Code of Conduct and Ethics

The Code of Conduct and Ethics applies to all the employees of Swin Technologies Pvt. Ltd., which is referred to in this Code as “Company” or “The Company”.

1. Equal Opportunity Workplace

SWIN Technologies Pvt. Ltd. strive to provide a work environment free of discrimination and harassment. The Company is an equal opportunity employer, and the employment decisions are based on merit and business needs. The Company is committed to following fair employment practices that provide equal opportunity in all areas of employment, which includes promotion, transfer, deputation, recruitment, layoff or termination, wages or other compensation, selection for training, including apprenticeship and / or on the job training. The Company does not discriminate or allow harassment based on race, color, creed, caste, religion, gender, nationality, disability, sexual orientation, gender expression, gender identity or any other legally protected status. The Company will ensure adherence to the laws of the land with regard to employment norms and will not indulge in practices such as employing bonded labour, child labour etc.

2. Safe Place

Workplace should be a healthy and safe environment to the employees. All forms of substance abuse as well as the use or distribution of drugs and alcohol while at work is prohibited. Unless required as part of the role (for instance, the security personnel where deemed necessary), possession and / or use of weapons / fire arms or ammunition while on business of the company is prohibited. If there is any unsafe situation observed at work, it needs to be reported and the employee could reach the helpline. Employees are advised to take some time to familiarize the emergency procedures and the safety manuals as applicable to the facility wherever they work.

3. Respect for Individuals

Mutual respect must be the basis for all work relationships. Engaging in behaviour that ridicules, belittles, intimidates, threatens or demeans, or any other conduct that interferes with a co-worker’s ability to do their job is treated as inappropriate. Employees are expected to treat others with respect and dignity in a professional manner creating a work environment that is inclusive, supportive and free of harassment and unlawful discrimination.

4. Sexual Harassment and any discriminatory Harassment

Sexual harassment and other discriminatory harassments are illegal and violate Company policies. Actions or words of a sexual nature that harass or intimidate others are prohibited. Similarly, actions or words that harass or demean based on race, color, creed, ethnicity, caste, religion, national origin, gender, sexual orientation, age, disability, covered veteran status, marital status, or any unlawful basis are also strictly prohibited.

5. Ethics

Employees should ensure that they comply both in letter and spirit – honesty, integrity and fair dealing. Employees should never offer directly or indirectly, any form of gift, entertainment or anything of value to any official, commercial partners including customers or their representatives to

- Obtain or retain any business
- Towards any unfair advantage
- Influence any business decision

This includes bribes, kickbacks and facilitation payments.

5.1 Gifts and Entertainment

When a gift is made to a customer, a Government official or any third party, employees should keep the following in mind

a) It is not done to obtain or retain business or gain an improper advantage in business.
b) It is lawful under the laws of the country where the gift is being given and permitted under the policies of the client;
c) It constitutes a bona fide promotion or goodwill expenditure;
d) It is not in the form of cash;
e) The gift is accurately recorded in the Company's books and records;
f) It is of nominal value

Accepting Gifts : The same principles apply if customer or supplier wishes to give the Company/employees a gift or any other token of their appreciation.

6. Conflicts of Interest

Company policy prohibit Conflicts of Interest. A "Conflict of Interest" occurs when your private interest interferes in any way with the interests of Company. In addition to avoiding conflicts of interest, you should also avoid even the appearance of a conflict.

6.1 Corporate opportunities:

You owe a duty to Company to advance its legitimate interests. You are prohibited from competing with the Company and from using Corporate property, information or position for personal opportunities or gain.

6.2 Outside activities

You may not serve as a Director, officer, trustee, and partner or in any other principal position of another for-profit or publicly held organization or company without the prior approval of Company's Director (or a designee). You should obtain approval from the Company before agreeing to serve on the board or in a principal position of a trade or professional association or of a non-profit organization. In any event, these outside activities must not impact in any way your daily job responsibilities in your current position.

6.3 Second Job

Unless the Company otherwise consents in its sole discretion, you will devote your entire resources and full and undivided attention exclusively to the business of the Company during the term of your employment with the Company and shall not accept any other employment or engagement (honorary or otherwise).

6.4 Vendors, Suppliers and Consultants

All Vendors, suppliers and consultants shall be approved in accordance with Company policies and procedures. Company's business relationships must be totally based on their ability to competitively meet the Company's business needs. If your association with a current or prospective Company Vendor, supplier or consultant is of a nature that gives rise, or potentially gives rise, to a conflict of interest, the Company may have to refrain from entering into the relationship and, in any event, you must not be involved in any way with approving, managing or influencing the Company's business relationship.

6.5 Communication of conflicts

All potential and actual conflicts of interest or material transactions or relationships that reasonably could be expected to give rise to such a conflict or the appearance of such a conflict must be disclosed. If you are doubtful whether a conflict of interest

exists after consulting this code, you should seek assistance from the management of the Company, so that you could make that determination.

7. Protecting Company assets

The confidential information is a valuable asset for the Company and every employee must protect it. Confidential information includes all non-public information (regardless of its source) that might be of use to the Company's competitors or harmful to the Company if disclosed. Employees must take care that all confidential information is used for Company business purpose only. Upon joining Swin Technologies Ltd, all employees sign a Confidentiality and Non-disclosure Agreement which details their confidentiality obligations to the Company. Confidential or proprietary information about clients, organization, or other parties, which has been gained through employment or affiliation with Swin Technologies Pvt Ltd., may not be used for personal advantage or for the benefit of third parties.

Employees must not post or discuss information concerning the Company's services or business on the internet unless they are authorized to do so. Employees should remember that their online posts would be available for a long time, and hence they are required to think carefully prior posting any information that could affect the Company.

The intellectual property of the Company includes copyrights, patents, trademarks, service marks, trade secrets, design rights, logos, brands and know-how. The IP of the Company must be protected as a vital business asset.

a) Expense Claims

Each manager and employee has an obligation to each other and to the Company to comply with Swin Technologies Pvt Ltd business expenses and reimbursement policies and practices. All business-related expense claims must be authorized by their respective managers before being incurred. Personal expenses will not be reimbursed by the Company. Original bills / receipts need to be submitted for re-imbursements as per actuals.

In case of any bills/receipts/any such documents submitted against claim/re-imbursements were found to be not true (fake bills), upon verification, necessary disciplinary action up to and including termination would be taken against the employee.

8. Commitment to Clients and Suppliers

All of the employees are expected to deal fairly with the Company's customers, suppliers, partners, service providers, competitors, and anyone else with whom there is interaction during work. Unfair advantage should not be taken by anyone through manipulation, concealment,

abuse of privileged information, misrepresentation of facts or any other unfair dealing practice. As employees have access to client information, that may not be available to the public, employees are required to preserve the confidentiality of information obtained in client service. Information of a confidential, private and sensitive nature must be used responsibly and controlled and protected to prevent its prohibited, arbitrary or careless disclosure. Employees should not knowingly make any false or misleading statements regarding our competitors or the products and services of our competitors, customers or suppliers. Collusion among competitors is illegal. Our communications with competitors should avoid subjects such as prices or other terms and conditions of sale, customers and suppliers. Employees should not enter into an agreement or understanding, written or oral, express or implied, with any competitor on these subjects.

9. IT Security:

9.1 Policy:

All information, data and messages created, received, sent or stored on Company's computer equipment are, at all times, the property of the Company.
Employees are responsible for maintaining confidentiality of the information stored in the device.
All installed software (free/purchased/open-source/trial versions) must comply with relevant licensing and Terms of Service.
The company reserves the right to audit the device on a regular basis to ensure compliance.

9.2 Email and Internet:

All email accounts maintained on the Company's email systems are property of the Company. Company has the right to monitor and keep a record of any email that users transmit via the Company's email system.
All company employees, full-time or part-time, independent contractors, interns, consultants, clients, and other third parties who have been granted the right to use the Company's email services are defined as the users.
Employees are advised to use shared drive link to exchange large files instead of sending them as email attachments, especially when there is a necessity to share the files with more than one associate. This will improve the speed of the email client and also reduce the storage use on the email server.
Emails are to be used only for business purposes and all email communications are considered "official".
The company reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose.

Please do not use e-mail, internet, and other company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal. Browsing, displaying on the screen, downloading or storing any such content will be considered as gross misconduct.

Any material that is fraudulent, harassing, profane, sexually explicit, obscene, intimidating, defamatory, or otherwise unlawful, offensive (including offensive material concerning sex, race, color, nationality, religion, age, disability, or any other characteristic protected by law), or in violation of Company's Equal Opportunity Employment Policy and its policies against sexual or other harassment may not be seen displayed, downloaded or stored in the Company's Computer. Employees encountering, witnessing or receiving any such material should immediately report the incident to their immediate reporting manager, HR and IT Security for immediate action.

a) Do not disclose personnel information unless authorised.
b) The Company may use softwares to identify websites with inappropriate content and may block them to be accessed through Company networks.
c) Do not use internet to download any games / entertainment software including wall paper and screen savers or to play games over the internet.
d) Keep passwords and accounts secure. It is unacceptable to share the password with other person either internal or external. It is also unacceptable to obtain password from others and try to access other's login. Every system's login including email system need to be used only by registered users and not anyone else.
e) Do not open any attachment from unknown / unsigned sources as they are the primary source of computer viruses.
f) Do not install any unauthorised software or hardware including modems.
g) Request approval from management prior to installing any software, hardware or third party connections etc.
h) Always leave desks clear of sensitive data and lock computer screens when unattended.

9.3 Unacceptable uses:

a) Installing un-authorized network access points / routers or other networking equipment.
b) Allowing non-employees to use the device (including family and friends)
c) Introduction of malicious programs into systems/network (viruses / trojans / malware / ransomware etc.) with an intention to infect, disrupt or damage the company's resources and equipment.
d) Installation of pirated software which does not have appropriate licensing.
e) Distributing or sharing access credentials (user name/passwords) to any internal or external resources.
f) Creating or enabling security breaches within the network or the company's devices.

g) Circumventing authentication/security measures of any machine, network or systems (except when duly authorized)
h) Establishing a persistent network tunnel or connections to allow unauthorized equipment to connect to the infrastructure (ssh/remote desktop etc).
i) Providing any information about the IT infrastructure, security measures, network settings, personnel details, vendors or service providers to external parties.

9.4 Information Security :

Any information about the Company or its clients is to be treated as confidential unless it is already available in the public domain.
The Confidential information shall not be copied to or stored on any non-Company devices.
Employees need to ensure the safety of any device with confidential data and make sure it meets the security requirements of encryption, physical device security and logical device security.
Employees must use extreme caution when opening mails or attachments from unknown senders.
Computers should have security patches and updates applied as soon as they are available.
Employees should always use their best judgement about storing and securing the devices in their possession.
They should never leave the equipment unattended in a public space and always lock it up and secure it when they are away from the device.
Information security incidents (violation of the policy) must be reported, without delay, to the individual responsible for incident response locally. An alert email must be sent to the management.
Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment.

10. Physical Security

Each and every employee would be given the access card to enter the office premises. Employees are requested to swipe their access card to enter the office premise/work station.

a) Tail gating is strictly prohibited. Use your own access card to make an entry. Do not tailgate.
b) In case of loss of the access card, it should be immediately reported to your Manager.
c) In the event of the employee not carrying the card on any given day, it needs to be reported to the manager and the admin giving the reasons for not able to produce the card. Admin would organize for a temporary access for that day.

d) Visitors must always be escorted by an employee when in areas which hold company / client sensitive information.
e) If in doubt / unclear of any of the policies / guidelines, please discuss with your manager / admin department.

11. Administering the Code

11.1 Reporting of unethical / illegal behaviour

If you are aware of any illegal or unethical behaviour or if you believe that an applicable law, rule or regulation or this code has been violated, the matter must be promptly reported to your Manager or Company executives.

Your Reporting Manager is normally the first person you should contact if you have questions about anything in this Code or if you believe Company or an associate is violating the law or Company policy or engaging in conduct that appears unethical. Under some circumstances, it may be impractical or you may feel uncomfortable raising a matter with your reporting manager. In those instances, you may contact the head of your department or any other Company executives. Furthermore, you should take care to report violations to a person who you believe is not involved in the alleged violation. All reports of alleged violations will be promptly investigated and, if appropriate, remedied and if legally required, immediately reported to the proper governmental authority.

You will be expected to cooperate in assuring that violations of this Code are promptly addressed. Company has a policy of protecting the confidentiality of those making reports of possible misconduct to the maximum extent permitted by law. In no event, will there be any retaliation against someone for reporting an activity that he or she in good faith believes to be a violation of any law, rule, regulation, internal policy of this Code. Any manager intimidating or imposing sanctions on someone for reporting a matter will be disciplined up to and including termination.

11.2 Disciplinary Action

Violations of this code, Company policies, and applicable laws are considered seriously. Where appropriate, the Company takes prompt corrective action, up to and including termination of employment.

All the employees are expected to adhere to these rules in carrying out their duties for the Company. The Company strives for consistency and fairness in discipline for Code violations. Discipline may include a verbal or written warning, suspension with or without pay, loss or reduction in bonus or stock options, or, for the most serious offenses or repeated misconduct, termination of employment.