SECURE CYBER GATES

CODE OF CONDUCT POLICY

SECURE CYBER GATES

DOCUMENT CONTROL PAGE

Document ID	SCG/COC/014/1.0
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 Code of Conduct serves as a guide for ethical decision-making. At [SecureCyberGates], we require that all of our employees conduct themselves according to the highest standards of ethics, integrity, and behavior when interacting with our clients, colleagues, and other stakeholders. This includes, but is not necessarily limited to, full compliance with all legal obligations imposed by statute or any other source of law.

This Code of Conduct establishes the standards of behavior that must be met by all employees. Where these standards are not met, appropriate disciplinary action will be taken.

It is important to note that every situation you face may not be addressed in this Code of Conduct; if you are unsure how [SecureCyberGates] standards or values apply in a given situation, please ask questions and seek further guidance from the appropriate personnel or department.

Each and every one of us is responsible for ensuring that we follow the highest ethical standards of business conduct, and we will be held accountable for upholding our commitments to this Code of Conduct and the related policies and procedures.

2) Roles &Responsibilities

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

3) Scope

This Policy applies to anyone employed by or conducting business for [SecureCyberGates], including:

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

4) Standards of Conduct

[SecureCyberGates] is committed to:

- Operating an economically successful business to provide a consistent level of steady work to all employees.
- Selecting people based on skill, training, ability, attitude, and character without discrimination regarding age, sex, color, race, creed, national origin, religious persuasion, marital status, political belief, or disability that does not prohibit performance of essential job functions.
- Compensating all employees according to their effort and contribution to the success of our business.
- Periodically reviewing wages, employee benefits, and working conditions to provide maximum benefits consistent with sound business practices.
- Providing paid vacations and holidays to all eligible employees.
- Providing eligible employees with medical, retirement, and other benefits.
- Dedicating efforts to exceed client expectations by providing high-quality services and timely deliverables.
- Developing competent people who understand and meet our objectives and accept with open minds the ideas, suggestions, and constructive criticisms of fellow co-workers.
- Assuring employees an opportunity to discuss any issues or concerns with the management of [SecureCyberGates].
- Making prompt and fair adjustments of any complaints that may arise in the everyday conduct of our business, to the extent practicable and reasonable.
- Respecting individual rights and treating all employees with courtesy and consideration.
- Maintaining mutual respect in our working relationships.
- Providing an attractive, comfortable, orderly, and safe building and offices.

5) Business Ethics

General we are committed to fostering an open and honest culture of trust and integrity. We interact responsibly, ethically, and transparently with all our stakeholders.

We are truthful in our interactions with patients, customers, and stakeholders, and we do not offer, promise, provide, or accept anything of value to inappropriately influence a decision or gain an unfair advantage. We do not allow others to give bribes on our behalf. This applies to all interactions with our stakeholders.

Compliance with laws and international standards for responsible business conduct inspires trust in our culture of integrity. We comply with all laws, regulations, policies, standards, and procedures that apply to our business.

5.1) Bribery and Improper Advantages

At [SecureCyberGates], we compete fairly and are responsible, ethical, and transparent in our business. We do not bribe or provide improper advantages. Bribes and improper advantages can be monetary, but they may also include non-monetary items such as improper gifts, products, hospitality and meals, travel and accommodation, or other items or services that ultimately mean the transfer of value in return for special consideration.

It does not matter whether you use your own private money or [SecureCyberGates]'s funds to pay a bribe or improper advantage or do so via a third party. All are against this Code of Conduct.

[SecureCyberGates] prohibits facilitation payments worldwide. A facilitation payment broadly means any unofficial transfer of value to a Public Official for taking routine governmental actions.

5.2) Fraud

We are committed to preventing and detecting fraud - we do not engage in any kind of fraud against [SecureCyberGates], any of our business partners, or government entities.

Generally, fraud means deliberately deceiving a person or company to unjustly obtain an unauthorized benefit, such as money, property, or services, and includes some of the following example activities:

- Theft of funds, inventory, or any other asset from [SecureCyberGates], including false expense reports
- Manipulation of accounting information or financial statements
- Misuse or forgery of any document (e.g., records, data, accounts, expense claims, or contracts)

5.3) Data Privacy

We respect the personal data that we collect from our employees, patients, Healthcare Professionals, and other stakeholders. We are committed to complying with all applicable laws related to data privacy.

When you use personal data as part of your work at [SecureCyberGates], you must:

- Use the least amount of personal data needed.
- Where required by local law and regulation, inform people about how we use their personal data.
- Only share personal data with those who need to know.
- Store personal data securely.
- Delete personal data when no longer needed.

5.4) Human Rights

We respect internationally recognized human rights. Our mission is to avoid infringing on the human rights of our employees, communities, and other stakeholders. We strive to prevent and mitigate adverse human rights impacts with which we are involved, either in our own business operations or through business relationships. We promote a positive and

inclusive work environment that respects the individual and is free from any form of discrimination or harassment.

6) Vendor Code of Conduct

The Company expects its vendors and suppliers to adhere to the highest ethical standards and comply with all applicable laws and regulations. Vendors are required to:

- Maintain integrity and professionalism in all business dealings.
- Respect intellectual property rights and safeguard confidential information.
- Provide accurate and truthful information regarding their products and services.
- Comply with relevant environmental, health, and safety regulations.
- Prohibit the use of forced labor, child labor, and unfair employment practices.
- Avoid conflicts of interest and disclose any potential conflicts to the Company.
- Refrain from offering or accepting bribes, kickbacks, or any form of improper payments.
- Cooperate with the Company's audits and provide access to relevant records upon request.

The Company reserves the right to terminate business relationships with vendors who fail to comply with this Vendor Code of Conduct

7) External Communications

Everything we communicate about our company can have an impact on our reputation, coworkers and the brand.

Press and Media Management

If you are ever contacted by the media, refer them to the Marketing and Communications OR HR team. Do refrain yourself from speaking on behalf of the company to avoid any confusion/sharing of inaccurate information.

Usage of Social Media

We are allowed to associate ourselves with the company when posting in social media, but we need to make it clear that they are personal opinions.

Rule(s) of thumb to follow:

- ✓ Be aware that you are responsible for what you publish, so use good judgment.
- ✓ Do not use social media to intimidate, harass, discriminate or defame against the company, customers or fellow coworkers.
- ✓ Be clear that your statements are your own opinions, not those of the Company's.
- ✓ Protect the company's proprietary information

Giving Advice

You can give advice, but you'll need to look out for the following:

✓ Do not divulge any confidential information about the company (this includes any of our customers, software, processes, slides, products, materials)

✓ Avoid sharing about events/incidents that can potentially leak any confidential information

✓ Do not mention any names, including customers, vendors, partners, or colleagues.

Conversely, sharing public information (e.g.: product information on our websites) is always welcomed.

Speaking at an Event

If you are invited to speak or present at an event, notify the Marketing and Communications or HR team before accepting and have them review and approve any materials you present or discuss.

✓ Ensure you speak positively about the company

✓ Make sure you are well groomed and looking your best

✓ Do not disclose any confidential information (this includes any of our customer's software)

✓ Do not mention any names, including customers, vendors, partners, or colleagues.

✓ Before accepting free travel or accommodation, check that the proposed hospitality is appropriate and will not be seen as bribes.

8) Report a Concern

[SecureCyberGates] encourages an open and honest culture of trust and integrity. Part of building a culture of trust is speaking up about any ethical or compliance concern so we can address possible issues.

Anyone who becomes aware of an actual or potential violation of this Code of Conduct can and should speak up. If you feel comfortable, talk to your manager about it. If you are not comfortable with this, please speak to the [HR@Securecybergates.com] at [SecureCyberGates].

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 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 HR department, in collaboration with the Information Security team, will conduct periodic audits and assessments to evaluate compliance with this HR 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	HR	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 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.

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

[SecureCyberGates]is committed to maintaining the highest standards for Data Security. Every employee plays a crucial role in safeguarding confidential information, and their diligence and cooperation are essential for the successful implementation of this policy.

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