and system use must comply with [SecureCyberGates] policies and standards.
- Unauthorized access to data and/or systems is prohibited.
- Users must prevent unauthorized disclosure or modification of sensitive information,
- including Personally Identifiable Information (PII).

5) Acceptable Use Principles

5.1) User Access and Responsibilities

- Only authorized users with a valid business need may access [SecureCyberGates] IT resources and data
- User accounts, passwords and other access credentials are for individual use only and must not be shared
- [SecureCyberGates] IT assets and services are provided for approved business purposes. Personal use should be limited in scope.
- Users must respect intellectual property rights, software licensing terms and copyright laws at all times
- [SecureCyberGates] data and systems must be properly secured based on data classification and sensitivity levels

5.2) Unacceptable Activities

To protect [SecureCyberGates] 's systems, data and overall security posture, the following activities are strictly prohibited:

- Access and/or share information outside the purview of their job function.
- Share Google Drive files and/or folders with anyone outside [SecureCyberGates].
- Direct or encourage others to violate organizational policies, procedures, standards or guidelines.
- Circumvent security safeguards or reconfigure systems except as authorized (e.g., violation of least privilege).
- Use another user's account, identity, or password.
- Exceed authorized access to sensitive information.
- Cause congestion, delay, or disruption of service to any organization-owned IT resource. For example, greeting cards, video, sound or other large file attachments can degrade the performance of the entire network, as do some uses of "push" technology, such as audio and video streaming from the Internet.
- Create, download, view, store, copy or transmit materials related to sexually explicit or sexually oriented materials.
- Create, download, view, store, copy or transmit materials related to gambling, illegal weapons, terrorist activities, illegal activities or activities otherwise prohibited.
- Store sensitive information in public folders or other insecure physical or electronic storage locations.
- Share sensitive information, except as authorized and with formal agreements that ensure third parties will adequately protect it.
- Transport, transfer, email, remotely access, or download sensitive information, inclusive of PII, unless such action is explicitly permitted by the manager or owner of such information.

- Store sensitive information on mobile devices such as laptops, smartphones, USB flash drives, or on remote systems without authorization or appropriate safeguards, as
- stipulated by organization policies.
- Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information for personal use for self or others.
- Use organization-provided IT resources for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g., such as consulting for pay, administration of business transactions, the sale of goods or services, etc.).
- Engage in any outside fund-raising activity, including non-profit activities, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited
- partisan political activity.
- Establish unauthorized personal, commercial or non-profit organizational web pages on organization-provided systems.
- Use organization-owned IT resources as a staging ground or platform to gain unauthorized access to other systems.
- Create, copy, transmit, or retransmit chain letters or other unauthorized mass mailings regardless of the subject matter.
- Use organization-owned IT resources for activities that are inappropriate or offensive to
- fellow employees or the public. Such activities include, but are not limited to hate speech, harassment, bullying, intimidation or other abusive conduct that ridicules others on the basis of race, creed, religion, color, age, sex, disability, national origin, or sexual orientation.
- Add personal IT resources to existing organization-owned systems without the appropriate management authorization, including the installation of modems on data lines and reconfiguration of systems.
- Intentionally acquire, use, reproduce, transmit, or distribute any controlled information including computer software and data that includes information subject to the Privacy
- Act, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data, or export-controlled software or data.
- Send anonymous messages.
- Remove organization-proved IT resources from organization property without prior management authorization.
- Modify software without management approval.
- Post information on external blogs, social networking sites, newsgroups, bulletin boards or other public forums which:
    - Derogatory to [SecureCyberGates] or its management.
    - Contrary to [SecureCyberGates]'s mission or stated positions; or
    - Brings discredit or embarrassment to [SecureCyberGates].
- Use public charging stations at any time.

6) System and Data Access Controls

To prevent unauthorized access to [SecureCyberGates] IT resources and data, the following controls are enforced

6.1) Access Based on Least Privilege and Separation of Duties

- Users will only be granted the minimum level of system and data access required to fulfil their job roles and responsibilities.
- Role-based access controls are used to restrict access to production systems, applications and data sources.
- Special approval is required to access [SecureCyberGates] client data environments or other highly sensitive information.
- Multi-factor authentication is required for all remote access sessions and privileged account access

6.2) Access Based on Least Privilege and Separation of Duties

- Use of shared, generic or default vendor accounts is not permitted, with limited exceptions for emergency accounts
- User accounts will be disabled after 30 days of inactivity and permanently deleted after 60 days
- User access will be promptly removed when employees are terminated or change roles
- Periodic access reviews will be conducted to validate continued business need for user permissions

6.3) Auditing and Monitoring

- Detailed audit logging of system activities, user actions, security events and administrative changes is enabled
- Audit logs will be retained for forensics and compliance purposes based on data sensitivity and retention requirements
- User activities, including email, web browsing and file access may be monitored to detect potential violations

7) Data Protection Standards

7.1) Data Encryption Requirements

- All confidential, sensitive or restricted data must be encrypted both at rest and in transit
- Only use approved [SecureCyberGates] encryption solutions
- Encryption keys must be managed through [SecureCyberGates]'s centralized key management solution

7.2) Endpoint Security

- Any laptops, workstations, servers or mobile devices issued by [SecureCyberGates] must have the following security controls:
- Full disk encryption enabled (e.g. Windows BitLocker)
- Updated anti-malware/anti-virus protection with regular scanning
- Host-based firewalls and intrusion prevention enabled
- Secure configuration based on [SecureCyberGates] system hardening standards
- Disabling or tampering with these security controls is strictly prohibited

7.3) Physical Security Controls

- Physical security controls like locked cabinets, safes and secure areas must be used for storing restricted IT assets
- Confidential information must be properly secured and kept out of sight when printing or working remotely
- [SecureCyberGates] will maintain formal media handling and disposal procedures to securely sanitize/destroy data storage devices

7.4) Protecting Customer Data

- Access and use of [SecureCyberGates]customer data is only permitted for legitimate business purposes related to delivering services
- Only access the specific customer environments and datasets that you have been explicitly authorized for.
- Sharing or disclosing any [SecureCyberGates] customer data to external parties requires formal approval from the data owner

7.5) Intellectual Property Protection

- Any software, code, product designs, documentation or other intellectual property created by [SecureCyberGates] employees is considered confidential company property
- Reproduction, distribution or unauthorized use of [SecureCyberGates] IP is strictly prohibited and may violate licensing terms

8) Email and Internet Usage

While [SecureCyberGates] provides internet connectivity and email services to enable core business functions, the following applies regarding acceptable use:

8.1) Business Use vs Personal Use

- [SecureCyberGates]'s internet, email and communication services are provided primarily for legitimate business purposes
- Reasonable personal use is permitted but should be limited in scope and must not violate policies or impact operations
- Personal use may still be subject to monitoring and should not be considered fully private

8.2) Handling Sensitive Data

- Confidential, sensitive or restricted data must be encrypted before being transmitted over external networks
- Use approved [SecureCyberGates] email encryption and rights management solutions for securing sensitive email communications

8.3) Prohibited Activities

- Mass email distribution, chain letters, solicitations or other forms of spam are not permitted
- Internet bandwidth should be preserved for business priorities - excessive streaming, gaming etc. should be avoided
- Users must not access, download, store or distribute illegal or unauthorized content such as:
  - Illegal or unlicensed software, media or other copyrighted material
  - Malicious content like malware, hacking tools, vulnerabilities
  - Content that is offensive, discriminatory, unethical or otherwise inappropriate
- Activities on [SecureCyberGates] systems are subject to monitoring, including website browsing, downloads and communications

9) Mobile Device Security

The use of mobile devices like laptops, tablets and smartphones to access [SecureCyberGates] data and systems introduces additional security risks that must be addressed:

Only [SecureCyberGates] approved devices can be used to access [SecureCyberGates] IT resources and data.

Mobile devices must have the following security controls properly configured:

- Passcode/password protection enabled with automatic locking
- Full disk encryption, either natively or through a third-party solution
- Remote wipe capabilities configured to corporate mobile device management (MDM)
- Antivirus/anti-malware protection with latest definitions
- Firmware/OS patched and up-to-date

When possible, mobile devices should only access [SecureCyberGates] networks over an approved and secured connection:

- Connect over [SecureCyberGates] 's VPN solution when off [SecureCyberGates] premises
- Connect directly to [SecureCyberGates] office networks when on-premises

- Connecting over unsecured public WiFi should be avoided when accessing [SecureCyberGates] resources

Mobile devices must be kept physically secured at all times:

- Do not leave devices unattended or unsecured in public areas
- Use cable locks or other deterrents to prevent theft when travelling
- Any lost or stolen devices must be immediately reported to the IT team for remote wipe

Accessing and Syncing Corporate Data:

- Users should only access and sync corporate data to mobile devices through approved and secured [SecureCyberGates] applications
  - This includes email clients, cloud storage apps, VDI clients, enterprise mobility management (EMM), etc.
  - Personal apps, cloud services like Dropbox/Google Drive and other consumer services should not be used to store or access [SecureCyberGates] data

- Data should be containerized within the managed [SecureCyberGates] environment on mobile devices

  - iOS: Use managed Apple IDs, MDM deployment, secure mail/data containers
  - Android: Deploy approved secure workspace containers, email and data protection

- EMM and MDM solutions will be used to centrally configure, update and wipe devices
- Only cloud services managed by [SecureCyberGates] like OneDrive, SharePoint can sync data
- Local storage of data on mobile devices should be avoided when possible

Mobile devices must be returned to [SecureCyberGates]'s IT team when rotating devices or separating from the company:

- Devices will be properly wiped of all data and configured for provisioning to other users
- Attempting to wipe or reset devices yourself is prohibited and could leave data unwiped

10) Remote Access

[SecureCyberGates] provides the ability for authorized users to remotely access internal networks, systems and data sources in order to perform job duties from off-premises locations. However, additional technical safeguards are required:

- Remote access is only permitted through [SecureCyberGates]'s centrally managed VPN solution. No other remote access tools may be installed or used to bypass the VPN without approval
- Multi-factor authentication is enforced and required for all remote access sessions
- Remote sessions should be terminated as soon as work is completed
- Leaving remote sessions connected and unattended poses security risks
- Users must take measures to maintain physical security when working remotely:
  - Ensure no one can view your screen or access your device when unattended
  - Connect headphones when discussing or reviewing sensitive data
  - Lock your screen or disconnect the session before leaving your laptop/device
- Activities on remote sessions are subject to monitoring and audit logging. User actions like browsing logs, application usage, file access etc may be recorded

11) Security Incident Handling and Reporting

All [SecureCyberGates] personnel, including employees, contractors and third parties, are responsible for identifying and immediately reporting any potential security incidents or events that could impact IT resources or data. These include:

- Suspected malware, virus or ransomware infections
- Potential data breaches, data exposure incidents or unauthorized data access attempts
- Hacking, system compromise or unauthorized access incidents
- Lost or stolen devices that may contain sensitive [SecureCyberGates]data
- Social engineering attempts to trick users into exposing passwords or data
- Vulnerabilities or misconfigurations that could enable security incidents in the future

Suspected incidents should be reported immediately by emailing security@securecybergates.com .The [SecureCyberGates] Security team will triage events, initiate investigations and take appropriate remediation steps which may include:

- Isolating and forensically imaging affected systems to investigate
- Disabling or resetting compromised user accounts
- Forcing password resets on associated user accounts and systems
- Remotely wiping data from lost or stolen devices
- Installing security updates or applying configuration changes to mitigate vulnerabilities
- Working with relevant internal teams and/or external authorities for major incidents

12) Employee Training and Awareness

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

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

13) Compliance and Monitoring

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

13.2) Third-party users, contractors, and vendors who **FAIL** to comply with this policy may have their access to [SecureCyberGates]systems 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].

13.3) Periodic Audits and Assessments : [SecureCyberGates]'s HR department, in collaboration with the Information Security team, will conduct periodic audits and assessments to evaluate compliance with this HR policy.

14) Escalation Matrix

14.1) 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	HR	Final-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]

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

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

15) Policy Exceptions

15.1) 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]]**

16) Policy Review and Updates

16.1) This HR 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.

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

16.3) 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.

16.4) 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.

17) Employee Signature

I hereby acknowledge that I've read the Acceptable Use Policy and have had the opportunity to ask questions. I agree to follow the guidelines outlined above.

________________________________ ____________

Employee Signature **Date**

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

https://securecybergates.com https://www.linkedin.com/in/aj57/