1. Acknowledgement and Agreement regarding the Company's Anti-Sexual Harassment Policy and Anti-Discrimination, Harassment and Bullying Policy

This is to acknowledge that I have received a copy of the Company's Anti-Sexual Harassment Policy, Anti-Discrimination, Harassment and Bullying Policy and understand the Company's policy that there be no discrimination or harassment against any employee or applicant for employment on the basis of sex, gender, race, color, religion, sexual orientation, age, mental or physical disability, medical condition, national origin, marital status, veteran status, or any other characteristics protected under Central or State law or local ordinances.

I understand the Company is committed to a work environment free of harassment and that the Company specifically prohibits retaliation whenever an employee or applicant makes a good faith complaint that they have been subjected to harassment. Accordingly, I specifically agree that to the extent I am the subject of any conduct which I view to constitute harassment or which is otherwise in violation of the Company's Anti-Harassment Policy, I will immediately report such conduct to my supervisor or to a management level employee with whom I feel comfortable.

I understand and agree that to the extent I do not use the grievance procedures outlined herein or in the Company's Anti-Harassment Policy, the Company shall have the right to presume that I have not been subjected to any harassment and/or that I have welcomed the conduct.

Name : **Sheng Lu**
E-Mail: **foretribe@gmail.com**

Time stamp: **8/23/2022 12:18:48 PM**
IP address: True-Client-IP ->'220.158.191.49' :: HTTP_X_FORWARDED_FOR ->'220.158.191.49,

2. Code of Conduct

All employees of Infosys are expected to abide by the value system and display openness, integrity, transparency and an attention to ethics in their behavior. Employees are depended on to exercise discretion in all dealings related to the company.

All Employees shall:

1. Maintain confidentiality of all transactions and not divulge any process or trade secret to any other organization or person.
2. Not receive or offer bribes to any person.
3. Use company equipment like computers and peripherals, etc., solely for the purpose of furthering company business interests and not for personal interests, whether monetary or otherwise.
4. Disclose the details of compliments received from customers/suppliers, etc., and acknowledge that the company reserves the right to periodically set limits, exceeding which the gift will be given to the company.
5. Not be involved in any other business for profit, while in the employment of company, other than as a shareholder. Employees shall be aware that any involvement with a non-profit organization shall be with the company's prior approval.
6. Not display any objectionable or distasteful material through the Bulletin boards, Intranet or any other company messaging service.
7. Not communicate in any way that utilizes the print or electronic media, without prior permission.
8. Disclose to the company, the details of any design or invention relating to the company's area of business, as the company reserves the right to treat it appropriately.
9. Not indulge in insider trading and not use any company information that he encounters while in his/her capacity as an employee, for personal benefit.
10. Behave in such a way that enhances the company's image while at a customer's site.
11. Follow the expense guidelines outlined by the company while on work in India or overseas.
12. Submit weekly time records of professional activities to their supervisor / manager on a regular basis.
13. Observe all company policies, rules and procedures

Name : Sheng Lu
E-Mail: foretribe@gmail.com

Time stamp: 8/23/2022 12:19:13 PM
IP address: True-Client-IP ->'220.158.191.49' :: HTTP_X_FORWARDED_FOR ->'220.158.191.49,

3. Privacy & data protection

Infosys Technologies Limited (ABN 52 090 591 209), its subsidiaries, associates and affiliated companies (collectively referred to as “Infosys”, “us”, “we”) are committed to process your personal data as per the laws of your jurisdiction. We hereby notify you the following information about your personal data processing -

Personal data elements collected/processed:

- **Personal Details** such as name, photograph, date of birth, Age, place of birth, nationality, domicile, gender, Marital status, Citizenship, Residential Status etc.
- **Contact information** such as contact Number, Emergency Contact Number, Location, City of Work, Permanent Address, Email ID (personal and Official), city, Residential Address in Australia, etc.
- **Family details** such as family members’ names, relationship, Date of Birth, etc.
- **Education details**: Such as marks/percentage, year of passing, board/university, degree/level, school/college, etc.
- **Work experience details** such as previous employer, designation in previous employment, role, date of employment, Previous salary details, Previous employment references etc.
- **National identification information** such as Passport and visa related information (e.g. date of application, dates of validity, emigration check requirement, address, place of issue, etc.), National Identification Number (or equivalent), Nationality, Citizenship, work permits, etc.
- **Benefits related information** such as your date of birth, National Identification number, marital status, information about your pension and other welfare benefits; this information may also include data about your dependents based on eligibility and choice of benefits provided etc.
- **Beneficiaries, dependents and emergency contact information** such as information about any beneficiaries, dependents, emergency contacts, next of kin etc.
- **Financial Information** such as your Taxation related details, Dependent care details, bank account details, local wages, investment proofs submitted by you, bills/receipts submitted by you, Claims (e.g. Bills and claims related to telephone, food etc.), locality name and project assignment details, etc.
- **Travel-related records** such as Passport and visa related information (e.g. date of application, dates of validity, emigration check requirement, address, place of issue, etc.); Itinerary (Date, pickup location, pickup time, Car type); mode of travel, travel class, location (from and to), departure date and time, food preferences and Travel related details such as Frequent flyer/traveler membership numbers/traveler preferences and accommodation details, etc.
- **Background checks and screening** (along with the results) such as education verification, past employment verification, criminal records, driver’s license checks, final BGC reports, referral checks etc.
- **Salary, Compensation, benefits and other financial information** such as performance based bonus letters, meal voucher letter; confirmation letter, disciplinary documents (if any), salary pay slips, separation related documents (if any), geo specific employment related documents (if any), National Identification details, benefit related data, Financial details such as Salary

Bank account details (as applicable), pension details, medical insurance, back ground check details, etc. Some of the data listed is directly collected from Infosys internal applications.

- **Employment related information and qualifications** such as role, Employee number, Date of Joining, Location of Joining, Location or City of Work, Country, Assignment Company, whether depute or base hire , Department, Unit, Employee Number, Employee Type, Job Level, Job Sub Level, Joining Date, joining details, Personal Level, Personal Sub Level, Practice unit, Project Details like Project Code etc.
- **Performance and development records** such as Career stream, Career Sub Stream, Certification Details, Confirmation Banding, Confirmation Rating, Confirmation date, , History of change in Role or Job Level, History of employment, Infosys Experience, Practice unit, Previous Experience, Role change history, Role Designation, Total Experience, Unit, Gender, training records (such as records of courses and training undertaken), performance reviews/appraisals, assessments, information security awareness score etc.
- **Disciplinary, capability and conduct records** such as details of warnings and other records relating to conduct, including grievances raised (as per HEAR and ASHI policy) etc.
- **Leave and Attendance records** such as Employee Number, Employee Name, Reason for leave, leave type (including special leaves, such as sick leave, maternity leave etc.) and associated supporting medical or other relevant documents as required, approver details etc.
- **Health and safety records** such as information relating to health and safety in the workplace, accidents and near misses, etc.
- **Information we obtain from monitoring** such as records of your use of our computer systems, corporate email or the Internet, and recordings from surveillance cameras on our business premises etc.
- **Individual opinion details** such as Employee related surveys etc.
- **Details related to social interaction on official forum** such as discussion on yammer, blog posts etc.
- **Official internal communication** and distribution lists
- **Information regarding your official phone or mobile device or SIM** such as your mobile phone number and mobile phone or device billing and usage records.
- **Digital Assets and IT related information** such as E-mail ID, IP address, passwords/PIN, domain user ID, mobile device details (manufacturer, model, serial number, IMEI number, SIM number, SIM Type, OS type, software), Wi-Fi details, Asset ID, MAC address, Meeting ID, VOIP Number, Phone Number, Device ID, Internet URL details, Software Type, Work location, Cubicle Id etc.
- **Biometric information** collected as part of ID cards for authorized access to work premises.

Purpose of collection: The Processing of the Personal data may be required for the following purposes:

- The Processing of your Personal data may be required in relation to a contract which You have entered with Infosys;
- To create and retain employee personal electronic files and for processing mandatory associated requests including but not limited to business travel, compensation review and processing, administration of benefits, transfers and confirmation;

- To maintain employment records;
- To conduct background checks or a verification on you;
- For IT services, support and security such as: Provision of hardware and software assets, Corporate Network Access, Communication and collaboration, Antivirus Installation, Storage Services, Infosys Internal Help desk (voice based support), Central authentication and authorization services, Internet usage, Messaging, Data sharing, storage, Hosting and backup, Resolution of technical issues, Enabling Use Your Own Device /Bring Your Own Device (if opted by you), etc.
- To administer/process your payroll, tax processing, compensation and benefits (salary fitment, review of compensation, health related benefits), insurance, pension contribution, salary and any other amounts we owe you.
- To determine your suitability for allocation to specific projects and positions that Infosys may need.
- When required to be Processed pursuant to Infosys' internal policies ad business requirements.
- To assess your personal and professional development, your suitability for allocation to specific projects and positions, promotions, benefits and other awards, internal job movements and staff restructuring, conflict of interest reporting, to fulfill our obligations to regulators (including demonstrating the suitability of employees for their role), etc.
- To process your leave and approvals, monitor absences etc. and address other issues that may arise from absences
- To be Processed based on a contract which Infosys may have with third parties for the receipt or provision of services;
- To provide services to our clients based on mutual agreed terms for sharing of data;
- To be Processed pursuant to a Financial obligation that Infosys has towards You
- To process/reimburse any expense claims incurred by you.
- To enable us to ensure that we are compliant with any application labor and/or other relevant laws in Australia;
- Your benefits related data will be required for the provision of various company related or statutory benefits, including insurance, to You (and your dependents), which will involve enrolling with external Insurance providers.
- For the provision of various company related or statutory benefits to You and for the administration of Benefits to You as an employee of Infosys;
- For global immigration purposes, work and residential permit, visa stamping process, determining your eligibility to work and fulfill our obligations such as tax reporting to relevant government authorities, etc.
- To address our legal obligations to you in relation to health and safety in the workplace, as applicable, etc.
- To assess and act related to disciplinary, capability, grievance and conduct issues, maintaining your employment records, monitoring and improving our human resources procedures etc.

- Comply with any applicable law, regulation, legal process or enforceable statutory requirement, enforce our site policies, or protect ours or other rights, property, or safety as required or permitted by law.
- To maintain your employee records, communicate with you for internal business purposes, tax reporting, issuance of tax statements or emergencies, maintain an internal employee directory, grant you access to internal systems, etc.
- To arrange or reimburse travel, contact you during travel, for taxing reimbursement of relocation expenses, statutory audits and as necessary with travel service providers, or in an emergency.
- In order to provide training to you during your course of employment with Infosys;
- To monitor electronic communications used on equipment provided by Infosys, which must only be used for business purposes etc.;
- To monitor your compliance with our internal policies and procedures, to investigate security breaches and misuse of computer equipment and systems, to protect the safety of employees and third parties, and to protect our property from theft, vandalism and damage.
- For security or the prevention, detection, or investigation of fraud, suspected or actual illegal activity, violations of company policy or rules, or other misconduct.

Data Recipients / Accessible to: Infosys may share the Personal data (as detailed above) with trusted third parties who assist us in conducting our business, or servicing you, with customary legal protections being embedded into the legal arrangements with such third parties including the third parties agreeing to keep this information confidential. Subject to the foregoing, the data recipients for the above Processing of Personal data may include but not be limited to the following:

- Internal recipients within Infosys, including Infosys' subsidiaries or affiliates, such as Human Resources, Finance, Facilities, Immigration, Travel, Project Delivery Units, Sales and Marketing, Infosys IT (IS, Computers and Communications Division/TIG), your manager, Units/Org Leadership;
- Infosys customers or third-party service providers or vendors who provide services to Infosys;
- Government Bodies including statutory, regulatory authorities, law-enforcement agencies;
- Auditors (internal/external);
- Banks (where applicable);
- Infosys' Clients; and
- Any other parties expressly or impliedly authorized by you for receiving such disclosures.

Data transfer (International): If necessary for the above stated purpose, the Personal Data listed above may be transferred to our offices, to our clients where applicable and our vendors/ third party service providers, in India and across the globe.

Data Storage: Your personal data will reside on Infosys', our Client's (as applicable) and our vendors/ third party service providers' servers located in India and across the globe.

Data Security: Appropriate measures will be taken to prevent unauthorized access, unlawful processing, unauthorized or accidental loss or destruction of the Personal Data.

Data Retention: Personal Data that is no longer required to be retained as per legal and business requirements will be disposed in a secure manner.

Data subject access rights: You are entitled at any time to access and rectify your personal data. In case of any requests, issues, concerns or queries you may reach out to your local HR via AHD.

Our Australia privacy policy, available at http://www.infosys.com/privacy-statement/Pages/australian-privacy-policy.aspx contains information about how you may access and correct the personal information that we hold about you and how to lodge a complaint relating to our treatment of your personal information, and how we will deal with such compliant. You may also contact us at details provided in the same privacy policy.

You acknowledge that any personal that you share about your dependents (or any other data subjects) is shared by **you only after seeking consent** from the person(s) to whom the personal data belongs. By **clicking the below button, you are confirming** that you have read this Privacy Notice for Infosys to hold and process your personal data for the above purposes.

Name : Sheng Lu
E-Mail: foretribe@gmail.com

Time stamp: 8/23/2022 12:19:04 PM
IP address: True-Client-IP ->'220.158.191.49' :: HTTP_X_FORWARDED_FOR ->'220.158.191.49,

4. Declaration – Information provided on joining

I certify that all information that I have provided Infosys with respect to my employment at Infosys, including my employment status, my personal background, professional standing, work history, criminal records and qualifications (whether educational, professional or otherwise) is true, complete and correct. I also certify that I have not withheld any information from Infosys that would affect my ability to carry out my employment with Infosys as set forth in my offer of employment. I agree that in the event that Infosys finds at any time that any such information given by me is not correct, true or complete in all respects, Infosys shall have the right to initiate appropriate legal action against me for the breach of this declaration and recover the costs of such legal actions including all damages and attorneys' fees. Infosys may also, at its discretion and to the fullest extent permitted by applicable law, initiate appropriate disciplinary action against me, including termination of my employment without provision of any notice period or payment of compensation.

I acknowledge that Infosys may, at any time and at its discretion, conduct all appropriate background checks to verify the accuracy and completeness of such information, including but not limited to an independent verification and validation of all information that I have provided. I hereby authorize, without reservation, Infosys or any agent or representative thereof to independently verify and validate all such information provided by me.

This authorization and release, in original, faxed or photocopied form, shall be valid for this and any future reports and updates that may be requested.

Name : **Sheng Lu**
E-Mail: **foretribe@gmail.com**

Time stamp: **8/23/2022 12:19:19 PM**
IP address: True-Client-IP ->'220.158.191.49' :: HTTP_X_FORWARDED_FOR ->'220.158.191.49,

5. Declaration of being relieved

The Vice President – HRD

Infosys Limited

Electronic City

Bangalore - 560 100

Dear HR Manager,

I wish to state that as of today, I am employed only with Infosys Limited. I also state that I have fully disclosed the information regarding whether I am on the Board of Directors, Partner or employee or hold any office in any Company or body corporate, whether organized for profit or not, other than Infosys Ltd. I have fulfilled all my commitments to my previous employer. I am also aware that any pending issues with my previous employer and consequences arising thereof will be resolved by me directly, and Infosys will not be held responsible at any stage.

Name : **Sheng Lu**
E-Mail: **foretribe@gmail.com**

Time stamp: **8/23/2022 12:19:24 PM**
IP address: True-Client-IP ->'220.158.191.49' :: HTTP_X_FORWARDED_FOR ->'220.158.191.49,

6. Declaration of having completed educational requirements

The Vice President – HRD
Infosys Limited Electronics City
Bangalore – 560 100

Dear HR Manager,

- ✓ I wish to state that as of today, I have fully completed my graduation / postgraduation and have completed all studies, course requirements and examinations required for the award of the educational qualification recorded by me in my application for employment with Infosys. Furthermore, I confirm that I have been declared as passed in all qualifying examinations by competent examination authority.

- ☐ I wish to state that as of today, I have fully completed the course requirements and examinations required for the award of the educational qualification recorded by me in my application for employment with Infosys. However, the results of my final examination have not been declared by my university college. I undertake to notify the results of my final examination to Infosys within ……weeks from today. I fully accept responsibility for collecting this information from my university and submitting all the mark sheets and the provisional certificate within the said period to the company. In case of any delay, I undertake to obtain written permission from the company for the same.

I agree that the company may initiate appropriate legal action against me for the breach of this declaration and recover the costs of such legal actions including all damages and attorneys' fees. The company may also, at its discretion, terminate my employment with the company.

Name : **Sheng Lu**
E-Mail: **foretribe@gmail.com**

Time stamp: **8/23/2022 12:19:59 PM**
IP address: True-Client-IP ->'220.158.191.49' :: HTTP_X_FORWARDED_FOR ->'220.158.191.49,

7. Employee Code of Conduct and Ethics

1. PREAMBLE

This Code of Conduct is intended to establish and clarify the standards for behaviour in the organisation. However, no Code of Conduct can cover all situations you may encounter. Thus, you need to utilise the following principles where specific rules cannot be established:

- Decisions made, and actions taken, by you must be consistent with company values and company objectives.
- Infosys is focused on delivering long-term value to its employees, shareholders and society. It is expected that you will do what is right to support the long-term goals of the company.
- Infosys competes to win, but only within the framework of integrity, transparency and compliance with all applicable laws and regulations.
- If you are ever in doubt about a decision, it should be escalated to a higher level of management for broader consideration.
- Should you ever see a deviation from the above principles, it is expected that you will utilise appropriate channels to report the violation.

2. INTRODUCTION

This Code of Conduct and Ethics (—Code‖) helps maintain the standards of business conduct of INFOSYS LIMITED, together with its subsidiaries (—Infosys‖ or the —Company‖), and ensures compliance with legal requirements, including with (i) Section 406 of the SarbanesOxley Act of 2002 and the U.S. Securities and Exchange Commission (—SEC‖) rules promulgated thereunder (ii) Clause 49 of the Listing Agreement entered into with the National Stock Exchange of India and the Bombay Stock Exchange, and (iii) Rule 5610 of the Nasdaq Global Select Market.

This Code is designed to deter wrongdoing and promote, among other things, (a) honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships, (b) full, fair, accurate, timely and understandable disclosure in reports and documents we file with or submit to the SEC and in our other public communications, (c) compliance with applicable laws, rules and regulations, (d) the prompt internal reporting of violations of this Code, and (e) accountability for adherence to this Code. All directors, officers, employees and trainees of the Company are expected to read and understand this Code, uphold these standards in day-to-day activities, comply with all applicable policies and procedures, and ensure that all agents, contractors, representatives, consultants, or other third parties working on behalf of the Company (collectively referred to as —third party agents‖) are aware of, understand and adhere to these standards.

Since the principles described in this Code are general in nature, the Code does not cover every situation that may arise. Please use common sense and good judgment in applying this Code. You should also check the Company policies, procedures and employees handbook as adopted at the location where you are posted for specific instructions.

Nothing in this Code, or in any company policy and procedures or in other related communications (verbal or written) shall constitute and shall not be construed to constitute a contract of employment for a definite term or a guarantee of confirmed employment. This Code supersedes all other such codes, policies, procedures, instructions, practices, rules or written or verbal representations to the extent that they are inconsistent.

The Company is committed to continuously reviewing and updating its policies and procedures. Therefore, the Company reserves the right to amend, alter or terminate this Code at any time and for any reason, subject to applicable law.

Please sign the acknowledgment form at the end of this Code and return the form to the Human Resources Department indicating that you have received, read, understand and agree to comply with its terms. The signed acknowledgement form will be saved and archived as part of your e-docket. You will be asked to sign an acknowledgment indicating your continued understanding of the Code once a year.

3. COMPLIANCE IS EVERYONE'S BUSINESS

Ethical business conduct is critical to our business and it is your responsibility to respect and adhere to these practices. Many of these practices reflect legal or regulatory requirements. Violations of these laws and regulations can create significant liability for you, the Company, its directors, officers, and other employees. You should be alert to possible violations and report them in the manner set forth under the relevant section of this Code. You must cooperate in any internal or external investigations of possible violations. In all cases, if you are unsure about the appropriateness of an event or action, please seek assistance in the manner set forth under the relevant section of this Code. Those who violate the policies in this Code will be subject to disciplinary action, up to and including termination from the Company.

Part of your job and ethical responsibility is to help enforce this Code of Business Conduct and Ethics. You should be alert to possible violations and report possible violations to the Human Resources Department or the Legal Department. You must cooperate in any internal or external investigations of possible violations. Reprisal, threats, retribution or retaliation against any person who has in good faith reported a violation or a suspected violation of law, this Code of Business Conduct or other Company policies, or against any person who is assisting in any investigation or process with respect to such a violation, is prohibited.

No adverse action will be taken against anyone for complaining about, reporting, participating or assisting in the investigation of a suspected violation of this Code, unless the allegation made or information provided is found to be wilfully and intentionally false. To the maximum extent possible, the Company will maintain utmost the confidentiality in respect of all the complaints received by it.

This Code is also available on Company’s website.

4. YOUR RESPONSIBILITIES TO THE COMPANY

4.1 General Standards of Conduct

The Company expects you to exercise good judgment to ensure the safety and welfare of Infoscions and to maintain a cooperative, efficient, positive, harmonious and productive work environment and business conduct. These standards apply while working on our premises, at offsite locations where our business is being conducted, at Company-sponsored business and social events, or at any other place where you are a representative of the Company. In addition, on client locations, you may be required to adhere to the clients’ code of conduct as well.

4.1.1 Honest and Ethical conduct

We expect you to act in accordance with the highest standards of personal and professional integrity, honesty and ethical conduct, while working on the Company's premises, at offsite locations where the Company's business is being conducted, at Company sponsored business and social events, or at any other place where you are representing the Company.

We consider honest conduct to be conduct that is free from fraud or deception. We consider ethical conduct to be conduct conforming to accepted professional standards of conduct. Ethical conduct includes the ethical handling of actual or apparent conflicts of interest between personal and professional relationships. This is discussed in more detail later in this Code.

4.1.2 Equal Opportunity Workplace free of Discrimination or Harassment

The Company is committed to providing a work environment free of discrimination and harassment. The Company is an equal opportunity employer and makes employment decisions based on merit and business needs. The Company policy prohibits harassment of any kind, including harassment based on pregnancy, childbirth or related medical conditions, race, religious creed, color, sex, national origin or ancestry, physical or mental disability, medical condition, marital status, age, sexual orientation, or any other basis protected by federal, state, or local law or ordinance or regulation. All such harassment is unlawful. The Company's anti-discrimination and anti-harassment policy applies to all persons involved in the operation of the Company and prohibits harassment by any employee of the Company towards other Infosys employees including supervisors, outside vendors, and clients. It also prohibits discrimination or harassment based on the perception that anyone has any of those characteristics, or is associated with a person who has or is perceived as having any of those characteristics.

The Company believes in equal work opportunities for all employees and does not condone favoritism or the appearance of favoritism at the workplace. If you believe that you have been discriminated against, harassed or not given equal opportunities at work, submit a complaint to your supervisor or the Human Resources Department as soon as possible after the incident. You may also report your complaint to the committee responsible for addressing grievances against harassment called HEAR (Hear Employees And Resolve) by sending an email to HEAR@infosys.com. Further, if you believe you have been sexually harassed, you can submit a complaint to the Grievance Redressal Body of the Company by sending an email to GRB@infosys.com . If you have any questions, relating to what constitutes discrimination or harassment, or if you have any other questions or concerns pertaining to discrimination or harassment, please refer to the Policy on Prevention and Redressal of Harassment at Infosys.

4.1.3 Safety at the Workplace

The safety of people at the workplace is a primary concern of the Company. Each of us must comply with all applicable health and safety policies. We are subject to compliance with all local laws to help maintain secure and healthy work surroundings. Please go through the safety instructions published on the Company intranet from time to time and contact your Unit HR representative for any clarifications.

4.1.4 Dress Code

Since each of us is a representative of the Company, we must pay attention to personal grooming and adhere to the recommended dress code. Employees are expected to dress neatly and in a manner consistent with the nature of the work performed. Please follow the Company's Dress Code policy made available on the intranet.

When visiting or working on a client site, employees must adhere to the dress code maintained at that particular customer site.

4.1.5 Drug, Alcohol and Weapons Abuse

To meet our responsibilities to employees, customers and investors, the Company must maintain a healthy and productive work environment. Substance abuse, or selling, manufacturing, distributing, possessing, using or being under the influence of illegal drugs and alcohol while at work is absolutely prohibited.

The possession and/or use of weapons/firearms or ammunition on Company premises or while conducting the business of the Company is strictly prohibited, except with the prior permission of the Company. Possession of a weapon can be authorized only for security personnel when this possession is determined necessary to secure the safety and security of Company's staff and employees. The provision of written permission by the Company, however, is not meant to be an indication that the Company claims any responsibility or liability for a person's possession and/or use of a weapon/firearm or ammunition and does not authorize the person to possess and/or use such weapon/firearm or ammunition on the Company's behalf. In addition to obtaining written permission from the Company, any person in possession of a weapon/firearm or ammunition on Company premises, is solely responsible for obtaining, and must have and maintain, any and all licenses/permissions that are required by applicable laws and regulations in the relevant jurisdiction. The person in possession of the weapons/firearms or ammunition maintains sole responsibility for ensuring that their possession and/or use of such weapons/firearms or ammunition is in conformance with all such laws and regulations.

4.1.6 Solicitation and Distribution of Literature

In order to ensure efficient operation of the Company's business and to prevent disruption to employees, the Company has established a protocol on solicitations and distribution of literature at the Company premises. No employee shall solicit or promote support for any cause or organization during his or her working time or during the working time of the employee or employees at whom such activity is directed. No employee shall distribute or circulate any written or printed material in work areas during his or her working time or during the working time of the employee or employees at whom such activity is directed. Under no circumstances will non-employees be permitted to solicit or to distribute written material for any purpose at the Company premises.

4.2 Conflicts of Interest

Your decisions and actions in the course of your employment with the Company should be based on the best interests of the Company, and not based on personal relationships or benefits. Each of us has a responsibility to the Company and its stakeholders. Although this duty does not prevent us from engaging in personal transactions and investments, it does demand that we avoid situations where a conflict of interest might occur or appear to occur or your ability to exercise independent judgment in the Company's best interest is

compromised. The Company is subject to scrutiny from many different individuals and organizations. We should always strive to avoid even the appearance of impropriety.

You must avoid situations involving actual or potential conflict of interest. Personal or romantic involvement with a competitor, supplier, or subordinate employee of the company, which impairs a person's ability to exercise good judgment on behalf of the Company, creates an actual or potential conflict of interest. Personal relationships and romantic liaisons in Supervisor-subordinate reporting structures may lead to team management challenges, possible claims of sexual harassment and reduced morale.

An employee involved in any of the types of relationships or situations described in this policy should immediately and fully disclose the relevant circumstances to his or her immediate supervisor, or any other appropriate supervisor, for a determination about whether a potential or actual conflict exists. If an actual or potential conflict is determined, the Company may take whatever corrective action appears appropriate according to the circumstances. Failure to disclose facts shall constitute grounds for disciplinary action, up to and including termination.

What constitutes conflict of interest? A conflict of interest exists where the interests or benefits of one person or entity conflict with the interests or benefits of the Company. It would be impractical to attempt to list all possible situations in which a conflict of interest may arise, but some common examples include:

4.2.1 Outside Employment

In consideration of your employment with the Company, you are expected to devote your full attention to the business interests of the Company. You are prohibited from engaging in any activity that interferes with your performance or responsibilities to the Company or is otherwise in conflict with or prejudicial to the Company. Our policies prohibit any employee from accepting simultaneous employment with any other company or business entity or from taking part in any activity that enhances or supports a competitor's position. This prohibition includes performing services as a director, employee, agent or contractor for a customer, a supplier or any other entity that has a business relationship with the Company, except as approved by the Company. Additionally, you must disclose to the Company any interest that you have that may conflict with the business of the Company. If you have any questions on this requirement, you should contact your Unit HR representative.

4.2.2 Outside Directorships

Directors: Executive directors may, with the prior consent of the Chairperson of the Board of Directors, serve on the boards of two other business entities, provided that such business entities are not in direct competition with our business operations. Executive directors are also allowed to serve on the boards of corporate or government bodies whose interests are germane to the future of the software business, or are key economic institutions of the nation, or whose prime objective is benefitting society. Independent directors are not expected to serve on the boards of competing companies.

Executive Officers: Members of the Executive Council (who are not members of the board of Infosys Technologies Limited) may, with the prior approval of the Chairperson of the Board and the Company’s Chief Executive Officer and Managing Director, serve on the board of one

other company, provided that such a company is not in direct competition with our business operations.

Employees: It is a conflict of interest for employees to serve as a director of any company that competes with the Company. Our policy requires that you obtain approval from the Company's Chief Executive Officer and Managing Director before accepting a directorship. For obtaining such approvals, please send your requests to Complianceandethics@infosys.com. Approvals are subject to compliance with the terms and conditions of specified actions and tasks.

4.2.3 Business Interests

If you are considering an investment that will lead to acquiring or holding a controlling stake in another company, you must disclose such facts to and seek the approval of the Company's Audit Committee. For the purpose of this Code, the term ―controlling stake‖ shall be generally understood to mean an investment by virtue of which you acquire 2% or more of the total equity/ common stock of a company OR are reasonably likely to be able to (i) receive a seat on a company's board of directors, (ii) influence the composition of the board of directors of a company, or (iii) control the management or policy decisions of a company. You should also not have a financial interest—including an indirect interest through, for example, a relative or significant other—in any organization if that interest would give you or appear to give you a conflict of interest with the Company. You should be particularly sensitive to financial interests in competitors, suppliers, customers, distributors and strategic partners. Questions in this regard should be directed toComplianceandethics@infosys.com.

4.2.4 Related Parties

As a general rule, you should avoid conducting Company business with a relative, or with a business in which a relative is associated in any significant role. Relatives include spouse, siblings, children, parents, grandparents, grandchildren, aunts, uncles, nieces, nephews, cousins, step relationships, and in-laws.

If such a related party transaction is unavoidable, you must fully disclose the nature of the related party transaction to the Company's Chief Financial Officer through Complianceandethics@infosys.com. If determined to be material to the Company by the Chief Financial Officer, the Company's Audit Committee must review and approve in writing in advance such related party transactions. The most significant related party transactions, particularly those involving the Company's directors or executive officers, must be reviewed and approved in writing in advance, by the Company's Audit Committee. The Company must report all such material related party transactions under applicable accounting rules, SEBI rules and regulations, Indian Companies Act, U.S. Federal securities laws, SEC rules and regulations, and the securities market rules. Any dealings with a related party must be conducted at arm's-length and with no preferential treatment.

The Company discourages the employment of relatives in positions or assignments within the same department and prohibits the employment of such individuals in positions that have a financial or other dependence or influence (e.g., an auditing or control relationship, or a supervisor/subordinate relationship). The purpose of this policy is to prevent the organizational impairment and conflicts that are a likely outcome of the employment of relatives or significant others, especially in a supervisor/subordinate relationship. If a

question arises about whether a relationship is covered by this policy, the Human Resources Department is responsible for determining whether an acknowledged relationship is covered by this policy and the decision. The Human Resources Department shall advise all affected persons of this policy. Wilful withholding of information regarding a prohibited relationship/reporting arrangement will be subject to corrective action, up to and including termination. If a prohibited relationship exists or develops between two employees, the employee in the senior position must bring this to the attention of his/her supervisor. The Company retains the prerogative to separate the individuals at the earliest possible time, either by reassignment or by termination, if necessary.

4.2.5 Other Situations

Since the situations for other conflicts of interest are wide and many, it would be impractical to attempt to list all possible situations. If a proposed transaction or situation raises any questions or doubts, you should consult the Legal Department at Complianceandethics@infosys.com or your Unit HR representative.

4.3 Applicable laws.

You must comply with all applicable laws, regulations, rules and regulatory orders. Further, you must acquire appropriate knowledge of the requirements relating to your duties sufficient to enable you to recognize potential dangers and to know when to seek advice from the Legal Department on specific Company policies and procedures. Violations of laws, regulations, rules and orders may subject you to individual criminal or civil liability, in addition to discipline by the Company, up to and including termination. Such individual violations may also subject the Company to civil or criminal liability or the loss of business or reputation. If compliance with the Code should ever conflict with applicable law, you must comply with the law.

4.3.1 Obligations under Securities Laws and Prohibition against Insider Trading

Obligations under the Indian and U.S. securities laws apply to everyone as the Company is listed both on the Indian and U.S. stock exchanges. In the normal course of business, you may have access to ―material‖ non-public Company information. Material non-public information is information about a company that is not known to the general public and that a typical investor would consider making a decision to buy, sell or hold securities.

Under applicable securities laws, it is unlawful for a person who has material non-public information about a Company to trade in the stock or other securities of the Company or to disclose such information to others who may trade. This information is the property of the Company – you have been entrusted with it. You have a duty to safeguard the confidentiality of all information obtained in the course of your work at the Company and should not use your position or knowledge of the Company to gain personal benefit or provide benefit to any third party and you may not profit from it by buying or selling securities yourself. Further, you are not to tip others (by way of making recommendations for purchase, sale or retention of the securities of the Company) to enable them to profit or for them to profit on your behalf. The purpose of this policy is both to inform you of your legal responsibilities and to make clear to you that the misuse of sensitive information is contrary to Company policy and applicable Indian and U.S. securities laws.

Insider trading is a crime, penalized by fines and imprisonment for individuals. In addition, regulatory authorities may seek the imposition of civil penalties on the profits made or losses avoided from the trading. Insider traders must also disgorge any profits made and they may also be subjected to an injunction against future violations. Finally, insider traders may be subjected to civil liability in private lawsuits.

Insider trading rules are strictly enforced, even in instances when the financial transactions seem small. The Company has imposed a trading blackout period on members of the Board of Directors, executive officers and all employees and they are not to trade in Company securities during the blackout period.

For more details, you should read the Company's Insider Trading Rules, paying particular attention to the specific policies and the potential criminal and civil liability and/or disciplinary action for insider trading violations. You should comply with the Company's Insider Trading Rules, follow the pre-clearance procedures for trading and trade only when the trading window is open.

Any person who violates this Policy will also be subject to disciplinary action by the Company, which may include termination of employment or of business relationship. All questions regarding the Company's Insider Trading Rules should be directed to the Legal Department at Complianceandethics@infosys.com.

4.3.2 Prohibition against Short Selling of Company Securities

No Company director, officer, employee or third party agent may, directly or indirectly, sell any equity security, including derivatives, of the Company if he or she (1) does not own the security sold, or (2) if he or she owns the security, does not deliver it against such sale (a "short sale ") within the applicable settlement cycle. No Company director, officer, employee or third party agent may engage in short sales.

4.3.3 Export Controls

A number of countries maintain controls on the destinations to which products or software may be exported. Some of the strictest export controls are maintained by the United States. The U.S. regulations are complex and apply both to exports from the United States and to exports of products from other countries, when those products contain U.S.-origin components or technology. Even if duplicated and packaged abroad, software created in the United States may be subject to these regulations. In some circumstances, an oral presentation containing technical data made to foreign nationals in the United States may constitute a controlled export. When working with U.S. based customers, U.S. export control compliance is the responsibility of the customer. Early on in any engagement with U.S.-based customers, all employees should exercise due diligence to determine this responsibility.

4.3.4 Free and Fair Competition

Most countries have well-developed bodies of law designed to encourage and protect free and fair market competition by regulating anti-competitive conduct. Substance and practice of competition law varies from jurisdiction to jurisdiction. The Company is committed to obeying both the letter and spirit of these laws. The consequences of not doing so can be severe for all of us.

The purpose of competition laws is to protect the competitive process which is detrimental to the consumers. Competition laws also protect companies from predatory or unfair acts by dominant companies. These laws often regulate the Company's relationships with its distributors, resellers, dealers, and customers. Competition laws generally address the following areas: pricing practices (including price discrimination), discounting, terms of sale, credit terms, promotional allowances, secret rebates, exclusive dealerships or distributorships, product bundling, restrictions on carrying competing products, termination, and many other practices.

Competition laws also govern, usually quite strictly, relationships between the Company and its competitors. As a general rule, communications with competitors should always avoid subjects such as prices or other terms and conditions of sale, customers, and suppliers. You should not knowingly make false or misleading statements regarding its competitors or the products of its competitors, customers or suppliers. Participating with competitors in a trade association or in a standards creation body is acceptable when the association has been properly established, has a legitimate purpose, and has limited its activities to that purpose.

No director, officer, employee or third party agent may at any time or under any circumstances enter into an agreement or understanding, written or oral, express or implied, with any competitor concerning prices, discounts, other terms or conditions of sale, profits or profit margins, costs, allocation of product or geographic markets, allocation of customers, limitations on production, boycotts of customers or suppliers, or bids or the intent to bid or even discuss or exchange information on these subjects. In some cases, legitimate joint ventures with competitors may permit exceptions to these rules as may bona fide purchases from or sales to competitors on non-competitive products, but the Company's Legal Department must review all such proposed ventures in advance. These prohibitions are absolute and strict observance is required. Collusion among competitors is illegal, and the consequences of a violation are severe.

Although the spirit of these laws, known as "antitrust," "competition," or "consumer protection" or unfair competition laws is straightforward, their application to particular situations can be complex. Violation of some of the provisions of the competition laws can lead to fines and imprisonment for the individuals involved and to even heavier fines for the Company. To ensure that the Company complies fully with these laws, each of us should have a basic knowledge of the applicable laws and guidelines and should involve our Legal Department early on when questionable situations arise.

4.3.5 Industrial Espionage

It is the Company's policy to compete in the market place with a complete understanding and adherence to the laws of the land. This commitment to fairness includes respecting the rights of our competitors and abiding by all applicable laws. The purpose of this policy is to maintain the Company's reputation as a lawful competitor and to help ensure the integrity of the competitive marketplace. The Company expects its competitors to respect our rights to compete lawfully in the marketplace, and we must respect their rights equally. You should not appropriate or unlawfully use the information, material, products, intellectual property, or proprietary or confidential information of anyone including suppliers, customers, business partners or competitors.

4.4 Financial Reporting and Accounting Requirements; Anti-Corruption Policy; Governmental Relations

4.4.1 Financial Reporting and Accounting Requirements

As a public company, we are required to follow strict accounting principles and standards, to report financial information accurately and completely in accordance with these principles and standards, and to have appropriate internal controls and procedures to ensure that our accounting and financial reporting complies with applicable law. The integrity of our financial transactions and records is critical to the operation of our business and is a key factor in maintaining the confidence and trust of our employees, security holders and other stakeholders.

4.4.1.1 Compliance with Rules, Controls and Procedures

It is important that all transactions are properly recorded, classified and summarized in our financial statements, books and records in accordance with our policies, controls and procedures, as well as all generally accepted accounting principles, standards, laws, rules and regulations for accounting and financial reporting. If you have responsibility for or any involvement in financial reporting or accounting, you should have an appropriate understanding of, and you should seek in good faith to adhere to, relevant accounting and financial reporting principles, standards, laws, rules and regulations and the company's financial and accounting policies, controls and procedures. If you are a senior officer, you should seek to ensure that the internal controls and procedures in your business area are in place, understood and followed.

4.4.1.2 Accuracy of Records and Reports

It is important that those who rely on records and reports—managers and other decision makers, creditors, customers and auditors—have complete, accurate and timely information. False, misleading or incomplete information undermines the company's ability to make good decisions about resources, employees and programs and may, in some cases, result in violations of law. Anyone involved in preparing financial or accounting records or reports, including financial statements and schedules, must be diligent in assuring that those records and reports are complete, accurate and timely. Anyone representing or certifying as to the accuracy of such records and reports should make an inquiry or review adequate to establish a good faith belief in their accuracy.

Even if you are not directly involved in financial reporting or accounting, you are likely involved with financial records or reports of some kind—a voucher, time sheet, invoice or expense report. In addition, most employees have involvement with product, marketing or administrative activities, or performance evaluations, which can affect our reported financial condition or results. Therefore, the Company expects you, regardless of whether you are otherwise required to be familiar with finance or accounting matters, to use all reasonable efforts to ensure that every business record or report with which you deal is accurate, complete and reliable.

4.4.1.3 Intentional Misconduct You may not intentionally misrepresent the Company's financial performance or otherwise intentionally compromise the integrity of the Company's reports, records, policies and procedures. For example, you may not:

- report information or enter information in the Company's books, records or reports that fraudulently or intentionally hides, misrepresents or disguises the true nature of any financial or non-financial transaction or result;
- establish any undisclosed or unrecorded fund, account, asset or liability for any improper purpose;
- enter into any transaction or agreement that accelerates, postpones or otherwise manipulates the accurate and timely recording of revenues or expenses;
- intentionally misclassify transactions as to accounts, business units or accounting periods; or
- Knowingly assist others in any of the above.

4.4.1.4 Dealing with Auditors

Our auditors have a duty to review our records in a fair and accurate manner. You are expected to cooperate with independent and internal auditors in good faith and in accordance with law. In addition, you must not fraudulently induce or influence, coerce, manipulate or mislead our independent or internal auditors regarding financial records, processes, controls or procedures or other matters relevant to their engagement. You may not engage, directly or indirectly, any outside auditors to perform any audit, audit-related, tax or other services, including consulting, without written approval from the Chief Financial Officer and the Audit Committee of the Board of Directors.

4.4.1.5 Obligation to Investigate and Report Potential Violations You should make appropriate inquiries in the event you may see, for example:

- financial results that seem inconsistent with underlying business performance;
- inaccurate financial records, including travel and expense reports, time sheets or invoices;
- the circumventing of mandated review and approval procedures;
- transactions that appear inconsistent with good business economics;
- the absence or weakness of processes or controls; or
- persons within the company seeking to improperly influence the work of our financial or accounting personnel, or our external or internal auditors.

Dishonest or inaccurate reporting can lead to civil or even criminal liability for you and the company and can lead to a loss of public faith in the Company. You are required to promptly report any case of suspected financial or operational misrepresentation or impropriety.

4.4.1.6 Keeping the Audit Committee Informed The Audit Committee plays an important role in ensuring the integrity of our public reports. If you believe that questionable accounting or auditing conduct or practices have occurred or are occurring, you should notify the Audit Committee of the Board of Directors. In particular, the Chief Executive Officer and senior financial officers such as the Chief Financial Officer and the Controller should promptly bring to the attention of the Audit Committee any information of which he or she may become aware concerning, for example:

- the accuracy of material disclosures made by the Company in its public filings;
- material weaknesses or significant deficiencies in internal control over financial reporting;
- any evidence of fraud that involves an employee who has a significant role in the Company's financial reporting, disclosures or internal controls or procedures; or
- any evidence of a material violation of the policies in this Code regarding financial reporting.

4.4.1.7 Disclosure to the Regulators and the Public

Our policy is to provide full, fair, accurate, timely, and clear disclosures in reports and documents that we file with, or submit to, the SEC, SEBI, stock exchanges and in our other public communications. Accordingly, you must ensure that you comply with our disclosure controls and procedures, and our internal control over financial reporting.

4.4.1.8 Expense Claims

All business related expense claims must be authorized by the manager of the employee before the incurrence. Personal expense will not be reimbursed by the Company. To know the individual business expenditure limit, please refer to the applicable policies given on the Company's intranet.

4.4.2 Anti-Corruption Policy

The Company's reputation for honesty, integrity and fair dealing is an invaluable component of the Company's financial success, and of the personal satisfaction of its employees. Among the several anti-corruption legislations worldwide, the most important legislation that is relevant to the Company, its directors, employees and third party agents is the U.S. Foreign Corrupt Practices Act, known as the FCPA.

The Company lists its ADSs on a U.S. stock exchange and is therefore subject to the FCPA. In addition, certain shareholders, directors and/or employees of Infosys are U.S. persons and thus, individually, subject to the FCPA. The Company is committed to compliance with all relevant anti-corruption legislation, including the FCPA (as if it were to be a US Incorporated Company), and the Bribery Act 2010 (U.K.) and the Prevention of Corruption Act, 1988 (India).

The FCPA has two major components: (1) the anti-bribery prohibitions; and (2) the accounting and recordkeeping requirements. Both components apply to the Company's business activities conducted in the U.S. and abroad. The FCPA anti-bribery prohibitions disallow a company or its employee or representative from giving, paying, promising, offering, or authorizing the payment, directly or indirectly through a third party, anything of value to any ―government official‖ (a broad term whose scope is discussed below) to persuade that official to help the company, or any other person, obtain or keep business. The FCPA bars payments even if: (1) the benefit is for someone other than the party making the payment; (2) the business sought is not with the government; (3) the payment does not work and no business is awarded; or (4) the government official initially suggested the payment.

The FCPA also requires the company to keep accurate and complete records in its books of accounts of the financial transactions in which it engages. The company must make goodfaith efforts to ensure that the ventures in which it owns a minority interest and the third party agents it engages also maintains such records in that party's books of accounts.

Compliance with the FCPA must be undertaken on a case-by-case basis and can be complex. Employees should not try to solve FCPA problems on their own. If a question arises regarding any improper payment related issue, please write to Complianceandethics@infosys.com.

4.4.2.1 Prohibition of Bribery Infosys strictly prohibits bribery in any form. As outlined above, the FCPA's anti-bribery provisions render illegal any corrupt offer, payment, promise to pay, or authorization to pay any money, gift, or anything of value to any government official for the purpose of:

- influencing any act or decision of the government official in his official capacity; inducing the government official to do or omit to do any act in violation of his lawful duty; securing any improper advantage; or
- Inducing the government official to influence a decision of a governmental authority,in order to obtain or retain business or to direct business to anyone.
- For the purpose of this Policy, the term —government official‖ includes:
- a public official, whether foreign or domestic;
- This includes all paid, full-time employees of a government department or agency (whether in the executive, legislative or judicial branches of government and whether at the national, provincial, state or local level). Government officials can also include part-time workers, unpaid workers, individuals who do not have an office in a government facility, and anyone acting under a delegation of authority from a government to carry out government responsibilities. This also includes officers and employees of companies or entities that have government ownership or control, such as state-owned enterprises and government-controlled universities and hospitals.
- a candidate or official of a political party, whether foreign or domestic;
- a representative of an organization wholly-owned or majority-controlled by a government, whether foreign or domestic; or
- an employee of a public international organization.

The term —anything of value‖ as used in this Policy may include cash payments, gifts, entertainment, excessive business promotional activities, covering or reimbursing expenses of government officials, in kind or political contributions, investment opportunities, shares, securities, loans or contractual rights, promise of future employment, payments under consulting agreements, subcontracts, stock options, and similar items of value provided to government officials.

Under the U.K. Bribery Act, a person is guilty of the offence of bribery if he/ she, whether directly or through a third party, offers, promises or gives a financial or other advantage to another person with the intent to induce or reward the improper performance of a function or activity. In some cases, the acceptance of the advantage would itself constitute the improper performance of a function or activity. The recipient need not be in public office or the public sector for the bribe to constitute an offence. Thus, the U.K. Bribery Act prohibits bribery in both the public and private sectors.

Under the Prevention of Corruption Act, 1988, bribery of governmental officials and agents, whether directly or indirectly, is strictly prohibited.

Anti-corruption legislation in your home jurisdiction, which is likely to include similar restrictions, must be followed.

4.4.2.2 Expenses Incurred on Government Officials

The FCPA permits companies to provide certain types of entertainment and travel to government officials provided that such entertainment and travel expenses are: (a) bona fide and related to a legitimate business purpose (i.e., not provided to obtain or retain business or to gain an improper advantage); (b) reasonable in amount; and (c) legal under the written laws of the government official’s home country.

Accordingly, no payments shall be made to or on behalf of a government official, whether directly or indirectly, in connection with efforts to obtain or retain business, except for

reasonable and bona fide payments (such as travel and lodging expenses) that are directly related to the:

- Promotion, demonstration or explanation of products or services of Infosys; or
- Execution or performance of a contract between Infosys and a governmental authority.

Prior to incurring any expenses for government officials, employees shall ensure that reimbursement of such expenses is permissible under applicable local laws and relevant client policies. All such expenses shall be fairly and accurately reflected in Infosys' books of accounts.

While making a claim for reimbursement through iClaim or iTravel, Employees shall be required to mention if the expenditure was incurred towards the travel, entertainment or meals of government officials.

No per-diem may be paid in cash to government officials. In addition, Infosys prohibits any expenditure, or any amount, in support of travel, entertainment or otherwise in support of the family of a government official.

Even if the expenditure is permitted under local law, prior written approval must be obtained from the CFO for local meals and entertainment that otherwise adhere to the above-described requirements but have a value exceeding US$100 (or its equivalent) per person. Please send your requests to Complianceandethics@infosys.com for obtaining such written approvals. In situations where pre-approval is impractical or impossible, the event should be reported to the CFO through Complianceandethics@infosys.com with all the relevant details.

4.4.2.3 Gifts

In connection with certain holidays and other occasions, it is customary in many parts of the world to give nominal gifts to customers, government officials and other parties that have a business relationship with the Company. Generally, a nominal gift can be made by a Company director, officer or employee to a government official without violating the FCPA if: (a) the giving of the gift does not meet the elements of an FCPA violation (i.e., the gift is not given to obtain or retain business or gain an improper advantage); (b) the gift is lawful under the laws of the country where the gift is being given; (c) the gift constitutes a bona fide promotion or goodwill expenditure; (d) the gift is not in the form of cash; (e) the gift is of nominal value (on an individual and aggregate basis); and (f) the gift is accurately recorded in the Company's books and records.

While no dollar amount is specified under the FCPA, in general, no gift with a value of more than US$100 (or its equivalent) should be given by an employee or third party agent to a government official without prior review and written approval by the CFO. For obtaining the relevant approvals, please send your requests to Complianceandethics@infosys.com. For gifts with a value of US$100 (or its equivalent) or less, you must obtain prior written permission from your supervisor. In the case of a third party agent, prior written permission must be obtained from the supervisor in charge of the relationship with the third party agent. No approval is required for providing Infosys promotional or advertising items with a value of less than US$50 (or its equivalent), such as pens or coffee mugs, as long as such activity does not otherwise violate any relevant laws or regulations. The number and value of items given, however, must be reasonable and the gift must otherwise abide by the above-described requirements.

Prior to giving any gifts to government officials, employees shall ensure that such gifting is permissible under applicable local laws and relevant client policies. Employees must ensure that any such gifts carry the Infosys logo and are suited for official use. All such gifts or payments shall be fairly and accurately reflected in Infosys' books of accounts.

4.4.2.4 Charitable Contributions

Infosys believes that charitable contributions and donations are an integral part of its corporate social responsibility. Typical areas for granting support are education and research, social welfare, disaster relief and other similar social causes. Charitable contributions and donations shall be made without demand or expectation of business return.

Before making a charitable contribution on behalf of Infosys, the credentials of the recipient must be verified and it must be ensured that such contributions are permissible under applicable local laws and that specific prior approval is received from the Board of Directors. For obtaining such approvals, please send your requests to Complianceandethics@infosys.com. Beneficiaries of any such charitable contributions should not be related to the directors or executive officers of Infosys, to avoid an appearance of impropriety. Relatives include spouse, siblings, children, parents, grandparents, grandchildren, aunts, uncles, nieces, nephews, cousins, step relationships, and in-laws.

No charitable contributions shall be made in cash or to the private account of an individual. Any amounts contributed or donations made towards charitable causes shall be fairly and accurately reflected in Infosys' books of accounts.

4.4.2.5 Political Contributions

Infosys reserves the right to communicate its position on important issues to the elected representatives and other government officials. It is Infosys' policy to comply fully with all local, state, federal, foreign and other applicable laws, rules and regulations regarding political contributions. Infosys' funds or assets must not be used as contribution for political campaigns or political practices under any circumstances without the prior written approval of the Board of Directors. For obtaining such approvals, please send your requests to Complianceandethics@infosys.com.

4.4.2.6 Transacting with Intermediaries

The FCPA establishes liability for payments made directly to an official as well as payments made indirectly. Employees must therefore endeavour, to the extent reasonably practicable, to directly interact with government officials.

However, in case intermediaries or third party agents are required to interface with government authorities on behalf of Infosys, employees must verify the credentials and reputation of such intermediary or third party agent prior to negotiating a business relationship and must also ensure that a contract formalizing the terms of the appointment is duly executed. All contracts with third party agents working on behalf of the Company must contain appropriate provisions requiring the third party agent to comply with the FCPA and a copy of this Policy must be provided to such third party agents.

Employees should be particularly alert to any ―red flags‖ that may be encountered during verification of or in transactions with third party agents. ―Red flags‖ that do not present serious issues at one stage of a transaction or relationship may pose significant liability risks

when they appear at a different stage or in combination with a different overall set of facts. All ―red flags‖ must immediately be investigated and appropriately addressed. The following are some illustrations of ―red flags‖ that frequently arise with third parties:

- A reference check reveals a third party agent's flawed background or reputation;
- The transaction involves a country known for corrupt payments;
- The third party agent is suggested by a government official, particularly one with discretionary authority over the business at issue;
- The third party agent objects to FCPA representations in Company agreements;
- The third party agent has a close personal or family relationship, or a business relationship, with a government official or relative of an official;
- The third party agent requests unusual contract terms or payment arrangements that raise local law issues, such as payment in cash or payment in another country's currency;
- The third party agent requires that his or her identity or, if the third party agent is a company, the identity of the company's owners, principals or employees, not be disclosed;
- The third party agent's commission exceeds the ―going rate‖ or must be paid in cash;
- The third party agent indicates that a particular amount of money is needed in order to "get the business" or "make the necessary arrangements";
- The third party agent requests that the Company prepare or accept false invoices or any other type of false documentation; or
- The third party agent requests payment in a third country (i.e., not where the services are rendered, or where the third party agent resides), or to an account in another party's name.

The Company and individual directors, officers or employees may be liable for a payment made by a third party agent, if the Company makes a payment or transfers other value to that third party agent ―knowing‖ that it will be given to a government official. Under the FCPA, firm belief that the third party agent will pass through all or part of the value received from the Company to a government official, or an awareness of facts that create a ―high probability‖ of such a pass-through, also constitute knowledge under this law.

Employees must therefore ensure that the fee, commission or other remuneration paid to intermediaries or third party agents is reasonable, bona fide and commensurate with the functions and services performed. Any such expenses shall be fairly and accurately reflected in Infosys' books of accounts.

4.4.2.7 Record Retention.

All records relating to FCPA compliance matters shall be maintained for a minimum of eight (8) years, and diligent efforts should be used to maintain original documents.

4.4.3 Governmental Relations

It is the Company's policy to comply fully with all applicable laws and regulations governing contact and dealings with government employees and public officials, and to adhere to high ethical, moral and legal standards of business conduct. This policy includes strict compliance with all local, state, federal, foreign and other applicable laws, rules and regulations. If you have any questions concerning government relations, contact the Company's Legal Department at Complianceandethics@infosys.com.

4.4.3.1 Lobbying

Employees or third party agents whose work requires lobbying communication with any member or employee of a legislative body or with any government official or employee in the formulation of legislation must have prior written approval of such activity from the CFO. For obtaining such approvals, please send your requests to Complianceandethics@infosys.com. Activity covered by this policy includes meetings with legislators or members of their staff or with senior government officials. Preparation, research, and other background activities that are done in support of lobbying communication are also covered by this policy even if the communication ultimately is not made.

4.4.3.2 Government Contracts

It is the Company's policy to comply fully with all applicable laws and regulations that apply to government contracting. It is also necessary to adhere to all terms and conditions of any contract with local, state, federal, foreign or other applicable governments compulsorily. The Company's Legal Department must review and approve all contracts with any government entity. No contract or agreement may be made with any business in which a government official or employee holds a significant interest, without the prior approval of the Company's Legal Department.

4.5 Protecting the Company's Confidential Information

The Company's confidential information is a valuable asset. The Company’s confidential information includes product architectures; source codes; product plans and road maps; proprietary and technical information, such as trade secrets and inventions; names and lists of customers, dealers, and employees; financial information and projections; non-public information about customers, suppliers and others; and much of its internal data. This information is the property of the Company and may be protected by patent, trademark, copyright and trade secret laws. All confidential information must be used for Company business purposes only. Every director, officer, employee and third party agent must safeguard it. This responsibility includes, not disclosing the Company confidential information such as information regarding the Company's services or business, over the internet. You are also responsible for properly labelling any and all documentation shared with or correspondence sent to the Company's Legal Department or outside counsel as "Attorney-Client Privileged". This responsibility includes the safeguarding, securing and proper disposal of confidential information and extends to confidential information of third parties, which is detailed elsewhere in this Code.

4.5.1 Proprietary Information and Invention Agreement

When you joined the Company, you signed an agreement to protect and hold confidential the Company's proprietary information. This agreement remains in effect for as long as you work for the Company and after you leave the Company. Under this agreement, you may not disclose the Company's confidential information to anyone or use it to benefit anyone other than the Company without the prior written consent of an authorized Company officer.

4.5.2 Disclosure of Company Confidential Information

To further the Company's business, from time to time, confidential information may be disclosed to potential business partners based on context and appropriateness. However, such disclosure should never be done without carefully considering its potential benefits and risks. If you determine in consultation with your manager and other appropriate Company

management that disclosure of confidential information is necessary, you must then contact the Legal Department to ensure that an appropriate written nondisclosure agreement is signed prior to the disclosure. The Company has standard nondisclosure agreements suitable for most disclosures. You must not sign a third party's nondisclosure agreement or accept changes to the Company's standard nondisclosure agreements without review and approval by the Company's Legal Department. In addition, all Company materials that contain Company confidential information, including presentations, must be reviewed and approved by your manager and other appropriate Company management prior to publication or use. Furthermore, any employee opinion as published content or publicly made statement that might be perceived or construed as attributable to the Company, made outside the scope of his or her employment with the Company, must be reviewed and approved in writing in advance by your manager and other appropriate Company management. This must include the Company's standard disclaimer that the publication or statement represents the views of the specific author and not of the Company.

4.5.3 Requests by Regulatory Authorities

The Company and its directors, officers, employees or third party agents must cooperate with appropriate government inquiries and investigations. In this context, however, it is important to protect the legal rights of the Company with respect to its confidential information. All government requests for information, documents or investigative interviews must be referred to the Company's Legal Department at Complianceandethics@infosys.com. No financial information may be disclosed without the prior approval of the Chief Financial Officer.

4.5.4 Company Spokespeople

The Corporate Communication and Analyst Policy has been established to set out who in the Company may communicate information to the press and the financial analyst community. All inquiries or calls from the press and financial analysts should be referred to the Investor Relations Department. The Company has designated its Chief Executive Officer, Chief Operating Officer, Chief Financial Officer and Investor Relations Department as official Company spokespeople for financial matters. All press releases, interviews, media replies should be pre-cleared by the Legal Department. The Company has designated its Public Relations Team as its official Company spokespeople for marketing, technical and other such information. These designees are the only people who may communicate with the press on behalf of the Company. It is critical that no one responds to any inquiries themselves because any inappropriate or inaccurate response, even a denial or disclaimer of information, may result in adverse publicity and could otherwise gravely affect the Company’s legal position.

4.6 Use of Company's Assets and Corporate Opportunities

Protecting the Company's assets is a key responsibility of every director, officer, employee and third party agent. Care should be taken to ensure that assets are not misappropriated, loaned to others, or sold or donated, without appropriate authorization. You are responsible for the proper use of Company assets, and must safeguard such assets against loss, damage, misuse or theft. Persons who violate any aspect of this policy or who demonstrate poor judgment in the manner in which they use any Company asset may be subject to disciplinary action, up to and including termination of employment or business relationship at the Company's sole discretion. Company equipment and assets are to be used for Company

business purposes only. You must not use Company assets for personal use, nor may they allow any other person to use Company assets. If you have any questions regarding this policy, please contact your Unit HR representative.

4.6.1 Company Brand and Logo

Infosys® is a registered trademark of the Company in India and/or the United States and it should be conspicuously marked with the ® designation or with a notation that it is a registered trademark of the Company whenever it is first used in any medium, presentation or other promotional context. For information on other trademarks of the Company and their correct usage, please refer to the Company's website and intranet. You may also contact the Corporate Marketing Department in this regard.

4.6.2 Physical Access Control

The Company has and will continue to develop procedures covering physical access control to ensure privacy of communications, maintenance of the security of the Company communication equipment, and safeguard Company assets from theft, misuse and destruction. You are personally responsible for complying with the level of access control that has been implemented in the facility where you work on a permanent or temporary basis. You must not defeat or cause to be defeated the purpose for which the access control was implemented. For more details please read the Company's Information Security Policy.

4.6.3 Company Funds

All Company employees are personally responsible for all Company funds over which they exercise control. Third party agents should not be allowed to exercise control over Company funds. Company funds must be used only for Company business purposes and not for any personal purpose. All Company employees and third party agents must take reasonable steps to ensure that the Company receives good value for Company funds spent, and must maintain accurate and timely records of every expense. Expense reports must be accurate and submitted in a timely manner.

4.6.4 Computers and Other Equipment

The Company strives to furnish employees with the equipment necessary to perform their duties efficiently and effectively. You must use the equipment responsibly and use it only for Company business purposes. If you use Company equipment at your home or off site, take precautions to protect it from theft or damage, just as if it were your own. Prior to leaving the services of the Company, you must immediately return all Company equipment. While computers and other electronic devices are made accessible to employees to assist them to perform their jobs and to promote the Company's interests, all such computers and electronic devices, must remain fully accessible to the Company and, to the maximum extent permitted by law, will remain the sole and exclusive property of the Company.

You should not maintain any expectation of privacy with respect to information transmitted over, received by, or stored in any electronic communications device owned, leased, or operated in whole or in part by or on behalf of the Company. To the extent permitted by applicable law, the Company retains the right to gain access to any information received by, transmitted by, or stored in any such electronic communications device, by and through its employees and third party agents at any time, either with or without an employee's or third

party's knowledge, consent or approval. For more details please read the Company's Information Security Policy, Email Usage Policy, Internet Access Policy, and the Bulletin Board Usage Policy.

4.6.5 Software

All software used by employees to conduct Company business must be appropriately licensed. Never make or use illegal or unauthorized copies of any software, whether in the office, at home, or on the road, since doing so may constitute copyright infringement and may expose you and the Company to potential civil and criminal liability. In addition, use of illegal or unauthorized copies of software may subject the employee to disciplinary action, up to and including termination. The Company's Computers and Communication Department will inspect Company computers periodically to verify that only approved and licensed software has been installed. Any non-licensed/supported software will be removed. For more details, please read the Company's Information Security Policy, Email Usage Policy, IT Infrastructure Acceptable Usage Policy and Internet Access Policy, and the Bulletin Board Usage Policy.

4.6.6 Electronic Usage

Employees must utilize electronic communication devices in a legal, ethical, and appropriate manner. This policy addresses the Company's responsibilities and concerns regarding the fair and proper use of all electronic communications devices within the organization, including computers, e-mail, connections to the Internet, intranet and extranet and any other public or private networks, voice mail, video conferencing, facsimiles, and telephones. Posting or discussing information concerning the Company's services or business on the Internet without the prior written consent of the Company's Legal Department is prohibited. Any other form of electronic communication used by employees currently or in the future is also intended to be encompassed under this policy. It is not possible to identify every standard and rule applicable to the use of electronic communications devices. Employees are therefore encouraged to use sound judgment whenever using any feature of our communications systems. For more details please read the Company's Information Security Policy, Email Usage Policy, IT Infrastructure Acceptable Usage Policy and Internet Access Policy, Bulletin Board Usage Policy.

4.6.7 Corporate Opportunities

You may not exploit opportunities that are discovered through the use of corporate property, information or position for your own personal gain unless the opportunity is disclosed fully in writing to the Company's Board of Directors and the Board of Directors declines to pursue the said opportunity.

4.7 Maintaining and Managing Records

The purpose of this policy is to set forth and convey the Company's business and legal requirements in managing records, including all recorded information regardless of the medium or its characteristics. Records include paper documents, CDs, computer hard disks, email, floppy disks, microfiche, microfilm or all other media. The Company is required by local, state, federal, foreign and other applicable laws, rules and regulations to retain certain records and to follow specific guidelines in managing its records. Civil and criminal penalties for failure to comply with such guidelines can be severe for the Company and its directors, officers, employees and third party agents and failure to comply with such guidelines may

subject the employee or third party agent to disciplinary action, up to and including termination of employment or business relationship.

4.7.1 Records on Legal Hold

A legal hold suspends all document destruction procedures in order to preserve appropriate records under special circumstances, such as litigation or government investigations. The Company's Legal Department determines and identifies what types of Company records or documents are required to be placed under a legal hold. Every Company director, officer, employee and third party agent must comply with this policy.

The Company's Legal Department will notify you if a legal hold is placed on records for which you are responsible. You then must preserve and protect the necessary records in accordance with instructions from the Company's Legal Department. Records or supporting documents that have been placed under a legal hold must not be destroyed, altered or modified under any circumstances. A legal hold remains effective until it is officially released in writing by the Company's Legal Department. If you are unsure whether a document has been placed under a legal hold, you should preserve and protect that document while you check with the Company's Legal Department. If you have any questions about this policy, contact the Company's Legal Department.

5 RESPONSIBILITIES TO OUR CUSTOMERS AND OUR SUPPLIERS

5.1 Customer Relationships

If your job requires interfacing or contacting any Company customers or potential customers, it is critical to remember that you represent the Company to the people with whom you are dealing. Act in a manner that creates value for our customers and help build a relationship based upon trust. The Company and its employees have provided services for many years and have built up significant goodwill over the years. This goodwill is one of our most important assets, and you must act to preserve and enhance our reputation.

5.2 Payments or Gifts from Others

Under no circumstances may employees or third party agents accept any offer, payment, promise to pay, or authorization to pay any money, gift, or anything of value from customers, suppliers, vendors, consultants, etc. that is perceived as intended, directly or indirectly, to influence any business decision, any act or failure to act, any commitment of fraud, or opportunity for the commission of any fraud. Inexpensive gifts, infrequent business meals, celebratory events and entertainment, provided that they are not excessive or create an appearance of impropriety, may not violate this policy. Before accepting anything of value from an employee of a government entity, please contact Complianceandethics@infosys.com.

5.3 Publications and Copyrights

The Company subscribes to many publications that aid employees to perform their duties better. These include newsletters, reference material, online reference services, magazines, books, and other digital and printed works. Copyright law generally protects these works, and their unauthorized copying and distribution constitute copyright infringement. You must first obtain the consent of the publisher of a publication before copying publications or significant

parts of them. When in doubt about whether you may copy a publication, consult the Company's Legal Department.

5.4 Handling Confidential Information of Others

The Company has many kinds of business relationships with many companies and individuals. Sometimes, they will volunteer confidential information about their products or business plans to induce the Company to enter into a business relationship. At other times, we may request that a third party provide confidential information to permit the Company to evaluate a potential business relationship with that party. Whatever the situation, we must take special care to handle the confidential information of others responsibly. We handle such confidential information in accordance with our agreements with such third parties.

Appropriate Nondisclosure Agreements. Confidential information may take many forms. An oral presentation about a company's product development plans may contain protected trade secrets. A customer list or employee list may be a protected trade secret. A demo of an alpha version of a company's new software may contain information protected by trade secret and copyright laws.

You should never accept information offered by a third party that is represented as confidential, or which appears from the context or circumstances to be confidential, unless an appropriate nondisclosure agreement has been signed with the party offering the information. The Legal Department can provide nondisclosure agreements to fit any particular situation, and will coordinate appropriate execution of such agreements on behalf of the Company. Even after a nondisclosure agreement is in place, you should accept only the information necessary to accomplish the purpose of receiving it, such as a decision on whether to proceed to negotiate a deal. If more detailed or extensive confidential information is offered and it is not necessary, for your immediate purposes, it should be refused.

Need-to-Know. Once a third party's confidential information has been disclosed to the Company, we have an obligation to abide by the terms of the relevant nondisclosure agreement and limit its use to the specific purpose for which it was disclosed and to disseminate it only to other Company employees with a need to know the information. Every director, officer, employee and third party agent involved in a potential business relationship with a third party must understand and strictly observe the restrictions on the use and handling of confidential information. When in doubt, consult the Company's Legal Department.

Notes and Reports. When reviewing the confidential information of a third party under a nondisclosure agreement, it is natural to take notes or prepare reports summarizing the results of the review and, based partly on those notes or reports, to draw conclusions about the suitability of a business relationship. Notes or reports, however, can include confidential information disclosed by the other party and so should be retained only long enough to complete the evaluation of the potential business relationship. Subsequently, they should be either destroyed or turned over to your manager or other appropriate company management for safekeeping or destruction. They should be treated just as any other disclosure of confidential information is treated: marked as confidential and distributed only to those the Company employees with a need to know.

Competitive Information. You should never attempt to obtain a competitor's confidential information by improper means, and you should especially never contact a competitor regarding their confidential information. While the Company may, and does, employ former employees of competitors, we recognize and respect the obligations of those employees not to use or disclose the confidential information of their former employers.

5.5 Selecting Suppliers

The Company's suppliers make significant contributions to our success. To create an environment where our suppliers have an incentive to work with the Company, they must be confident that they will be treated lawfully and in an ethical manner. The Company's policy is to purchase supplies based on need, quality, service, price and terms and conditions. The Company's policy is to select significant suppliers or enter into significant supplier agreements though a competitive bid process where possible. Under no circumstances should any Company director, officer, employee or third party agent attempt to coerce suppliers in any way. The confidential information of a supplier is entitled to the same protection as that of any other third party and must not be received before an appropriate nondisclosure agreement has been signed. In some cases where the products or services have been designed, fabricated, or developed to our specifications the agreement between the parties may contain restrictions on sales.

6 REPORTING VIOLATIONS

Violations of law, this Code or other Company policies or procedures by Company employees can lead to disciplinary action up to and including termination. Disciplinary actions may include immediate termination of employment at the Company’s sole discretion. Where the Company has suffered a loss, it may pursue legal actions against the individuals or entities responsible. Where laws have been violated, the Company will cooperate fully with the appropriate authorities.

6.1 Whistleblower cases

If you find or have concerns related to: (i) questionable accounting, accounting controls, auditing matters, or reporting of fraudulent financial information to our shareholders, government or the financial markets; or (ii) grave misconduct, i.e., conduct which results in a violation of law by the Company or in a substantial mismanagement of Company resources which if proven, would constitute a criminal offence or reasonable grounds for dismissal of the person engaging in such conduct; or (iii) conduct which is otherwise in violation of any law, you should promptly contact your immediate supervisor or the corporate counsel, in accordance with the Company’s Whistleblower Policy.

You may also report your concerns anonymously by sending an e-mail to whistleblower@infosys.com or by sending an anonymous letter to the corporate counsel. If you have reason to believe that both of those individuals are involved in the matter you wish to report, you should report those facts to the Audit Committee of the Company’s Board of Directors. For more details, you should read the Company’s Whistleblower Policy available on the Infosys intranet.

6.2 Other cases

Other violations that do not fall within the scope of the Whistleblower Policy or any other section detailed in this Code, must be reported in the manner set forth under the relevant section of this Code to:

- your Unit HR representative; or
- Legal Department at Complianceandethics@infosys.com

6.3 Prohibition against Retaliation

Reprisal, threats, retribution or retaliation against any person who has in good faith reported a violation or a suspected violation of law, this Code or other Company policies, or against any person who is assisting in any investigation or process with respect to such a violation, is prohibited.

7 WAIVERS

A waiver of any provision of this Code must be approved in the manner provided below, unless a separate procedure is specified under any existing corporate policy of the Company:

For a director or executive officer: A waiver must be approved in writing by the Company's Board of Directors and promptly disclosed.

For employees or third party agents: A waiver must be approved in writing by the CEO, COO or the CFO.

For obtaining such approvals, please send your request to Complianceandethics@infosys.com.

8 DISCIPLINARY ACTIONS

The matters covered in this Code are of the utmost importance to the Company, its stockholders and its business partners, and are essential to the Company's ability to conduct its business in accordance with its stated values. We expect all of our directors, officers, employees and third party agents to adhere to these rules in carrying out their duties for the Company.

The Company will take appropriate action against any person whose actions are found to violate these policies or any other policies of the Company. Disciplinary actions may include immediate termination of employment or business relationship at the Company's sole discretion. Where the Company has suffered a loss, it may pursue legal actions against the individuals or entities responsible. Where laws have been violated, the Company will cooperate fully with the appropriate authorities. You should review all the Company's policies and procedures on the Company intranet for more detailed information.

9 MODIFICATIONS

We are committed to continuously reviewing and updating our policies and procedures. Therefore, this Code is subject to modification. Any amendment or waiver of any provision of this Code must be approved in writing by the Company's Board of Directors and promptly disclosed on the Company's website and in applicable regulatory filings pursuant to applicable laws and regulations, together with details about the nature of the amendment or waiver.

10 ACKNOWLEDGMENT OF RECEIPT OF CODE OF CONDUCT AND ETHICS

I read the Company's Code of Conduct and Ethics. I understand the standards and policies contained in the Company Code of Conduct and Ethics and understand that there may be additional policies or laws specific to my job. I further agree to comply with the Company Code of Conduct and Ethics.

If I have questions concerning the meaning or application of the Company Code of Conduct and Ethics, any Company policies, or the legal and regulatory requirements applicable to my job, I know I can consult my manager, the Human Resources Department or the Legal Department, knowing that my questions or reports to these sources will be maintained in confidence.

The Code of Conduct is an Infosys Generic Policy which is applicable worldwide. Applicable local law and regulation will prevail over the policy.

Name : **Sheng Lu**
E-Mail: **foretribe@gmail.com**

Time stamp: **8/23/2022 12:18:53 PM**
IP address: True-Client-IP ->'220.158.191.49' :: HTTP_X_FORWARDED_FOR ->'220.158.191.49,

8. Fair Work Information Statement

From 1 January 2010, this Fair Work Information Statement is to be provided to all new employees by their employer as soon as possible after the commencement of employment. The Statement provides basic information on matters that will affect your employment. If you require further information, you can contact the Fair Work Infoline on 13 13 94 or visit www.fairwork.gov.au.

The National Employment Standards

The Fair Work Act 2009 provides you with a safety net of minimum terms and conditions of employment through the National Employment Standards (NES).

There are 10 minimum workplace entitlements in the NES:

1. A maximum standard working week of 38 hours for full-time employees, plus 'reasonable' additional hours.
2. A right to request flexible working arrangements.
3. Parental and adoption leave of 12 months (unpaid), with a right to request an additional 12 months.
4. Four weeks paid annual leave each year (pro rata).
5. Ten days paid personal/carer's leave each year (pro rata), two days paid compassionate leave for each permissible occasion, and two days unpaid carer's leave for each permissible occasion.

6. Community service leave for jury service or activities dealing with certain emergencies or natural disasters. This leave is unpaid except for jury service.
7. Long service leave.
8. Public holidays and the entitlement to be paid for ordinary hours on those days.
9. Notice of termination and redundancy pay.
10. The right for new employees to receive the Fair Work Information Statement.

A complete copy of the NES can be accessed at www.fairwork.gov.au. Please note that some conditions or limitations may apply to your entitlement to the NES. For instance, there are some exclusions for casual employees.

If you work for an employer who sells or transfers their business to a new owner, some of your NES entitlements may carry over to the new employer. Some NES entitlements which may carry over include personal/carer's leave, parental leave, and your right to request flexible working arrangements.

Right to request flexible working arrangements

Requests for flexible working arrangements form part of the NES. You may request a change in your working arrangements, including changes in hours, patterns or location of work from your employer if you require flexibility because you:

• are the parent, or have responsibility for the care, of a child who is of school age or younger
• are a carer (within the meaning of the Carer Recognition Act 2010)
• have a disability
• are 55 or older
• are experiencing violence from a member of your family or
• provide care or support to a member of your immediate family or household, who requires care or support because they are experiencing violence from their family.

If you are a parent of a child or have responsibility for the care of a child and are returning to work after taking parental or adoption leave you may request to return to work on a part-time basis to help you care for the child.

Modern awards

In addition to the NES, you may be covered by a modern award. These awards cover an industry or occupation and provide additional enforceable minimum employment standards. There is also a Miscellaneous Award that may cover employees who are not covered by any other modern award.

Modern awards may contain terms about minimum wages, penalty rates, types of employment, flexible working arrangements, hours of work, rest breaks, classifications, allowances, leave and leave loading, superannuation, and procedures for consultation, representation, and dispute settlement. They may also contain terms about industry specific redundancy entitlements.

If you are a manager or a high income employee, the modern award that covers your industry or occupation may not apply to you. For example, where your employer guarantees in writing

that you will earn more than the high income threshold, currently set at $138,900 per annum and indexed annually, a modern award will not apply, but the NES will.

Agreement making

You may be involved in an enterprise bargaining process where your employer, you or your representative (such as a union or other bargaining representative) negotiate for an enterprise agreement. Once approved by the Fair Work Commission, an enterprise agreement is enforceable and provides for changes in the terms and conditions of employment that apply at your workplace. There are specific rules relating to the enterprise bargaining process. These rules are about negotiation, voting, matters that can and cannot be included in an enterprise agreement, and how the agreement can be approved by the Fair Work Commission. You and your employer have the right to be represented by a bargaining representative and must bargain in good faith when negotiating an enterprise agreement. There are also strict rules for taking industrial action. For information about making, varying, or terminating enterprise agreements visit the Fair Work Commission website, www.fwc.gov.au.

Individual flexibility arrangements

Your modern award or enterprise agreement must include a flexibility term. This term allows you and your employer to agree to an Individual Flexibility Arrangement (IFA), which varies the effect of certain terms of your modern award or enterprise agreement. IFAs are designed to meet the needs of both you and your employer. You cannot be forced to make an IFA, however, if you choose to make an IFA, you must be better off overall. IFAs are to be in writing, and if you are under 18 years of age, your IFA must also be signed by your parent or guardian.

Freedom of association and workplace rights (general protections)

The law not only provides you with rights, it ensures you can enforce them. It is unlawful for your employer to take adverse action against you because you have a workplace right. Adverse action could include dismissing you, refusing to employ you, negatively altering your position, or treating you differently for discriminatory reasons. Some of your workplace rights include the right to freedom of association (including the right to become or not to become a member of a union), and the right to be free from unlawful discrimination, undue influence and pressure. If you have experienced adverse action by your employer, you can seek assistance from the Fair Work Ombudsman or the Fair Work Commission (applications relating to general protections where you have been dismissed must be lodged with the Fair Work Commission within 21 days).

Termination of employment

Termination of employment can occur for a number of reasons, including redundancy, resignation and dismissal. When your employment relationship ends, you are entitled to receive any outstanding employment entitlements. This may include outstanding wages, payment in lieu of notice, payment for accrued annual leave and long service leave, and any applicable redundancy payments. Your employer should not dismiss you in a manner that is 'harsh, unjust or unreasonable'. If this occurs, this may constitute unfair dismissal and you may be eligible to make an application to the Fair Work Commission for assistance. It is important to note that applications must be lodged within 21 days of dismissal. Special

provisions apply to small businesses, including the Small Business Fair Dismissal Code. For further information on this code, please visit www.fairwork.gov.au.

Right of entry

Right of entry refers to the rights and obligations of permit holders (generally a union official) to enter work premises. A permit holder must have a valid and current entry permit from the Fair Work Commission and, generally, must provide 24 hours notice of their intention to enter the premises. Entry may be for discussion purposes, or to investigate suspected contraventions of workplace laws that affect a member of the permit holder's organisation or occupational health and safety matters. A permit holder can inspect or copy certain documents, however, strict privacy restrictions apply to the permit holder, their organisation, and your employer.

The Fair Work Ombudsman and the Fair Work Commission

The Fair Work Ombudsman is an independent statutory agency created under the Fair Work Act 2009 , and is responsible for promoting harmonious, productive and cooperative Australian workplaces. The Fair Work Ombudsman educates employers and employees about workplace rights and obligations to ensure compliance with workplace laws. Where appropriate, the Fair Work Ombudsman will commence proceedings against employers, employees, and/or their representatives who breach workplace laws. If you require further information from the Fair Work Ombudsman, you can contact the Fair Work Infoline on 13 13 94 or visit www.fairwork.gov.au. The Fair Work Commission is the national workplace relations tribunal established under the Fair Work Act 2009 . The Fair Work Commission is an independent body with the authority to carry out a range of functions relating to the safety net of minimum wages and employment conditions, enterprise bargaining, industrial action, dispute resolution, termination of employment, and other workplace matters. If you require further information, you can visit the Fair Work Commission website, www.fwc.gov.au.

Name : Sheng Lu
E-Mail: foretribe@gmail.com

9. Policy on Confidential and Proprietary information owned by previous employer/s

At Infosys, you are not to improperly use or disclose any proprietary information or trade secrets of your former employer/s. Moreover, you are not to bring onto company premises any unpublished documents or property belonging to your previous employer/s unless it has explicitly consented in writing to your doing so. In short, you are not to bring any third party confidential information to Infosys and you are not to utilize any such information in any way while you perform your duties for Infosys.

With regard to your non-solicitation/no service obligations, we ask that you ensure that you are familiar with the particulars of your obligations to your previous employer/s. While Infosys certainly has questions regarding the enforceability of these provisions under law in different countries, in an effort to avoid any unnecessary disputes with your previous employer/s, we encourage you to adhere to those obligations.

To that end, if any member, officer or employee contacts you regarding employment opportunities at Infosys, we ask that you not discuss employment with that person without first directing that person to the attention of Human Resources. At that point, Human Resources will handle the employment/recruitment process, and you will be involved only to the extent the company believes that it is appropriate to do so.

Nanjappa Bottolanda Somanna

Head – Employee Relations

Name : **Sheng Lu**
E-Mail: **foretribe@gmail.com**

Time stamp: **8/23/2022 12:18:59 PM**
IP address: True-Client-IP ->'220.158.191.49' :: HTTP_X_FORWARDED_FOR ->'220.158.191.49,

10. Whistleblower policy

The Purpose of this Policy

Infosys Limited ("Infosys") and its subsidiaries (collectively the "Company") are committed to complying with the foreign and domestic laws that apply to them, satisfying the Company's Code of Conduct and Ethics, and particularly to assuring that business is conducted with integrity and that the Company's financial information is accurate. If potential violations of Company policies or applicable laws are not recognized and addressed promptly, both the Company and those working for or with the Company could face governmental investigation, prosecution, fines, and other penalties. That can be costly. Consequentially, and to promote the highest ethical standards, the Company will maintain a workplace that facilitates the reporting of potential violations of Company policies and applicable laws. Employees must be able to raise concerns regarding such potential violations easily and free of any fear of retaliation. That is the purpose of this policy (the "Policy" or the "Whistleblower Policy"). You are required to read this Policy and submit the attached certification that you will comply with it.

Your Duty to Report

Everyone is required to report to the Company any suspected violation of any law that applies to the Company and any suspected violation of the Company's Code of Conduct and Ethics. It is important that you report all suspected violations. This includes possible accounting or financial reporting violations, insider trading, bribery, or violations of the anti-retaliation aspects of this Policy. Consult the Company's Code of Conduct and Ethics for a more detailed description of potential violations and other areas of particular concern. Retaliation includes adverse actions, harassment, or discrimination in your employment relating to your reporting of a suspected violation.

It is the policy of the Company that you must, when you reasonably suspect that a violation of an applicable law or the Company's Code of Conduct and Ethics has occurred or is occurring, report that potential violation. Reporting is crucial for early detection, proper investigation and remediation, and deterrence of violations of Company policies or applicable laws. You should not fear any negative consequences for reporting reasonably suspected violations because retaliation for reporting suspected violations is strictly prohibited by Company policy. Failure to report any reasonable belief that a violation has occurred or is occurring is itself a violation of this Policy and such failure will be addressed with appropriate disciplinary action, including possible termination of employment.

How to Report

You must report all suspected violations to (i) your immediate supervisor; (ii) the Chief Compliance Officer; at complianceoffice@infosys.com or (iii) anonymously, by sending an e-mail to: whistleblower@infosys.com
If you have reason to believe that your immediate supervisor or the Chief Compliance Officer is involved in the suspected violation, your report may be made to the Audit Committee of Infosys' Board of Directors (the
"Audit Committee") at:

Chairperson, Audit Committee

Infosys Limited

44 Electronics City

Hosur Road

Bangalore - 560100

Because you have several means of reporting, you need never report to someone you believe may be involved in the suspected violation or from whom you would fear retaliation.

Your report should include as much information about the suspected violation as you can provide. Where possible, it should describe the nature of the suspected violation; the identities of persons involved in the suspected violation; a description of documents that relate to the suspected violation; and the time frame during which the suspected violation occurred. Where you have not reported anonymously, you may be contacted for further information.

Investigations after You Report

All reports under this Policy will be promptly and appropriately investigated, and all information disclosed during the course of the investigation will remain confidential, except as necessary to conduct the investigation and take any remedial action, in accordance with applicable law. Everyone working for or with the Company has a duty to cooperate in the investigation of reports of violations. Failure to cooperate in an investigation, or deliberately providing false information during an investigation, can be the basis for disciplinary action, including termination of employment. If, at the conclusion of its investigation, the Company determines that a violation has occurred, the Company will take effective remedial action commensurate with the nature of the offense. This action may include disciplinary action against the accused party, up to and including termination. Reasonable and necessary steps will also be taken to prevent any further violations of Company policy.

Retaliation is not Tolerated

No one may take any adverse action against any employee for complaining about, reporting, or participating or assisting in the investigation of, a reasonably suspected violation of any law, this Policy, or the Company's Code of Conduct and Ethics. The Company takes reports of such retaliation seriously. Incidents of retaliation against any employee reporting a violation or participating in the investigation of a reasonably suspected violation will result in appropriate disciplinary action against anyone responsible, including possible termination of employment. Those working for or with the Company who engage in retaliation against reporting employees may also be subject to civil, criminal and administrative penalties.

Document Retention

All documents related to reporting, investigation and enforcement pursuant to this Policy shall be kept in accordance with the Company's record retention policy and applicable law.

Modification

The Audit Committee or the Board of Directors of Infosys can modify this Policy unilaterally at any time without notice. Modification may be necessary, among other reasons, to maintain compliance with federal, state or local regulations and / or accommodate organizational changes within the Company.

This is to acknowledge that I have received a copy of the Company's Whistleblower Policy. I understand that compliance with applicable laws and the Company's Code of Conduct and Ethics is important and, as a public Company, the integrity of the financial information of the Company is paramount. I further understand that the Company is committed to a work environment free of retaliation for employees who have raised concerns regarding violations of this Policy, the Company's Code of Conduct and Ethics or any applicable laws and that the Company specifically prohibits retaliation whenever an employee makes a good faith report regarding such concerns. Accordingly, I specifically agree that to the extent that I reasonably suspect there has been a violation of applicable laws or the Company's Code of Conduct and Ethics, including any retaliation related to the reporting of such concerns, I will immediately report such conduct in accordance with the Company's Whistleblower Policy. I further agree that I will not retaliate against any employee for reporting a reasonably suspected violation in good faith.

I understand and agree that to the extent I do not use the procedures outlined in the Whistleblower Policy, the Company and its officers and directors shall have the right to presume and rely on the fact that I have no knowledge or concern of any such information or conduct.

Name : Sheng Lu
E-Mail: foretribe@gmail.com

Time stamp: 8/23/2022 12:19:01 PM
IP address: True-Client-IP ->'220.158.191.49' :: HTTP_X_FORWARDED_FOR ->'220.158.191.49,