



INDEX

Anti – Bribery & Corruption Policy	27
Sustainability Policy	33
Outside Employment Policy	35
Sanctions and Trade Controls Policy	37
Conflict of Interest Policy	44
Communication Devices & Workplace Tools Policy	53
Electronic Monitoring and Recordings Policy	58
Drug-Free Workplace Policy	59
Equal Employment Opportunity Policy	64
Anti-Harassment, Discrimination, and Retaliation Prevention Policy	66
Anti-Sexual Harassment Policy	68
Anti-Discrimination on the Basis of Gender, Gender Identity or Transgender Status Policy	71
Diversity, Equity and Inclusion Policy	73
Human Rights Policy	75
Data Protection & Privacy Policy	78
Health, Safety & Environment Policy	79
Search, Inspection & Investigation Policy	85
Compensation & Benefits	88
Internal Job Posting (“IJP”) Policy	91
Promotion Policy	93
Leave Policy	97
Global Travel Policy	104
Employee Resources	111
Whistleblower Policy	113
Enterprise Information Security Policy	122
Non-Solicitation & Non-Disparagement Policy	125
Positive Work Environment Policy	127
Privacy Policy	137

Everise Data Privacy Statement for Employees	140
Progressive Coaching Process.....	149
Employee Acceptable Use Policy.....	150
Social Media Policy.....	154
Separation and Termination Process	160
Acknowledgement of Employee Handbook.....	161



Welcome to Everise!

As an Everiser, you are now part of an award-winning, next-generation experience company! As part of a growing team, you play a crucial role in helping some of the world's leading brands transform their customers into fans and products into passions.

OUR STORY

Everise Holdings Pte. Ltd. and its wholly-owned direct and indirect subsidiaries (collectively referred to as "**Everise**", "**we**", "**us**", "**our**" or the "**company**"), was established in 2016 by founder and CEO Sudhir Agarwal, with a vision to disrupt the Business Process Outsourcing (BPO) industry by identifying companies that showed potential in transforming customer experience elements. These companies included C3|CustomerContactChannels, Trusource Labs, Hyperlab, and Globee. Together, we are Everise - a truly disruptive company that offers unique Customer Experience (CX), Digital Experience (DX), and Product Experience (PX) solutions with proven results for leading enterprises and renowned unicorns.

WE ARE EVERISE

Globally, the Everise family is 12,000 people strong across seven countries and creates more than 500,000 daily customer experiences in 20 different languages. Our domain expertise lies in making complex support simple in connected industries such as Health & Wellness, Connected Health, Smart Home, Tech & Software, Travel & Hospitality, Media & Communications, Financial Services, and Logistics & Supply Chain. This allows us to nurture innovation and deliver immersive experiences for the brands of tomorrow.

OUR PURPOSE

At Everise, we believe that to truly transform customers into fans and products into passions, and we need to start with our purpose and people. As Everisers, our purpose is to elevate the experience for our customers and fellow employees. We do this by being people-focused, celebrating diversity, incubating innovation, and accelerating your development. Ultimately, we aim to ensure that a future exists where technology is powered by people and is for the benefit of people.

OUR VALUES

We Are People-First

Be recognized for your hard work and achievement. We have a sharp eye for potential, and we reward our people through recognition programs, performance awards, and celebrations. We ensure a supportive work environment with initiatives that push personal growth and career advancement.



We Incubate Innovation

Be creative and elevate yourself by working with amazing companies. Through our Experience Labs and advanced digital products, we are a globally enabled workforce focused on embracing new technologies and fresh ideas to transform how we work.

We Celebrate Diversity

Be yourself and feel at home with our multicultural team. Supporting over 20 languages in our locations, we encourage diversity at all levels through community service programs, Everise Cares initiatives and our E-Talk forums.

We Accelerate Your Growth

Everise University

As a progressive global experience company, we have developed our very own learning platform and resource. This allows our people to benefit from a large pool of knowledge that's accessible anytime.

Everise Accelerator Training

A week of instructor-led classroom training to teach Supervisors' foundational skills and ensure consistent coaching and management processes across all global sites.

Everise Career Development

We pair promising employees with department leaders who provide career coaching and skills development. This powerful mentor relationship increases your readiness for career advancement. Coming soon to more sites.

Purpose of the Employee Handbook

This employee handbook (Employee Handbook) has been written to serve as a guide for all employees of Everise working from India (Everise India) and to present an overview of the company's policies and practices in one reference source and supersedes and all prior handbooks, written documents or oral representations regarding its subject matter, other than the employment contract between you and Everise or Everise India (Employment Contract). There are several things that are important to keep in mind about this Employee Handbook. First, it contains only general information and guidelines. It is not intended to be comprehensive or to address all the possible applications of, or exceptions to, the general policies and procedures described. This Employee Handbook is not exhaustive and does not contain all the policies of Everise India. The Employee Handbook may be supplemented (including by adding additional policies), updated, revised and / or amended from time to time and it shall be your duty to check any supplements, updates, revisions, and / or amendments made to the Employee Handbook. Extraordinary issues or situations are not covered in this Employee Handbook and should these actually arise, they are to be referred to management for appropriate disposition. Irrespective of the provisions of this Employee

Handbook, the employees shall be required to comply with all laws, rules and regulations applicable to the employees of Everise India. This Employee Handbook does not in any manner limit the scope of any laws, rules and regulations applicable to the employees. References to Everise under this Employee Handbook shall mean Everise India and shall apply to the employees of Everise India. Each of the policies, regulations, rules and provisions set out under this Employee Handbook shall be read together and in conjunction with each other. Unless otherwise expressly provided in your Employment Contract, the handbook and the contract should be read together and interpreted harmoniously. In case of any conflict between: (a) any of the policies, regulations, rules and provisions of this Employee Handbook, or (b) any of the policies, regulations, rules and provisions of this Employee Handbook on the one hand and the provisions of the Employment Contract on the other hand, then the legal department of Everise ("Legal Department") shall, in each case, have the sole right to resolve such conflict and the decision taken by the Legal Department be final and binding.

If employees have any questions concerning eligibility for a particular benefit or the applicability of a policy or practice, they should address their specific questions to their supervisor or the Human Resources Department (HR). You can access a copy of the Employee Handbook on the Workday. If you are unable to access the Employee Handbook via the intranet, please seek assistance from the Human Resources Department. This Employee Handbook is deemed as a confidential company document. As such, it may be used, shared, and discussed only among employees of Everise.

This Employee Handbook and the contents herein are exclusive properties of Everise. It is prohibited to wholly or partially sell, copy, modify, reproduce, republish, transcribe, transmit, or distribute any or all of the contents of this Employee Handbook in any way, in the language in which it is written or translated, without the Everise's prior written consent.

All employees shall be furnished a copy of this Employee Handbook, the same to be acknowledged in writing and the Acknowledgment shall form part of the employee's personnel file. All provisions of this Employee Handbook shall form part of the employee's Employment Contract regardless of tenure or appointment in Everise. All employees shall be bound by the provisions of this Employee Handbook.

Our Employment Philosophy

At Everise India, it is important that employees represent professional values and principles and perform at the highest level of personal integrity. We will do our best to provide an open, honest and supportive work environment, and we ask that our employees contribute the same energy and dedication to maintaining a respectful, clean and professional workplace. Everise India pledges to treat employees fairly and in a dignified manner, providing them with a quality work environment, fair compensation, the right to be heard, and opportunities to learn and grow within our organization.

Starting Employment – Probationary Period

As a new employee, it is normal that it will take time before you are fully familiar with the people, procedures, and responsibilities of your assignment. For this reason, the first six

months of employment are considered an introductory period to allow you to acclimate to your new environment, as well as provide an opportunity for both the company and you to confirm both sides have made a good employment decision. Your performance and acclimation are monitored closely to ensure you are provided the appropriate coaching and support for a successful transition.

Completion of this introductory period does not change or alter the agreed employment relationship between you and the company. You shall continue to have the right to terminate your employment at any time, with or without cause, and the company reserves its rights to terminate your employment with just cause or in the manner set out under your Employment Contract. However, this is subjected to your probation confirmation within the stipulated time stated in your Employment Contract. You will be receiving a confirmation letter upon successful completion of your probation.

Employee Records

The company complies with applicable laws regarding access to personnel records. All employee information and records are the sole property of the company and are considered confidential. The personnel file includes records related to performance and training as well as other records used for hiring, promotion and disciplinary decisions. It will not include any reference checks, medical records or investigation files.

The Human Resources Department maintains an employment record in the HR systems for every employee. It is important that this record be up to date. Please notify your Human Resources Department of any changes in your address, telephone number, marital status, and number of dependents, educational progress, and any other data which is maintained or should be maintained in your employment records.

Only active (currently employed and working) employees may review their records by scheduling an appointment with their Human Resources Department. A representative of the Human Resources Department must be present during the review.

An employee's supervisor or manager who has an employment related need to know personal information may inspect certain documents related to an employee over whom they have supervisory responsibility.

Managers are not permitted to remove any documents from the employee file.

Redeployment and Transfer

Subject to business needs, an employee may be released by the current program. During such instance, the account intending to release an employee from their current program should inform the Human Resources Department by including all the details of the business decision.

HR will schedule a discussion with the employee to document the release and transfer process. Once the release is effective, employee will be redeployed to other available

programs in the company. For non-working days, the employee will be unpaid up until a new program is identified and upon a successful transfer.

An Employee may be required to comply and go through the application process prior to release if the identified new program so requires.

Willful refusal to comply with the redeployment process shall be a violation of this Employee Handbook and other applicable covenants as provided in the Employment Contract.

Employee Records

- The Human Resources Department maintains an employment record in Workday for every employee. It is important that this record be up to date. Please notify your Human Resources Department of any changes in your address, telephone number, marital status, and number of dependents, educational progress, and any other data which is maintained or should be maintained in your employment records. Most of this information may be updated directly in our Human Resources Information System by utilizing employee self-service through one of our designated company computer kiosks or the Internet at: Workday.
- An employee who needs assistance using Workday should contact their supervisor or Human Resources Department.
- Only active (currently employed and working) employees may review their records by scheduling an appointment with their Human Resources Department. A representative of the Human Resources Department must be present during the review.
- An employee's supervisor or manager who has an employment related need to know personal information may inspect certain documents related to an employee over whom they have supervisory responsibility.
- Managers are not permitted to remove any documents from the employee file.

Classification of Employees

Everise employees are classified as follows:

Probationary Employee

Probationary refers to a newly hired employee. The probation period is from the date the employee started working up to the sixth month (180 days), unless otherwise stated in the Employment Contract.

Regular Employees

An employee who has completed the required probationary period and who has been satisfactorily appraised by his/her immediate supervisor and the Department Head. It also covers new employees hired as regular employees. This status carries entitlement to certain

benefits, as established in accordance with the company's policies and procedures on benefits coverage and utilization.

Everise Business Code of Conduct

Summary of the Code's Principles

Protecting the company's Assets, Resources & Data

- We often have sensitive confidential information about Everise, other companies, our clients and investors, and our directors, officers and employees; preserving the integrity of this information is vital to our business and reputation and is necessary to meet our obligations under data protection laws.
- Electronic communications relating to business activities may not be conducted through electronic communication systems that have not been specifically approved for business activities, including (among others) personal email accounts, personal text messaging, nonapproved chat forums, and social media.

Accuracy of Books & Records & Public Disclosures

- We should take care that our books and records are accurate and that all of our business transactions are properly authorized.

Duties To Stakeholders

- A company's reputation is everything and we should act responsibly in dealings with our customers, clients, investors, suppliers, other stakeholders and competitors.

Communications & Media

- In this digital era, be careful in your written communications made over company information systems, such as email, as this is a permanent record.
- You must ensure that your online activities, including your use of social media, are appropriate and reflect well on Everise.
- The Code does not prohibit an employee from engaging in such communications that are intended to address employee concerns involving terms and conditions of employment.

Conflicts of Interest & Personal Behavior

- Everise is a global brand and as a representative of the company your personal behavior must be consistent with our values.
- Be cognizant that you face a risk that your personal interests may conflict with or appear to conflict with the interests of the company.

Positive Work Environment

- We value diversity and we should all do our part to maintain a respectful work environment where everyone feels safe, included and productive.
- Our success is dependent on establishing a workplace culture free from discrimination, violence and harassment.

Compliance with Laws, Rules, Regulations & Policies

- We operate in many jurisdictions and are subject to different laws, rules and regulations; you need to be aware of the laws that apply to your activities so that you can comply with them; ignorance of the law is no excuse.
- The company has corporate policies that you must be familiar with, as they govern your activities, business practices and other conduct while at Everise.

Frequently Asked Questions

Why do we have a code?

The Code serves as a guide for how you should conduct yourself as a member of the Everise team. Preserving our corporate culture and ensuring compliance with legal and regulatory duties is vital to the organization and following the Code helps us do that.

Who must follow the Code?

The Code applies to all directors, officers, employees and temporary workers of Everise.

What are your responsibilities?

You have two responsibilities. First, you must follow every aspect of the Code and certify your commitment each year. Second, if you suspect someone may be violating the Code or the policies referred to herein, you have an obligation to report it. To make a report, follow the section of the Code: "Reporting Potential Code Violations."

How will I know if there is a problem?

The Code attempts to deal with the most common issues that you may encounter, but it cannot address every question that may arise. When you're not sure what to do, ask yourself the following questions:

- Is it illegal?
- Does it feel like the wrong thing to do?
- Would you feel uncomfortable if others knew about it?
- Will it have the potential to create a negative perception of you or the company?

- Do you have a personal interest that has the potential to conflict with the company's interest?

If you answer “yes” to any of these questions your proposed conduct may violate the Code and you should ask for help.

How Should I Ask for Help?

If you have questions about the Code, any policies or guidelines referred to herein, or about the best course of action to take in a particular situation, you should seek guidance from your supervisor or a member of the Legal Department by emailing legal@weareeverise.com.

What if I would like to make an anonymous report?

You may make an anonymous report by contacting the company's reporting hotline, which is operated by an independent third-party and is available 24 hours a day, 7 days a week ('Reporting Hotline'). The Reporting Hotline phone numbers by jurisdiction are set forth on Schedule A. If you choose to make an anonymous report, your anonymity will be protected to the fullest extent possible as permitted by law. Keep in mind, however, that maintaining your anonymity may limit the company's ability to investigate your concerns.

What are the consequences for violating the code?

Violations of the Code or the policies and guidelines incorporated by reference herein, can vary in its consequences. If you're an employee, it could result in a reprimand or other disciplinary action, including the termination of your employment with the company for cause. If you're a member of an Everise Board of Directors, a violation may necessitate your resignation. Certain violations of the Code also contravene applicable laws and therefore can have severe consequences outside of Everise. Depending on your actions, failing to comply with the Code could lead to civil or criminal prosecution, which could result in substantial fines, penalties and/or imprisonment.

Introduction

This Code of Business Conduct and Ethics (“**Code**”) applies to all directors, officers, employees and temporary workers¹ (collectively, “you” or “employee”) of Everise.

Standards of Business Conduct

Everise seeks to foster and maintain a reputation for honesty, openness, trust, integrity and professionalism. The confidence and trust placed in Everise by our clients and investors is something we value greatly and endeavor to protect. In many respects, our reputation is our

¹ For purposes of the Code, “temporary workers” include non-full-time employees and consultants and contractors etc. that work on our premises. The business group retaining a temporary worker is responsible for ensuring that the temporary worker certifies their commitment to comply with the Code.

most vital business asset. Accordingly, all our activities should be conducted with honesty and integrity and in compliance with applicable legal and regulatory requirements.

We have adopted the Code and related policies and procedures to preserve our culture and to ensure compliance with legal and regulatory requirements applicable to our activities. We expect and require that you meet the letter and spirit of the Code (and related policies and procedures). This Code incorporates by reference the following corporate policies and programs, which may be included in the Employee Handbook relevant to your jurisdiction or provided to you separately, and should be read in conjunction with the Code:

- Records Retention Policy;
- Anti-Bribery and Corruption Policy;
- Sanctions and Trade Controls Policy;
- Data Protection Policy and Data Protection Program;
- Confidentiality and Non-Disclosure Policy;
- Enterprise Information Security Policy;
- Positive Work Environment Policy; Financial Authority Matrix
- Travel and Entertainment Expense Policy; and
- Whistleblower Policy.

Protecting The company's Assets, Resources & Data

The company's assets are to be used for legitimate business purposes only.

The company's assets are for business, not personal use. The company's assets span many categories. Assets can be physical, tangible goods, such as office supplies, furniture, computers or intangible items, such as intellectual property. You have a responsibility to safeguard the company's assets from loss, damage, theft, misuse and waste. If you become aware of loss, damage, theft, misuse or waste of our assets, or have questions about your proper use of them, you should speak with your supervisor. The company's name (including its corporate letterhead and logo), facilities and relationships are valuable assets and must only be used for authorized company business.

If you use the company's assets for personal benefit or are otherwise wasteful with the company's assets, you may be in breach of your duty to the company. You have a responsibility not to abuse company resources for reimbursement. Any requests for reimbursement for authorized company expenses must be for legitimate business expenses. If you are unsure whether a certain expense is legitimate, you should speak with your supervisor or refer to the company's *Travel and Entertainment Expense Policy* in the Employee Handbook.

Confidential information must be protected at all times.

We must protect confidential information in our possession, both information about us and information about other companies and our clients and investors. Confidential information includes, but is not limited to, material non-public information, all confidential memos, notes, lists, records and other documents in your possession, in hard and soft copy. All of these are to be delivered to the company promptly after your employment ceases or at any time upon the company's request, and your obligation to protect this information continues after you leave the company. You must protect hard and soft copies of confidential information that are removed from the office (e.g., to be worked with at home or at external meetings).

It is important to use discretion when discussing company business. This includes respecting information barrier protocols and discussing company business only with those individuals at the company that have a "need to know" the information. Additionally, be careful not to discuss company business in public places such as elevators, restaurants, and public transportation or when using your phone or email outside of the office. You should also be careful not to leave confidential information in unattended conference rooms or in public places where others can access it. While employed by Everise, if you become aware of confidential information about the company or another entity that you know or suspect has been inadvertently disclosed, seek guidance from a member of the Legal Department before using or acting upon this information.

Personal data held by or on behalf of the company must be used in compliance with data protection laws.

The company collects personal data regarding individuals both inside and outside the organization where we have the lawful basis for doing so. This is necessary to effectively and efficiently administer and manage the operation of our business. Personal data includes, among other things, sensitive personal data, medical and financial information. We should take all reasonable steps to only hold personal data for as long as we have a need to retain it.

Collection and use of personal data are subject to various legal and regulatory requirements. You must take all reasonable steps to ensure that personal data is kept confidential and accessed only by those individuals at the company that need to know this information to carry out their duties. In addition, if it is necessary to the conduct of business to disclose personal data to a third-party (e.g., so that a third-party may provide services to the company or acquire an asset or business of the company) then you must ensure that such transfer complies with applicable legal and regulatory requirements. This may include ensuring the third-party is subject to a written agreement which contains confidentiality obligations and, where relevant, other obligations which must be included under the data protection laws of certain jurisdictions in which we operate or have clients or investors. In all other cases, you may only disclose personal data pursuant to a legal or regulatory requirement.

In the ordinary course, the company transfers personal data between jurisdictions in which the company operates, including the United States, Bermuda, Ireland, Guatemala, Colombia,

and the Asian Pacific Region (“APAC”). If you transfer personal data outside these areas, then you must ensure that it is permissible for you to do so (e.g., consent has been given by the individual or an appropriate data transfer agreement has been signed). In addition, you should ensure that the personal data is protected in a manner that is consistent with how personal data is protected by the company within these jurisdictions, and in any event in compliance with all applicable data protection laws.

You are responsible for ensuring that you understand and comply with our data protection/privacy policies. For more information about compliance with data protection laws, refer to the company’s *Data Protection and Privacy Policy* in the Employee Handbook.

Intellectual property belongs to the company.

During the course of your employment, you may be involved in the creation, development or invention of intellectual property such as concepts, methods, processes, inventions, confidential information and trade secrets, know-how, physical products, ideas, plans, programs, software, applications, code, works of authorship, trademarks, service marks and designs, alone or jointly with others, including but not limited to the improvement of existing intellectual property belonging to the company. All such intellectual property and the rights therein shall be owned by the company and your moral rights to such intellectual property, if any, will be waived. You are responsible for cooperating with the company and providing all necessary assistance, including the preparation and execution of any necessary documentation such as assignments and applications to register rights before relevant government authorities on behalf of the company, to ensure that all intellectual property and related rights become or are recognized as the exclusive property of the company.

The documents of the company must be preserved.

It is critical that you help preserve our business records, follow the guidelines set forth in any document retention policies and comply with related legal and regulatory requirements. If you are notified that your documents are relevant to an anticipated or pending litigation, investigation or audit, you must follow the guidance set forth in a litigation hold memorandum or any similar notice you receive from legal counsel regarding retention of documents.

Accuracy of books & records and public disclosures

Ensure that the books and records of the company are complete and accurate and that all business transactions are properly authorized.

The books and records of the company must reflect all its transactions in order to permit the preparation of accurate financial statements. Employees must never conceal information from:

- (i) an external auditor;
- (ii) an internal auditor; or

(iii) an audit committee of the company.

In addition, it is unlawful for any person to fraudulently influence, coerce, manipulate or mislead an external auditor of the company.

The company's contracts and agreements govern our business relationships. As the laws governing contracts and agreements are numerous and complicated, we have put in place policies and procedures to ensure that any contract entered into by the company has the appropriate level of approval. As a result, employees who enter into contracts or agreements on behalf of the company must have proper authorization to do so and, prior to their execution, these documents must be reviewed by legal counsel. If you are unsure whether you have proper authorization to enter into a contract on behalf of the company, consult the Chief Legal Officer.

Ensure that the company provides full, true and plain public disclosure.

All employees who are responsible for the preparation of the company's public disclosures, or who provide information as part of this process, must ensure that public disclosures of information are made honestly and accurately. Employees must be aware of and report any of the following: (a) fraud or deliberate errors in the preparation, maintenance, evaluation, review or audit of any financial statement or financial record; (b) deficiencies in, or noncompliance with, internal accounting controls; (c) misrepresentations or false statements in any public disclosure document, such as annual and quarterly reports, prospectuses, information/proxy circulars and press releases; or (d) deviations from full, true and plain reporting of the company's financial condition.

Additionally, each person who is in a financial reporting oversight role, and their family members, are prohibited from obtaining any tax or other services from the external auditor, irrespective of whether the company or such person pays for the services.

Duties to Stakeholders

Deal fairly with the company's stakeholders.

You must deal fairly with the company's customers, clients, suppliers, communities in which we operate, other stakeholders and competitors. To preserve our reputation and relationship, do not engage in any illegal or unethical conduct.

Communication & Media

Use the company's various forms of communication properly and appropriately.

All business matters that involve electronic, written communication must be conducted by employees on the company's email system or through other systems provided and approved by the company. You must always use our e-mail, Internet, telephones and other forms of communication appropriately and professionally. While we appreciate the need for limited use of these tools for personal purposes, any such use should not be excessive or detract from your work. As outlined in the summary of the Code's principles, electronic

communications relating to business activities may not be conducted through electronic communications system that have not been specifically approved for business activities, including (among others) personal email accounts, personal text messaging, non-approved chat forums and social media.

Employees should not email business information to their personal email accounts or maintain a copy of business information on their personal computers or other non-work electronic devices. When using company-provided technologies, such as computers, cell phones and voicemail, you should not expect that the information you send or receive is private. Your activity may be monitored to ensure these resources are used appropriately and are in compliance with the company's policies and laws and regulations. The Code does not prohibit an employee from engaging in such communications that are intended to address employee concerns involving terms and conditions of employment. Please refer to the *Data Protection and Privacy Policy* in the Employee Handbook.

Be cautious in your use of social media.

The company's social media policy is that, unless you are expressly authorized, you are strictly prohibited from commenting, or posting about, or otherwise discussing the company, its customers and clients, its (and its clients') investors, its employees, and its securities, investments and other business matters on all social media forums, including, but not limited to, social networks, chat rooms, wikis, virtual worlds and blogs (collectively, "social media"). You are a representative of Everise when engaging in online activities and you must ensure that your behavior online, including on social media, is appropriate and consistent with our values. For further details on the appropriate use of social media, you should refer to the Employee Handbook.

Employees must not use internet-based platforms including, but not limited to, blogs, social networking sites, chat rooms, wikis, virtual worlds, or personal websites (collectively, "social media") to disparage² the company, its associates, customers, clients, vendors, business practices, or other employees of the company. Unless you are expressly authorized, you are strictly prohibited from commenting, or posting about, or otherwise discussing information that reveals the identity of the company's clients who have engaged the company for services. We encourage you to use good judgment when communicating on internet-based platforms. You are a representative of the company when engaging in online activities and you must ensure that your behavior online, including on social media, is appropriate and consistent with our values. Disparaging communications, as well as statements revealing our clients' use of our services, even if made on your own time using your own resources, may be grounds for discipline up to and including immediate termination. For further details on the appropriate use of social media, you should refer to the Employee Handbook. The company's social media policy does not prohibit an employee from engaging in such

2 For purposes of this Code, the term "disparage" means to make statements that are egregiously offensive, purposely malicious, knowingly false, publicly disparaging the company's services without relating the complaint to any labor controversy, or otherwise reasonably calculated to harm the company's reputation and reduce its income.

communications that are intended to address employee concerns involving the terms and conditions of employment.

Conflicts of Interest & Personal Behavior

Exhibit personal behavior that reinforces a positive image of you and the company.

Your personal behavior, both inside and outside work, should reinforce a positive image of you, the company and its business activities. It is essential to use good judgment in all your personal and business dealings. You should refrain from engaging in activities or making disparaging statements that maliciously hurt the company's reputation, or yours, and that could undermine the relationship of trust between you and the company or the company and its clients. Employees who have acted inappropriately may be subject to disciplinary action up to and including termination for cause.

Remember your duties to Everise when participating in outside personal interests; obtain permission before pursuing business activities outside the scope of your role with the company

The company encourages directors and employees to be active participants in their community. While pursuing personal, political, not-for-profit activities or other like activities, be mindful that your participation in any outside interest must not prevent you from adequately discharging your duties to Everise. In addition, ensure that when you are involved in these activities you are not seen to be speaking or acting on behalf of the company without express authority.

"Outside Business Activities," otherwise known as "OBAs" include any business activities outside the scope of one's role with the company, including any activity as an employee, independent contractor, sole proprietor, officer, director, or partner of another business organization, regardless of whether compensation is involved. Employees must receive approval from their supervisor prior to accepting an OBA. If the direct business unit supervisor has doubts or concerns regarding the approval, you should consult with a member of the Legal Department or email legal@weareeverise.com. Directors of the company must advise the Chief Legal Officer prior to taking on any OBAs. Prior approval is not required to serve on boards of charities or small, private family holding companies that have no relation to the company. For greater clarity, approval is not needed to serve on the board of a family holding company which is an extension of one's personal business affairs; however, it is needed to serve on the board of a private operating business with significant operations. When in doubt whether you need to obtain permission, consult with a member of the Legal Department.

Avoid situations in which your personal interests conflict with the interests of the company, its clients or investors in Client accounts.

A "conflict of interest" for this purpose occurs when a person's private interest inclines the person, consciously or unconsciously, or appears to incline the person to act in a manner which is not in the commercial interests of the company. You may have a conflict of interest if you are involved in any activity that prevents you from performing your duties to the

company properly, or that may create a situation that could affect your ability to act objectively, effectively and in the best interests of the company, including due to among other things, personal interests or receipt of benefits from our relationships with companies, business partners, counterparties, service providers, and other constituencies. Accordingly, you must place the company's interest in any business matter ahead of any personal interest. Remember that the company's interest includes the company's obligations to its clients.

You may also have a conflict of interest or the appearance of a conflict of interest as a result of a "close personal relationship" with another employee at Everise or a counterparty with which Everise is engaging (e.g., a company employee's spouse works at an entity that is being considered as a service provider). To ensure that these relationships are managed appropriately, and to deal with any possible conflicts of interest in an appropriate and responsible manner, you are expected to disclose the existence of such relationships to your Human Resources ("HR") department.

For the purposes of the Code, a close personal relationship includes, but is not limited to, relationships with a parent or parent equivalent (e.g., adoptive parent), close relative, spouse, fiancée, common law, or anyone else with whom you are in, or have been in, a romantic or intimate relationship.

The best way to judge whether you may have a conflict of interest is to ask yourself whether a well-informed person would reasonably conclude that your interest, activity or close personal relationship could in any way influence your decision or performance in carrying out a duty on behalf of the company. To avoid conflicts of interest, identify potential conflicts when they arise; contact the Legal Department if you are unsure whether a specific interest or activity gives rise to a conflict situation or contact HR to disclose any close personal relationship that may give rise to a conflict. In addition, if you become aware of any conflict or potential conflict of another director, officer, or employee, you should consult HR, and the Legal Department, as appropriate.

Do not take corporate opportunities as your own personal opportunities.

You are prohibited from taking personal advantage of a business opportunity that you become aware of through your work at Everise. You owe a duty to the company to advance its commercial interests when the opportunity arises, and you must not compete with the company in any way.

Positive Work Environment

Be committed to our respectful work environment free from discrimination,³ violence⁴ and harassment.⁵

We value diversity and we should all do our part to maintain our respectful work environment where everyone feels safe, included and productive. The company does not tolerate workplace discrimination, violence or harassment. All directors, officers and employees must work to ensure that the company is a safe and respectful environment where high value is placed on integrity, fairness and respect. For more information on the company's commitment to its positive work environment, refer to the company's *Positive Work Environment Policy*.

You have a duty to report discrimination, violence and harassment.

If you experience or become aware of what you believe to be discrimination, violence or harassment, you are expected to report it in accordance with the "Reporting Potential Code Violations" section of the Code and/or in accordance with the *Positive Work Environment Policy*. Reports of discrimination, violence or harassment will be taken seriously and investigated. If you are found to be discriminating against, acting or threatening to act violently towards, or harassing any individual at Everise, or if you knowingly condone the discrimination of, violence towards, or harassment of another individual, you will face corrective action up to and including termination without notice and for cause.

We want to create a culture of reporting when it comes to discrimination, violence and harassment, as reporting is essential for us as a company to stamp out these behaviors. While we reserve the right to take corrective action if you knowingly make a false accusation about an innocent party, you will not face retaliation for making a good faith report or assisting in the investigation of a report.

3 "Discrimination" means the differential treatment of an individual or group based on prescribed characteristics protected by law. Prescribed characteristics generally include age, color, race, religion, sex, gender, marital status, ancestry, sexual orientation, national origin, disability. It does not matter whether the discrimination is intentional; it is the effect of the behavior that matters.

4 "Violence" means an action (oral, written or physical) which causes, is intended to cause, could reasonably be interpreted as a threat to cause, or is capable of causing death or bodily injury to oneself or others, or property damage.

5 For purposes of the Code, "harassment" means conduct which is known or ought reasonably to be known to be unwelcome and includes conduct (e.g., comments and actions) which would be perceived by a reasonable person as being hostile, humiliating or abusive or cause him/her torment. Harassment covers a wide range of conduct and includes sexual harassment, bullying and psychological harassment. Harassment may occur in a variety of ways and may, in some circumstances, be unintentional, but regardless of intent, all harassment negatively affects individual work performance and our workplace as a whole. This definition should not be interpreted so as to prohibit U.S. employees from engaging in "protected concerted activity" under the federal law known as the National Labor Relations Act.

Be committed to ensuring the health and safety of fellow directors, officers and employees.

We all have the right to work in an environment that is safe and healthy. In this regard, while at work you must:

- a. comply strictly with all occupational, health and safety laws and internal procedures;
- b. not engage in nor condone illegal or dangerous behavior, including any acts or threats of violence;
- c. not possess, distribute or be under the influence of drugs while on company premises or when conducting company business; and
- d. not possess or use weapons or firearms or any type of combustible material in the company's facilities, or at company-sponsored functions.

If you or someone you know is in immediate danger of serious bodily harm, first call local law enforcement authorities and then report the incident in accordance with the "Reporting Potential Code Violations" section of the Code and/or in accordance with the *Positive Work Environment Policy* in the Employee Handbook.

Human Rights and Modern Slavery

We are committed to conducting business in an ethical and responsible manner, including by carrying out our activities in a manner that respects and supports the protection of human rights through:

- a. the elimination of discrimination in employment;
- b. the prohibition of child and forced labor; and
- c. the eradication of harassment and physical or mental abuse in the workplace.

We strive to embed these standards into all our core business activities, including training, communications, contracts and due diligence processes. These practices extend to our interactions with our key suppliers and other business partners.

Environmental, Social and Governance ("ESG") Management

Our ESG principles are embedded throughout our operations and [are integral to building resilient](#) businesses and creating long-term value for our investors and other stakeholders. These include:

1. Mitigate the impact of our operations on the environment

- a. Strive to minimize the environmental impact of our operations and improve our efficient use of resources over time.

- b. Support the goal of net zero greenhouse gas (GHG) emissions by 2050 or sooner.
- 2. **Ensure the well-being and safety of employees;**
 - c. Foster a positive work environment based on respect for human rights, valuing diversity, and zero tolerance for workplace discrimination, violence or harassment.
 - d. Operate with leading health and safety practices to support the goal of zero serious safety incidents.
- 3. **Uphold strong governance practices;**
 - a. Operate to the highest ethical standards by conducting business activities in accordance with the Code.
 - b. Maintain strong stakeholder relationships through transparency and active engagement.
- 4. **Be good corporate citizens.**
 - a. Ensure the interests, safety and well-being of the communities in which we operate are integrated into our business decisions.
 - b. Support philanthropy and volunteerism by our employees.

Compliance with Laws, Rules, Regulations & Policies

Know and comply with all laws, rules, regulations and policies applicable to your position.

Our business is highly regulated, and the company is committed to compliance with applicable laws, rules, regulations and policies. Each of us must recognize our personal obligations as individuals, to understand and comply with the laws, rules, regulations and policies that apply to us in the conduct of our duties.

Many of the company's activities are governed by laws, rules, regulations and policies that are subject to change. If you have questions about the applicability or interpretation of certain laws, rules, regulations or policies relevant to your duties at Everise, you should consult with a member of the Legal Department. In the event a local law, custom or practice conflicts with the Code you must adhere to whichever is most stringent. If you know of any of our practices that may be illegal, you have a duty to report it. Ignorance of the law is not, in general, a defense to breaking the law. We expect you to make every reasonable effort to become familiar with the laws, rules, regulations and policies affecting your activities and to comply with them. If you have any doubts as to the applicability or interpretation of any of the above, you should obtain advice from the company's Legal Department.

Do not give or receive bribes, including “facilitation payments.”

We value our reputation for conducting business with honesty and integrity. It is vital for us to maintain this reputation as it generates confidence in our business by our stakeholders, which ultimately means it is good for business. We do not pay bribes in furtherance of our business, either directly or indirectly, and you are not permitted to pay bribes on our behalf or authorize others to pay bribes on our behalf. This commitment comes from the highest levels of management, and you must meet this standard. A bribe is anything of value that is offered, promised, given or received to improperly influence a decision or to gain an improper or unfair advantage in promoting, enhancing, obtaining or retaining business. Bribery may not always be in the form of cash payments and may take many other forms, including gifts, travel, hospitality, political contributions, charitable donations, lobbying payments, sponsorships, employment opportunities, internships, and secondments. Facilitation payments⁶ are also a form of bribe and are therefore not permitted. For further details, refer to company's *Anti-Bribery and Corruption Policy*.

Giving or receiving gifts/entertainment should be reasonable, and in certain cases prohibited.

Gifts and entertainment given to or received from persons who have a business relationship with the company are generally acceptable, if the gift or entertainment is modest in value, appropriate to the business relationship, and does not create an appearance of impropriety. No cash or cash equivalent payments should be given or received, except in limited circumstances preapproved by the Legal Department. Employees who do not comply with these requirements may be required to reimburse the company for the value of any gifts or benefits they make or receive on behalf of the company and may be subject to disciplinary action up to and including termination for cause. For further details, refer to the company's *Anti-Bribery and Corruption Policy*.

There may be restrictions on your political donations to candidates and political parties.

In certain jurisdictions, political donations made on behalf of the company are prohibited. Political donations made by individuals on their own behalf should comply with local laws and regulations. In the U.S., various federal, state, and municipal laws and regulations impose specific restrictions and rules with respect to political contributions, both those made on behalf of the company or made by individuals on their own behalf, which can carry significant penalties for the company for violations. To ensure that we do not breach the law regarding political donations in any country, all political donations, no matter how small, made on behalf of the company (directly or indirectly) or by individuals and/or their family members must be approved in advance by the applicable regional head or the Legal Department.

6 Facilitation payments are small payments made to secure or speed up routine actions or otherwise induce public officials or other third-parties to perform routine functions they are otherwise obligated to perform, such as issuing permits, approving immigration documents or releasing goods held in customs. This does not include legally required administrative fees or fees to fast-track services.

We must prevent the use of our operations for money laundering or any activity that facilitates money laundering, the financing of terrorism, or other criminal activities.

The company is strongly committed to preventing the use of its operations for money laundering, the financing of terrorism, or other criminal activities, and will take appropriate actions to comply with applicable anti-money laundering laws. Everise has procedures for conducting anti-money laundering due diligence on investments and divestments.

You should consider your rights and obligations when providing information to governmental authorities.

During your employment at Everise you may be contacted by governmental authorities (e.g., law enforcement, securities regulators, etc.) who are seeking confidential information from you which you obtained through your association with Everise.

Whether you are able to respond to these questions or not, we strongly recommend that, for your own protection, you do not speak with authorities without first seeking legal advice on your obligations. In this situation, you may contact the Legal Department to guide you on how to proceed.

Notwithstanding the foregoing, nothing in the Code prohibits or restricts you in any way from providing information to a government authority pursuant to a subpoena or applicable whistleblowing regulations. For further information, refer to the *Whistleblower Policy*.

You have internal reporting obligations in the event you are convicted of a felony or misdemeanor.

We are only as good as our people, and therefore our reputation as a leading global alternative asset manager depends on the reputation of the individuals who serve the company as a director, officer or employee. Our screening process at Everise is rigorous and includes background checks so that we have the best information possible about our prospective directors, officers and employees. Once at Everise, we expect you to continue to adhere to these principles of openness, honesty and transparency. If at any time while you are employed with the company you are convicted of a felony or misdemeanor (or been subject to any similar conviction in any jurisdiction) or are involved in any conduct that you think may be relevant to your reputation, you have an obligation to report this information to the Legal Department or your supervisor so that it may be appropriately documented internally.

Reporting Potential Code Violations

You are expected to make good faith reports.

Internal reporting is critical to the company's success, and it is both expected and valued. You are required to be proactive and promptly report any suspected violations of the Code, or any illegal or unethical behavior or misconduct that you become aware of or are involved with. When making a report, please include specific details and back-up documentation

where feasible in order to permit adequate investigation of the concern or conduct reported. Vague, nonspecific or unsupported allegations are inherently more difficult to pursue.

Employees are expected to report actual or potential misconduct or violations of the Code to their supervisor in the first instance, since their supervisor is generally in the best position to resolve the issue. Alternatively, you may contact the HR Department or the Legal Department to report any actual or potential misconduct or Code violations, or if you have any specific or general questions.

If you have questions about the Whistleblower Policy, contact the Legal Department.

In the event you do not want to report violations to your supervisor, HR, or the Legal Department, you can always make a report through the company's reporting hotline.

Our Reporting Hotline is managed by an independent third-party. The Reporting Hotline allows anyone to call anonymously (if they so choose) to report suspected unethical, illegal or unsafe behavior in English and other languages. The Reporting Hotline is available toll-free, 24 hours a day, 7 days a week. Refer to the "Contact Information" section of the Code for the Reporting Hotline phone numbers by jurisdiction. If you choose to make an anonymous report, your anonymity will be protected to the fullest extent possible as permitted by law. If you have an HR-related issue, the HR Department runs a ticketing platform that is suitable for addressing interpersonal or other workplace issues that are not Code violations.

Reports will be kept confidential and will be dealt with appropriately.

The confidentiality of reported violations will be maintained to the fullest extent possible, consistent with the need to conduct an adequate review and subject to applicable law. You may wish to identify yourself to facilitate our investigation of any report; however, you can make an anonymous report by calling the Reporting Hotline. The party receiving the initial report must record its receipt, document how the situation was dealt with and file a report, which will be retained for the record. The Chief Legal Officer or the Chief People Officer, as appropriate, will report all illegal and unethical conduct in violation of the Code to the appropriate Everise Board of Directors, or a committee thereof as appropriate, and externally in accordance with applicable laws.

Everise prohibits retaliation against anyone who reports suspected violations of the Code or any law or regulation.

No retribution or retaliation will be taken against any person who has filed a report based on the reasonable good faith belief that a violation of the Code or any law or regulation has occurred or may in the future occur; however, making a report does not necessarily absolve you (if you are involved) or anyone else of the breach or suspected breach of the Code. The company reserves the right to discipline you, up to and including termination for cause, if you provide false information or make an accusation you know to be untrue. This does not mean that the information that you provide has to be correct, but it does mean that you must reasonably believe that the information is truthful and demonstrates at least a possible

violation of the Code. If you believe that you have been unfairly or unlawfully retaliated against, you may file a report with your supervisor, the HR team, or the Legal Department, or by calling the Reporting Hotline.

Disciplinary Action For Code Violations

Please note that we reserve the right to take disciplinary action for Code violations that fits the nature and particular facts of the violation. This could include suspension or immediate termination for cause and, if warranted, legal proceedings may be brought against you.

Statement of Compliance

Upon starting at Everise, each director, officer, employee and temporary worker who is subject to this Code will be provided with a copy of the Code and other policies referenced herein and is required to be reviewed and signed. The acknowledgement is maintained by the HR Department in your personnel file. On an annual basis, each director, officer, employee and temporary worker who is subject to this Code will be required to re-certify compliance with the Code via an acknowledgement of the Employee Handbook.

Waivers

A waiver of the Code will be granted only in very exceptional circumstances. A Code waiver for Everise employees, must be approved by the Chief Legal Officer and the Chief People Officer.

Amendments

The Board of Directors of Everise reviews and approves each updated edition of the Code and is ultimately responsible for monitoring compliance with the Code.

SCHEDULE A CONTACT INFORMATION

Below are the international calling instructions for employees (Worldwide Toll-Free Number) for countries that do not use a direct dial toll-free number.

1. For Employees:

- a. Make sure you have an outside line.
- b. Enter the Access Code for the country and/or the telephone system you are calling from.
- c. An English-language voice prompt will ask for the number you are calling.
- d. Enter our toll-free number: 800-603-2869. There is no need to dial '1' before the toll-free number. You are now connected to the hotline.
- e. A Lighthouse greeting will be played in multiple languages. Make a choice from the prompts or press 0 and tell the English operator the language you speak (preferably in English). An interpreter will then join the call in 2 – 3 minutes. The Lighthouse operator will interview you aided by the interpreter.
- f. A report in English is then sent to the designated recipient(s) of your company.
- g. Access codes are subject to change.

2. Calling Instructions

- a. Make sure you have an outside line.
- b. Enter the Access Code for the country and/or telephone system you are calling from. You will then hear a 'bong'.
- c. An English-language voice prompt will ask for the number you are calling.
- d. Enter our toll-free number **800-603-2869** There is no need to del "1" before the toll-free number.
- e. You are now connected to the hotline
- f. A Lighthouse greeting will be played in multiple languages Make a choice from the pre-recorded language prompts' or press 000 and tell the English operator the language you speak (preferably in English) An interpreter will then join the call in 2 ± 3 minutes. The Lighthouse operator will interview you, aided by the interpreter
- g. A report in English is then sent to the designated recipient(s) of your company.

h. Access codes are subject to change.

The following automated in-language greetings are provided to the caller.

English	press 1	Hungarian	press 01	Finish	press 001
Spanish	press 2	Polish	press 02	Russian	press 002
French	press 3	Dutch	press 03	Hindi	press 003
Mandarin	press 4. wait for greeting, then press 1	Czech	press 04	Hebrew	press 004
Cantonese	press 4, wait for greeting, then press 2	Taiwanese	press 05	Turkish	press 005
German	press 5	Korean	press 06	Other	press 000
Italian	press 6	Tagalog	press 07		
Portuguese	press 7	Vietnamese	press 08		
Japanese	press 8	Indonesian	press 09		
Arabic	press 9				

3. Access Codes for calls made outside North America:

Guatemala	
English	999-9190
Spanish	999-9190
Malaysia	
Singapore	
SingTel	800-011-1111
StarHub	800-001-0001
Philippines	
PLDT English	1010-5511-00
PLDT Tagalog	1010-5511-10, 2nd Option 105-11
Globe English	105-11
Globe Tagalog	105-12
Philcom English	105-11
Philcom Tagalog	105-12
Digitel	105-11

<i>Digitel Tagalog</i>	<i>105-12</i>
<i>Smart English</i>	<i>105-11</i>
<i>Smart Tagalog</i>	<i>105-12</i>
<i>Bayan</i>	<i>105-11</i>
<i>Colombia</i>	<i>01-800-911-0010</i>
<i>Japan</i>	
<i>Japan (KDDI)</i>	<i>00-539-111</i>
<i>Japan (NTT)</i>	<i>0034-811-001</i>
<i>Japan (Softbank Telecom)</i>	<i>00-663-5111</i>
<i>Ireland</i>	
<i>Ireland</i>	<i>1-800-550-000</i>
<i>Ireland (UIFN)</i>	<i>00-800-222-55288</i>
<i>India</i>	<i>000-117</i>

Chief Legal Officer

Helen Franco

Email: helen.franco@weareeverise.com

Chief People Officer

Sheena Ponnappan

Email: sheena.ponnappan@weareeverise.com

LEGAL NOTICE

The company reserves the right to modify, suspend or revoke the Code and any related policies, procedures, and programs at any time. The company also reserves the right to interpret and amend the Code and these policies in its sole discretion. Any amendments to the Code will be disclosed and reported as required by applicable law.

Neither the Code, nor any of the policies referred to herein, confer any rights, privileges or benefits on any employee, create an entitlement to continued employment with the company, establish conditions of employment for the employee or create an express or implied contract of any kind between employees and the company. In addition, the Code does not modify the employment relationship between employees and the company.

The Code is posted on Workday and included in each edition of the Employee Handbook. The posted version of the Code may be more current and supersedes any paper copies, should there be any discrepancy between paper copies and what is posted.

May 03, 2023

ANTI – BRIBERY & CORRUPTION POLICY

1. Introduction

This Anti-Bribery and Corruption Policy (“**ABC Policy**”) applies to all directors, officers and employees (collectively, “**you**”) of Everise.

Everise is committed to operating with the highest ethical standards and this includes preventing bribery in our business activities. This ABC Policy sets forth key principles and standards, as well as key supporting policies and procedures, with respect to addressing bribery risks in our business, which should guide your conduct.

This ABC Policy should be read in conjunction with the (“**Code**”), which serves as a guide for how you should conduct yourself as a member of the Everise team.

2. Zero-Tolerance Approach to Bribery

Do not give or receive bribes, including facilitation payments.

We have, over many years, built a reputation for conducting business with honesty and integrity. It is vital for us to maintain this reputation as it generates confidence in our business from our customers, clients, investors, investees, and others – which ultimately means it is good for business.

We do not pay bribes in furtherance of our business and expect that you will not do so on our behalf. We have a zero-tolerance approach towards bribery. This commitment comes from the highest levels of management, and you must meet this standard.

A bribe is anything of value that is offered, promised, given, or received to improperly influence a decision or to gain an improper or unfair advantage in promoting, enhancing, obtaining or retaining business. Bribery may not always be in the form of cash payments and may take many other forms, including:

- Gifts, travel, entertainment, and hospitality;
- Political contributions and charitable donations;
- Employment opportunities, directorships, internships, or secondments;
- Procurement and service contracts;
- Phony jobs or “consulting” relationships;
- Excessive discounts or rebates; or
- Non-arm’s length loans, forgiveness of debt or other transactions.

Facilitation payments are also a form of bribe and are, therefore, not permitted. Facilitation payments are small payments made to secure or speed up routine actions or otherwise induce public officials or other third-parties to perform routine functions they are otherwise obligated to perform, such as issuing permits, approving immigration documents or releasing goods held in customs. This does not include official, legally permitted statutory or administrative fees formally imposed and codified by government agencies for expedited service.

3. Dealing with Public Officials

Interactions with public officials require enhanced scrutiny & sensitivity.

A public official is any person who is employed by or is acting in an official capacity for a government, a department, agency or instrumentality of a government, or a public international organization. This includes elected or appointed persons who hold legislative, administrative or judicial positions, such as politicians, bureaucrats, civil servants, and judges. It also includes candidates for political office, political party officials and persons who perform public functions, such as professionals working for public pension plans, public health agencies, water authorities, planning officials and agents of public international organizations, such as the United Nations or World Bank. A public official may also include persons in the service of or employees of government-owned or controlled businesses, including sovereign wealth funds and state-owned utility companies. For example, if a government has an interest in a utility and exercises control over the activities of that utility, then the utility's officials are likely to be considered public officials. Third parties acting at the direction of these individuals and entities, should also be considered public officials.

There is increased sensitivity and scrutiny of dealings with public officials because this has traditionally been an area where bribery activity is more likely to occur. Be cognizant of these risks in your dealings and interactions with public officials and consider how your actions may be viewed. For example, payments, gifts, or employment to close relatives of public officials have been treated by enforcement authorities as direct payments to the public officials and, therefore, may constitute violations of law.

Hiring public officials or persons referred by public officials requires enhanced scrutiny.

Hiring public officials or applicants related to, or referred by, public officials could be seen as a bribe in certain situations and should be subject to enhanced review to ensure that the related risks are appropriately mitigated. Consult your Human Resources team for procedures related to identifying and mitigating these risks.

In practice, situations can be complex and this ABC Policy does not cover every circumstance that you may encounter. When in doubt, please contact the company's Legal and Regulatory Group for assistance.

4. Third Parties

Third Parties are not permitted to pay bribes on our behalf.

The company may be scrutinized and/or prosecuted for failing to detect and prevent bribery by a person associated with it. This includes any individual or entity that performs services for or on behalf of the company. Employees should avoid doing business with third-parties who do not have a zero tolerance approach to bribery.

This means due diligence should be undertaken on contractors, joint venture partners, agents, and other third-parties to establish their anti-bribery credentials, where warranted by the assessed level of risk. This due diligence could include meeting with them to better assess their business practices and anti-bribery and corruption policies/controls and making inquiries into their reputation and past conduct. Other risk mitigation strategies, such as including anti-bribery language in agreements, should also be implemented, as appropriate.

Please refer to the company's third-party due diligence procedures for further details.

5. Gifts, Meals & Entertainment

The giving or receiving of gifts, meals & entertainment should be proportionate & reasonable for the circumstances, for legitimate purposes only, not with a view to improperly inducing third-party to misuse their position, as a quid pro quo for official action or with linkage to an official decisions.

Gifts (e.g. merchandise, event tickets) given to or received from persons who have a business relationship with the company are generally acceptable, if the gift is reasonable in value, infrequent, appropriate to the business relationship, and does not create an appearance of impropriety. No cash payments should be given or received.

Meals and entertainment (e.g. sporting events or the theatre, concerts, rounds of golf) given to or received from persons who have a business relationship with the company are generally acceptable, but again only if the meal or entertainment is reasonable in value, appropriate to the business relationship, infrequent, does not create an appearance of impropriety, is otherwise in accordance with applicable laws and regulations, and if a representative from the sponsoring organization (the party paying for the meal or entertainment) is present at the event. For the avoidance of doubt, if a representative from the sponsoring organization is not present at the event, the meal or entertainment would be considered a gift. Also, be aware that many jurisdictions have laws restricting meals and entertainment given to public officials or their close relatives that must be followed.

Gifts, meals and entertainment that are repetitive, no matter how small, may be perceived to be an attempt to create an obligation to the giver and should not be

provided. Gifts or entertainment given close in time to when a decision impacting Everise's business is being made (including by a private business partner) may be perceived as a bribe in return for a favorable decision and should also not be provided. Employees should not pay for gifts, meals and entertainment personally to avoid having to report or seek approval.

Travel (e.g. for due diligence or site visit) and related items given or received should follow the same principles as for gifts, meals and entertainment. When travel or related items are given, payment should be made directly to the provider (as opposed to providing a reimbursement to the individual), whenever possible. Under no circumstances should cash or per diem reimbursements be provided.

To help ensure that our practices are reasonable, appropriate and otherwise in accordance with applicable regulatory requirements, certain gifts, meals and entertainment must be logged and/or pre-approved.

If you are in doubt as to whether proposed gifts, meals or entertainment to be given or received are appropriate, please consult the Legal Department for assistance.

6. Charitable Donations

Do not solicit or offer donations to clients, suppliers, vendors, public officials or others in a manner which communicates that a donation is a prerequisite for future business or that the offer of a donation is intended to obtain or retain business and a business advantage.

We encourage our directors, officers, and employees to contribute personal time and resources to charities and not-for-profit organizations. However, unless approved, you are prohibited from using the company's name, resources or business contacts for solicitation of donations. Charitable donations made by directors, officers, and employees on their own behalf should have no relationship to company business and must comply with local laws and regulations.

Requests for donations may take many forms (e.g. direct requests or indirect requests such as purchasing a table, a round of golf or otherwise contributing to an event designated to raise money for a particular charitable cause/organization). All requests for donations to charities and other not-for-profit organizations (e.g. schools, hospitals, libraries, etc.) must be approved in advance by the Chief Financial Officer and the Chief Legal Officer. If you are requested by a public official to make a donation to a particular charity, please obtain approval before agreeing to or making the donation. Also consider conducting due diligence when the proposed charity or not-for-profit organization is not well-known or there may be question as the legitimacy of the organization as a charity or not-for-profit.

7. Political Contributions & Lobbying

Do not offer or make contributions to political parties, officials and/or candidates that might influence, or be perceived as influencing, a business decision.

In the U.S. and other jurisdictions, various federal, state, and municipal laws and regulations impose specific restrictions and rules with respect to political contributions, including both those made on behalf of the company or made by individuals on their own behalf. Violation of these laws and regulations can carry significant penalties for the company.

If you are in doubt as to whether a proposed political contribution is appropriate, please consult the Legal Department for assistance.

Do not engage in any lobbying activities on behalf of the company without specific authorization.

Lobbying activities generally include attempts to influence the passage or defeat of legislation and may trigger registration and reporting requirements. In many jurisdictions, the definition of lobbying activity is extended to cover efforts to induce rule-making by executive branch agencies or other official actions of agencies, including the decision to enter into a contract or other arrangement.

You may not engage in lobbying activities on behalf of the company without the prior written approval of the Legal Department.

8. Record -Keeping

Record all our transactions in a complete, accurate and detailed manner so that the purpose and amount of the transaction is clear.

In addition to prohibiting bribery, anti-bribery legislation and other laws expressly require accurate and complete recordkeeping and the establishment and maintenance of an adequate system of internal controls. One purpose of these provisions is to prevent companies from concealing bribes and to discourage fraudulent accounting practices.

All transactions should be recorded completely, accurately and with sufficient detail so that the purpose and amount of any such payment is clear. No undisclosed or unrecorded funds or assets of the company should be established for any purpose. False, misleading, or artificial entries should never be made in the books and records of the company for any reason.

9. Reports and Complaints

Internal reporting is critical to the company's success, and it is both expected and valued. You are required to be proactive and promptly report any suspected violations of this ABC Policy, or any illegal or unethical behavior of which you become

aware, including, but not limited to, any situations where a public official or other party requests or appears to request an inappropriate benefit. The confidentiality of reported violations will be maintained to the fullest extent possible, consistent with the need to conduct an adequate review and subject to applicable law. No retribution or retaliation will be taken against any person who has filed a report based on the reasonable good faith belief that a violation of the ABC Policy has occurred or may in the future occur. Employees may report actual or potential misconduct or violations of the ABC Policy to their supervisor in the first instance, since their supervisor is generally in the best position to resolve the issue. Alternatively, you may contact the Human Resources Department or the Legal Department to report any actual or potential misconduct or ABC Policy violations, or if you have any specific or general questions. Members of the subsidiary Boards of Directors should promptly report violations to the Chief Legal Officer. In the event you do not want to report violations to your supervisor, the Human Resources Department or the Legal Department, you can always make a report through the company's reporting hotline. See the Code for our reporting hotline information, which is managed by a third-party and allows for anonymous reporting of suspected violations by phone or email.

Disciplinary Action for ABC Policy Violations

Please note that we reserve the right to take disciplinary action for ABC Policy violations that fits the nature and particular facts of the violation. This could, in the most severe circumstances, include immediate termination for cause and, if warranted, legal proceedings may be brought against you.

10. Key Contacts

If you have any questions on this ABC Policy, please contact:

Dave Palmer, President, dave.palmer@weareeverise.com

Sheena Ponnappan, Chief People Officer, sheena.ponnappan@weareeverise.com

Helen Franco, Chief Legal Officer, helen.franco@weareeverise.com

SUSTAINABILITY POLICY

1. Purpose

To ensure the understanding of the fundamental principles for our commitment to the well-being of employees, communities and the environment, and complying with applicable laws.

Everise will do this by:

- Adherence to current environmental legislation where applicable.
- Streamlining business processes, creating less waste, & using less energy in Everise facility.
- Create a better reputation with environmentally conscious customers.
- Supporting and respecting the protection of human rights and ensuring the company is not complicit in human rights abuses.
- Work against corruption in all its forms, including extortion and bribery.

2. Corporate Responsibility Statement

Everise activities and services will be legally and ethically conducted by treating employees, environments, and cultures with respect. We will minimize negative environmental impacts and ensure social responsibility efforts are done with transparency and openness.

3. Transparency Pledge

Everise pledges to conduct its corporate responsibility and sustainability efforts with transparency and openness. We expect our suppliers to conduct their business in the same way.

4. Roles & Responsibilities

Facilities

- Monitor workplace practices, procedures, and material use, and promote those providing the greatest reduction of energy, water and materials; and reduce employee exposure to toxic substances and harm to the environment.
- Lead & facilitate the development of sustainable operations.
- Review building maintenance contracts, remodeling and new building construction proposals, and internal work plans. Revise as appropriate to ensure Everise conserves resources and uses non-toxic materials.

- Assist with the development of sustainable operations.

Purchasing

- Write procurement specifications and contract language ensuring contractors, vendors use resources in the most sustainable manner.
- Research products and practices to be used in the normal and the unique business of Everise that can be used to further these sustainability goals.
- Monitor the use of sustainable purchasing/procurement procedures.
- Assist with the development of sustainable operations.

Everise Employee

- Reduce or eliminate unnecessary use of supplies and other resources.
- Turn off personal, non-essential computers when leaving work for the day.
- Turn off monitors when leaving work area for an extended period throughout the workday.
- Comply with the policies outlined in this document.

OUTSIDE EMPLOYMENT POLICY

1. Objective

At Everise, we continue to evolve robust protocols for our employees to support our valued customers, one of which is to prohibit our employees from engaging in outside employment (moonlighting). All employees must inform, and obtain the prior written permission of, the Chief People Officer to engage, or continue to engage, in outside employment. If permission is granted, the terms and conditions of Everise's Outside Employment Policy ("**OE Policy**") shall apply to the outside employment. For purposes of this OE Policy, outside employment shall mean any employment, engagement, consultancy, self-employment which is outside the employment with Everise.

2. Scope

This OE Policy applies to all full-time and part-time employees of Everise who are not parties to Employment Contracts that contain restrictions and/or requirements relating to outside employment.

3. Policy Guidelines

- **Permissible if No Conflict of Interest:** Outside employment must not adversely affect an employee's ability to meet the company's work requirements or create a conflict of interest. Under certain circumstances, if an employee's outside employment or personal conduct begins to adversely affect their performance on the job or begins to make it impossible for them to carry out any or all of their job duties while at work, appropriate disciplinary action up to and including termination of employment may be appropriate.
- **Clients, Customers and Competitors of the Employer:** Employees may not work for any client or customer of Everise outside of regular work hours as described above without the approval of the Chief People Officer or a designated representative. Employees are prohibited from engaging in outside employment that directly or indirectly competes with the business of the company.
- **No Liability:** Everise will not assume any responsibility for an employee's outside employment. Specifically, the company will not provide workers' compensation coverage or any other benefit for injuries occurring from or arising from such outside employment. The company will not pay medical benefits for injuries or sickness to an employee resulting from employment by any employer other than the company.
- **For U.S. Employees Only – NLRA Activity:** Protected concerted activity covered by the U.S. National Labor Relations Act (NLRA) or the particular collective bargaining agreement is not prohibited by this OE Policy.

4. Activities Adversely Affecting Employment

Following are examples of outside employment that might adversely affect an employee's ability to perform their job duties and are prohibited:

- Employment that directly or indirectly competes with the business of the company;
- Employment that conflicts with the employee's work schedule, duties, and responsibilities or creates an actual conflict of interest (see the COI Policy in the Code);
- Employment that impairs or has a detrimental effect on the employee's work performance with the company; and
- Employment that requires employees to conduct work or related activities on company property, during company working hours, or using company facilities and/or equipment.

5. Guidelines for Outside Employment

The following guidelines apply to all outside employment of Everise employees:

- The employee cannot use the company name nor allude to their position in any way in connection with their outside employment unless specifically approved by the Chief People Officer in writing.
- The employee shall not use any company property, services, supplies, stationery, phone, fax, email, or other company resources to conduct work-related tasks on behalf of the Outside employer during company work time.
- Employees shall not disclose or otherwise use in their outside employment any confidential business information received as a result of working for Everise unless such information is generally known to the public or to those in the particular industry in which the outside employment is undertaken. Such information is proprietary and confidential to Everise. The employee must comply with the company's Confidentiality Policy, Non-Solicitation, and Non-Disparagement Policy included in the Employee Handbook.

Except as stated in paragraph 2 above regarding Employment Contracts, this OE Policy supersedes all prior policies, arrangements or understandings regarding its subject matter, including without limitation any conflicting statements or requirements of outside business activities set forth in the Code of Conduct.

Everise reserves the right to modify, withdraw, supplement or make exceptions to this OE Policy in its sole discretion at any time or from time to time.

SANCTIONS AND TRADE CONTROLS POLICY

1. Introduction

Scope

This Sanctions and Trade Controls Policy (the **Policy**) applies to all Employees (collectively **you**) of Everise and its wholly-owned subsidiaries (collectively **we, us, our** or the **company**).

We also expect Associated Persons engaged directly or indirectly by Everise to comply with this Policy.

Purpose

Everise is committed to complying with all international Sanctions and Trade Controls that apply to its business. This Policy applies to all Employees and Associated Persons who must comply with in the conduct of their day-to-day business.

2. Definitions

"Associated Persons" means agents, advisers, brokers, consultants, contractors or other third parties who perform services for or on behalf of Everise.

"Controlled Item" means an Item that is controlled for the purposes of applicable laws, rules or regulations, (for example, the Item requires a licence or authorisation from the applicable government(s) prior to export, re-export, transfer, or re-transfer).

"Dual-Use Items" means any Items which can be used for both civil and military purposes and including all Items which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices.

"Employees" means Board members (executive and non-executive), all employees (full time or part time), secondees, agency workers, and temporary workers⁷ and any other individual who is engaged by or under the effective control of Everise.

"Item(s)" means any goods, part, product, component, software, technology, or related technical data.

"Manager" means in relation to (a) Employees, the person to whom they directly report; and (b) in relation to Associated Persons who are not Employees, the Employee who manages their services and/or contract with Everise.

⁷ For purposes of the Policy, "temporary workers" include non-full-time employees and consultants and contractors etc. that work on our premises. The business group retaining a temporary worker is responsible for ensuring that the temporary worker certifies their commitment to comply with the Policy.

“Sanctioned Countries” means countries and/or territories that are subject to country- and/or territory-wide Sanctions. As at the date of this Policy, this covers the following countries and territories: Cuba, Crimea, Donetsk, Luhansk, Iran, North Korea and Syria.

“Sanctioned Persons” means persons, entities or any other parties (a) located, domiciled, resident, or organised in a Sanctioned Country; (b) targeted by any Sanctions administrated by the United Nations, the European Union, the US, the UK, and/or any other applicable country; and/or (c) owned or controlled by or affiliated with persons, entities, or any other parties as referred to in (a) and (b).

“Sanctions” means any international economic, financial or trade sanctions laws, regulations, orders or embargoes or measures having similar effect, in each case, adopted, administered, enacted or enforced from time to time by countries and countries’ bodies, agencies and institutions.

“Trade Controls” means any prohibitions or restrictions on the trade or movement of goods, products or services from, to, from or through a particular country, imposed by the government or relevant authority of a country. Restrictions may be imposed over direct and indirect imports, exports, re-exports, transfers, and re-transfers in respect of (a) particular kinds of goods, products or services; (b) the exporting or destination country or geographic territory; and/or (c) the identity of the exporter or recipient.

3. Policy Statements

Everise is committed to compliance with applicable Sanctions and Trade Controls and ensuring that our Employees and Associated Persons do likewise when carrying on business anywhere in the world.

We recognise that a failure to comply with applicable Sanctions and Trade Controls, or to prevent or manage this risk, would not only constitute a breach of legal and/or regulatory requirements, but could carry significant reputational damage, legal and regulatory action and financial loss for Everise.

This Policy sets out the company’s minimum standards and expectations to ensure compliance with applicable Sanctions and Trade Controls as well as its approach to identifying, mitigating and managing Sanctions and Trade Controls compliance risks. Where local laws are more stringent than the standards contained herein, such local law requirements should be applied in addition to the standards set out in this Policy.

4. Roles & Responsibilities

You must:

- read, understand and comply with this Policy and any other documents aimed at its implementation;

- demonstrate ethics, integrity and accountability at all times and expect the same from others;
- ensure that you comply with all applicable Sanctions, including those of the country or jurisdiction where you may be working, and laws of your country or countries of citizenship;
- comply with the sanctions screening and due diligence requirements in sections of this Policy;
- understand the Trade Controls relevant to any Items that you deal with as part of your role and comply with them;
- remain vigilant to ensure compliance with this Policy and applicable Sanctions and report potential breaches;
- not act in a way which is intended to avoid or evade applicable Sanctions obligations or conceal detection of a transaction which would otherwise breach this Policy; and
- notify the Chief Legal Officer immediately if you become a target of any Sanctions.

5. Sanctions

We must ensure that we are aware if the people, companies, and countries that we are doing business with are Sanctioned Persons or Sanctioned Countries. This is because Sanctions can restrict the provision of money, goods, and services to Sanctioned Persons and Sanctioned Countries.

There are many different types of Sanctions, including:

- targeted financial restrictions on people, companies, governments, and countries, such as asset freezes or “blocking” sanctions;
- economic sanctions that restrict the financing or provision of financial services in relation to certain goods, services, or financial products;
- trade-related restrictions that stop or limit the provision of certain goods and services in relation to targeted people, companies, governments, and countries;
- travel bans on named individuals; and
- anti-boycott regimes.

Sanctions can target either specific individuals or entities, or may target industry sectors or entire countries/territories. Sanctioned Persons can be anywhere in the world.

To ensure compliance, Everise should undertake the sanctions screening and due diligence process described below, in parallel to any additional third party due

diligence checks (including the procedures outlined in the Third-Party Due Diligence Procedures). We also expect our Associated Persons to conduct similar levels of checks and diligence when conducting business for or on behalf of Everise.

Sanctions Screening

Prior to engaging with any counterparties (e.g. customers, end-users, agents, suppliers and any other Associated Persons), Employees must conduct Sanctions screening on those counterparties.

Sanctions screening involves checking whether the potential counterparty has any links to a Sanctioned Country and/or whether they are listed in any of the following lists:

- the United Nations Security Council Consolidated List;⁸
- OFAC's Specially Designated Nationals and Blocked Persons list and Consolidated Sanctions List;⁹
- the EU's Consolidated List of Persons, Groups and Entities Subject to EU Financial Sanctions;¹⁰
- the UK's Consolidated List of Financial Sanctions Targets; and¹¹
- equivalent lists of other relevant countries.

Sanctions screening should also be performed, where possible, on any other persons who are known to be connected to the proposed transaction. This will need to be judged on a case-by-case basis.

Sanctions screening should be conducted through a third party screening tool available to Everise. Basic internet searches may also be carried out.

If any "hits" against any of these sanctions lists are identified, the matter must be referred to the Chief Legal Officer who will confirm whether the proposed transaction or activity can go ahead or whether further diligence is required (see below).

Sanctions Due Diligence

Sanctions due diligence must be carried out if (i) the Chief Legal Officer determines that a proposed transaction with a counterparty carries a Sanctions risk and/or (ii) if

8 <https://www.un.org/securitycouncil/content/un-sc-consolidated-list>

9 <https://sanctionssearch.ofac.treas.gov/>

10 https://ec.europa.eu/info/business-economy-euro/banking-and-finance/international-relations/restrictive-measures-sanctions_en

11 <https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets>.

a proposed counterparty is located in, resident in or incorporated under the laws of, a Sanctioned Country and/or (iii) if there are any other material red flags from the information available.

The precise scope of the further diligence to be carried out must be agreed with the Chief Legal

Officer on a case-by-case basis and in accordance with Everise procedures.

If the further due diligence raises any Sanctions-related concerns, the Chief Legal Officer must provide prior written approval before proceeding with the transaction.

The Chief Legal Officer will also advise on what further steps you should take to ensure that the relationship does not give rise to any Sanctions risks to the company. This may include incorporating specific language in the relevant contractual documents in order to provide adequate contractual protection against Sanctions-related risks and on-going monitoring.

6. Trade Controls

Many countries impose Trade Controls on the export, import, transfer, re-export, and re-transfer of military goods and Dual-Use Items. Broadly, Dual-Use Items are items that are capable of a military or civilian use. The rules are complex and can capture the transfer of technical data, as well as the movement of physical goods. Often the controls are related to the identity of the country of destination, the exporter, or the recipient of the Items and can extend upon Dual-Use Items.

Each Everise company must ensure that it:

- understands the Trade Controls relevant to and classification of any Items that it exports, imports, transfers, re-exports, and re-transfers;
- appropriately secures and maintains any Controlled Items in accordance with applicable laws and regulations;
- implements any necessary travel protocols and data security measures needed to protect Technical Data relating to Controlled Items;
- secures where required end-user certificates and includes an appropriate statement on relevant sale, supply, and shipping documents preventing the diversion of the Items; and
- complies with the terms of any Licenses.

Employees must ensure that they:

- understand the Trade Controls relevant to any Items that they deal with as part of your role;

- undertake a geographic risk-assessment before the import, export, transfer, re-export, or re transfer of any Items takes place and ensure that Items are not delivered to prohibited end-users or for prohibited end-uses;
- obtain prior written approval from the Legal Department before they export, transfer, re-export, or re-transfer of Controlled Items; and
- follow this Policy and any policies imposed by the Everise business they work for.

7. Reporting & Investigating Issues

Reporting actual or suspected issues

Internal reporting is critical to the company's success, and it is both expected and valued. You are required to be proactive and promptly report any suspected violations of this Policy. The confidentiality of reported violations will be maintained to the fullest extent possible, consistent with the need to conduct an adequate review and subject to applicable law. No retribution or retaliation will be taken against any person who has filed a report based on the reasonable good faith belief that a violation of the Policy has occurred or may in the future occur. This rule is applicable even if it is later discovered that they had been mistaken about the concern raised

Employees may report actual or potential misconduct or violations of the Policy to their supervisor in the first instance, since their supervisor is generally in the best position to resolve the issue. The supervisor must judge whether the issue or allegations are material. If so, they must immediately report the issue to the Chief Legal Officer.

Alternatively, you may contact the company's Chief Legal Officer to report any actual or potential misconduct or Policy violations, or if you have any specific or general questions. In the event you do not want to report violations to your supervisor or the Chief Legal Officer, you can always make a report through the company's reporting hotline. See the Code of Business Conduct and Ethics for contact information for our reporting hotline, which is managed by a third-party and allows for anonymous reporting of suspected violations.

Investigating actual or potential incidents

Any reports of known or suspected violations of this Policy or applicable Sanctions and Trade Controls must be promptly and appropriately investigated by the Chief Legal Officer. Precisely how the investigation must proceed should be considered on a case-by-case basis.

Communications With Governments & Regulations

You must obtain approval from the Chief Legal Officer prior to entering into any communications with a government or regulator regarding Sanctions. Such

communications could involve potential or actual breaches of law, disclosures, audits, information requests, or the start of an investigation.

8. Breaches of this policy

Everise takes its responsibilities with regard to Sanctions issues very seriously. Proven violations of this Policy may lead to severe disciplinary action, which could involve:

- a formal reprimand;
- suspension;
- restitution; and/or
- termination of employment and/or Associated Persons and other contracts.

These penalties may be imposed over and above any separate penalties that may arise from action taken by regulatory or prosecution authorities. Employees may also be subject to disciplinary action for failing to assist with the implementation of this Policy.

9. Policy Review

The Chief Legal Officer is responsible for the overall implementation, maintenance and upkeep of this Policy. This Policy will be reviewed regularly to confirm that it remains fit for its purpose and to ensure that it is being appropriately implemented.

10. Key Contacts

If you have any questions on this Policy, please contact:

Helen Franco – Chief Legal Officer, helen.franco@weareeverise.com

CONFLICT OF INTEREST POLICY

1. Objective

This Conflict of Interest Policy ("COI Policy") defines the parameters of Conflict of Interest for all the employees of Everise. Our employees shall always act in the interest of our company and ensure that any business or personal association does not create a conflict of interest with their roles & duties in our organization and will maintain the highest standard of ethics. This COI Policy defines and addresses the potential, apparent, and actual conflict of interest. It provides guidance to employees so that conflicts of interest are recognized to enable the concerned employee to take the necessary action as advised to resolve or avoid the conflict in an expeditious manner.

We have a zero-tolerance approach to conflict of Interest and are committed to act professionally and with integrity in all our business dealings and relationships. We uphold all the Laws relevant to conflict of interest in all the jurisdictions in which we operate. Our COI Policy aims to be more practical in its application and considers business ethics as its overall standards and objectives, considering the legislative requirements.

2. Scope

All employees and business associates of Everise, which includes outsourced personnel working in the company premises, consultants, suppliers, and vendors associated either directly or indirectly with the company.

3. Policy Guidelines

- This COI Policy is in addition to and should be read in conjunction with the Code.
- The company will circulate this COI Policy on conflicts periodically and provide a means for employees to disclose actual or potential conflicts.
- Conflict of interest may arise when an employee places his or her personal interests before the company's interests and where such personal interests unduly influence that employee's business judgments, decisions, or actions. The employee must not permit 'relationships with others' or 'external business activities' to conflict or appear to conflict, with the company's interests.
- The company respects all employees' rights to engage in activities outside the employment, provided such activities do not conflict with or reflect adversely on the company's interest or deprive the company of the appropriate measure of time and effort.
- The company requires all employees to avoid situations involving conflicts including, but not limited to, financial dealings that are contrary to the company's best interests, membership or employment relationships that may be in conflict, acceptance of

favors, money, or other considerations which might obligate the recipient to act adverse to the company's interest.

- The company will provide suitable mechanisms for resolving conflicts of interest so that the company's best interests will be protected while observing its standards of ethics.
- The COI Policy will be reviewed annually to ensure alignment with relevant legislation.

4. Definitions

Conflict of Interest: A 'conflict of Interest' means a potential, apparent or actual conflict where an employee's financial or other personal interest, whether direct or indirect, conflict or appears to conflict with the employee's responsibility to the company or with the employee's participation in any recommendation or decision with the company.

External Activity: It means any activity of an employee outside the scope of his/her employment with the company undertaken as part of a commercial or volunteer enterprise.

Relationships: Relationship means any relationship of the employee to a person of his or her immediate family, whether related by blood, adoption, marriage and any relationship of an intimate and/or financial nature during the preceding one year, any supervisor-subordinate relationship which is intimate in nature or between any two members which gives rise to a conflict of interest, or any other past or present relationship that may give rise to a reasonable apprehension of bias.

Supervisors: Supervisors means the person to whom employee reports, whether directly or indirectly.

Superior- Subordinate Relationship: Supervisor – subordinate relationship means a relationship in which one employee reports, whether directly and/ or indirectly, to the other employee.

Specific Conflict: A specific conflict of interest occurs when any undue influence is exercised to alter the materiality of an outcome to the benefit of one or all the parties involved in the situation.

Potential Conflict: A potential conflict of interest occurs when there is a divergence between an individual's private interests and his or her professional obligation to the company such that an independent observer might reasonably question whether the individual's professional actions or decisions are determined by considerations of personal interest, gain, financial or otherwise.

Actual Conflict: An actual conflict of interest depends on the situation and not on the individual's character or actions. Further, actual conflict involves a direct conflict between current duties and responsibilities and existing private interests.

Perceived Conflict: A perceived conflict of interest has the appearance of affecting an individual's professional judgment in exercising any company's duty or responsibility.

Third-Party: Any product supplier (insurer), any other financial services provider, any distribution channel (a company that assists with the sale of insurance products to the greater financial industry), and any other person or company that has a relationship with companies within the financial industry (other than suppliers and service providers defined below).

Supplier: Suppliers of services or goods to the company outside the insurance business, e.g., stationery, IT, accounting.

Financial Interest: This means any cash, cash equivalent vouchers, gifts, service, advantage, benefit, discount, domestic or foreign travel, hospitality, accommodation, sponsorship, other incentives or valuable consideration, other than an ownership interest and training, that is not exclusively available to a selected group of providers or representatives on

- Product and legal matters related to those products
- General financial and industry information
- Specialized technological systems of a third party necessary for the rendering of a financial service; but excluding travel and accommodation associated with that training.

Immaterial Financial Interest: This means any financial interest with a determinable monetary value, the aggregate of which does not exceed USD 10,000.00 in any calendar year from the same third party in that calendar year received by

- A provider who is a sole proprietor; or
- A representative for that representative's direct benefit
- A provider, who for its benefit or that of some or all of its representatives, aggregates the immaterial financial interest paid to its representatives.

5. Specific Situations of Conflict of Interest

This section sets out examples of the situations that shall be considered to create a conflict of interest, whether specific, actual, potential, or perceived:

- Engages in a business, activity, or relationship with anyone who is a party to a transaction with our company.

- Is in a position to derive an improper benefit, personally or for any family members or any person in a close personal relationship by influencing decisions relating to any transaction.
- Utilizing company time and/ or resources to promote personal interests or the interest of any person with whom the employee has a relationship.
- An employee or serving as a consultant to another similar business organization without the company's consent. The management must authorize permission to provide services to other similar businesses.
- "Dating," attempt to "date" and engaging in close emotional or physical relationships with a supervisor or other forms of romantic, intimate or physical or sexual contact with the supervisor.
- To influence the outcome of the appointment, hiring, promotion, supervision, or evaluation of a person with whom the employee has or has had a relationship.
- Directing an employee to carry out tasks of personal nature or for a company or firm in which the employee or a member of his/her immediate family has a financial interest.
- Having a source of income/ borrowing money from a vendor or supplier with whom the company conducts business or with one of the company's competitors.
- Conducting company business with whom the employee has a Relationship (as defined above) or with a business in which the employee or any person with whom the employee has a relationship has a significant interest.
- Accepting gifts, other personal obligations, or being entertained, which are substantial for him/herself or a family member from the client and/ or suppliers, whether local or foreign. Any gift so received, either in cash, bonds, stocks, or similar item or in-kind, should be shared among employees.
- Misusing information to which the employee has access due to his position, such as disclosing confidential information to competitors or others outside the business or using such information for personal use.
- Offering personal/unauthorized facilities/ services to customers rather than using the facilities/services provided by the company or its clients.
- Speculating or dealing with equipment, supplies, properties or materials or property purchased by the company or dealing with his/her own account on products sold by the company.

Apart from the above guidelines, other relationships or interests that might conflict with the company's best interests should also be disclosed.

6. Obligations of the Employees

- Employees are expected to avoid situations of conflict of interest, whether specific, actual, perceived, or potential as defined in the COI Policy
- Employees are responsible not to create circumstances that create an actual weakness or the appearance of a weakness in the company's system of internal controls
- External activities of any employee which has the effect of creating a Conflict of Interest, whether actual, specific, perceived, or potential, are strictly prohibited
- Any contract/agreement signed by the employee during the Investigation Period shall not bind to the company. He/ She shall not sign any contract or agreement on behalf of the company during the period between the commencement of investigation and completion of the investigation, proceeding ("Investigation Period") by the HR Department under this COI Policy.
- Employees shall not directly or indirectly engage in any business similar to that of the company which is directly/indirectly competitive with the business of the company as the owner, partner, agent, representative or as an employee of any person, firm, corporation or other entity.

7. Company Action

Upon receiving the report regarding the Relationships that have the effect of creating a Conflict of Interest, whether actual, specific, potential or perceived, HR shall develop a plan to manage or eliminate the conflict of interest within fifteen (15) working days. This plan shall document in writing the actions that shall be taken, including one or more of the following actions:

- Transferring either of the individuals to another department or geography
- Transferring the supervisor, decision – making and /or evaluative responsibilities
- Providing an additional layer of oversight to the supervisory role
- Taking any other action reasonably necessary to manage or eliminate the actual or potential conflict of interest and/or mitigate adverse effects
- In case alternate arrangements are not feasible, then the employer will have a choice to ask the employee to exit the company. The termination of employment shall be in accordance with the Exit Management Policy of the company and applicable law and shall not be constructed to be unjust and/ or unfair for any reasons whatsoever. Consequentially, the employee shall not be liable for any compensation/ settlement pecuniary or otherwise other than the past dues/salaries, which shall be settled in accordance with the procedure set out in the Exit Management Policy of the company and Local Labor Legislation.

8. Confidentiality of Disclosure

The company ensures that the disclosures made by the employees, whether in the Disclosure Statement or otherwise, are kept strictly confidential and are protected from misuse, within the requirements of the Law.

9. Policy Violation and Treatment

If an employee's Relationship:

- Has the effect of creating a Conflict of Interest, whether actual, specific, potential or perceived
- Interferes with the work of any employee
- Creates a harassing or hostile working environment for any employee
- Disrupts the smooth and orderly flow of work within the office, or the delivery of services to the company's clients or customers
- Harms the goodwill and reputation of the company among its customers or in the community at large

The employee who is responsible for such a problem will be subject to disciplinary action up to including termination/dismissal from the services.

Disclosure Statement
Conflict of Interest Disclosure Form

Directions: This form enables the employees to disclose and document all actual, specific, perceived, and/or potential conflicts of interest or conflicts of commitment thoroughly as specified by the company's Conflict of Interest Policy ("COI Policy").

As on -----, all employees, by signing this form, acknowledge their understanding of their responsibilities as outlined in this COI Policy

Name		Employee Id	
Band		Sub Band	
Date of Joining		Location	
Title		Department	

Section 1: Relationships

During the past twelve (12) months, have you participated directly/indirectly in a decision that provided benefits (e.g., hiring, transfers, promotions, performance appraisals, etc.) to persons related to you by blood, marriage, or members of the same household including domestic partners or persons with whom you have a personal relationship? If yes, kindly give a description of the nature of the relationship and the consequent Conflict of Interest, whether actual, specific, potential or perceived.

Section 2: Outside Employment And External Activities

During the past twelve (12) months, did you work as an employee, independent contractor, or consultant for any organization other than the company? If yes, please list all the activities below and nature of your relationship with that organization, i.e. name, the position held, tenure, and nature of work.

During the past twelve (12) months, did you have a management role in any organization other than the company? This includes, but is not limited to, service as an officer, board of director, manager, or any other supervisor at an organization other than the company for which you might or might not have received remuneration. If yes, please list all the activities below and nature of your relationship with that organization, i.e. name, the position held, tenure, and nature of work.

During the past twelve (12) months, have you either directly/indirectly engaged in any business or activity that is competitive with the company's business either as the owner, partner, agent, representative, or as an employee of any firm, company, or other entity? If yes, please list all the activities below and nature of your relationship with that organization, i.e. name, the position held, tenure, and nature of work.

During the past twelve (12) months, have you ever made decisions or have an authority to decide as part of the company with respect to any organization from which you have accepted gifts, favors, or any other monetary value, including and not limited to current or potential vendors or contractors of their agents? Exceptions include ordinary business

courtesies, such as payment for a meal or event, or acceptance of gifts that are promotional items without significant value and that are distributed routinely. If yes, please provide a brief analysis and description below of the real or potential conflict of interest or commitment regarding the company, nature of work & relationship, and value of the gifts/favors received.

Section 4: Gift Solicitation And Use Of company Resources

During the past twelve (12) months, have you taken gifts from contractors, vendors, local businesses, company departments, or others with whom there is a potential or ongoing professional relationship? If yes, please provide a brief description of the real or potential conflict of interest or commitment.

During the past twelve (12) months, have you accepted gifts from vendors, contractors, or others with whom there is a potential or an on-going professional relationship? The list includes but is not limited to travel expenses, meals, hotel accommodations or their reimbursement, etc. Exceptions include ordinary business courtesies such as payment for a meal or event or gifts, which are promotional items without significant value and which are distributed routinely. If yes, please provide a brief description of the real or potential conflict of interest or commitment.

During the past twelve (12) months, have you engaged in fundraising events with co-workers on behalf of any charitable organization? Exceptions are company-sponsored activities. If yes, then please provide a brief description of the real or potential conflict of interest or commitment.

During the past twelve (12) months, have you used your office equipment, supplies, computers, telephone, staff time for non – company-related activities? Exceptions include personal use of the telephone for local calls, emails, etc., that are incidental and kept to a minimum. If yes, please provide a brief description of the real or potential conflict of interest or commitment.

Section 5: Signatures And Review

Employee Signature:

By signing this form, you

- Certify that you have read the company's Conflict of Interest Policy;
- Certify that the information contained in this disclosure statement is complete and accurate to the best of your knowledge; and
- Acknowledge your continuing obligation to complete and submit a new Conflict of Interest Policy – Disclosure Statement when there is any actual or anticipated significant change in your outside activities or related financial interests.

Signature:

Date:

Violation of the company's Conflict of Interest Policy, including failure to complete this form, is considered a serious matter and may result in disciplinary action up to and including termination of employment

Review: After you have reviewed the Disclosure Statement, please check the appropriate statement, and sign below.

I have reviewed this disclosure form and determined that:

- The Individual has no material conflict of interest or commitment with regards to his/her responsibilities
- The individual had a material conflict, and the following description is how she/he will eliminate the conflict

Suggestions/Remarks:

Supervisor Name:

Date:

Supervisor Signature:

COMMUNICATION DEVICES & WORKPLACE TOOLS POLICY

1. Objective

The Communication Devices & Workplace Tools Policy (“CDWT Policy”) establishes guidelines on the use of communication devices, systems and networks in the workplace. The purpose of this CDWT Policy is to clarify how the company would provide monthly reimbursement of mobile bills based on the entitlements to the employees whose job requires the use of mobile phones to facilitate business. It also provides guidelines on issuing laptops as the role requires.

2. Scope

This CDWT Policy is applicable to Band 3 and above employees, except that sections 3.7 and 3.8 of this CDWT Policy apply to all employees.

3. Guidelines

3.1 Mobile Phones – Bring Your Own Device (BYOD)

- All employees are expected to use their own handsets and subscribe to individual mobile phone usage plans. All employees are expected to use their own handsets and subscribe to individual mobile phone usage plans. Employees of support functions in Band 4 may be eligible for this benefit, based on the requirement of the role and after obtaining approval from the department head, Chief People Officer.
- Entitlement for reimbursement are as follows:

Bands	Designation	Entitlement (Per Month)
Band 1	CXO/SVP/EVP	INR. 2,000.00
Band 2	VP/Sr. Director/Director	INR 1,500.00
Band 3	Sr. Manager/Manager/Asst. Manager & Lead	INR 1,000.00
Band 4	Specialists (Support Staff only)	INR 750.00

- The bills shall be paid by the employee and claimed back as “Reimbursement” on a monthly basis.
- If the bill exceeds the eligibility limits, then the employee also has to get it approved by his/her immediate supervisors & Department Heads.

International Service

- Employees on individual plans should contact their mobile carrier regarding available international plans and rates. International charges should be submitted on an expense report, provided you have prior approval from your manager.

- Whether on a company plan or individual plan, the following guidelines apply while travelling abroad:
 - Use local mobile phone connections.
 - Limit usage of cellular data (i.e.: email, Internet, etc.).
 - Turn off cellular data in your phone settings when not in use.
 - Limit usage of voice calling. Calling rates can vary per minute based on the country you are visiting and/or your wireless carrier.
 - Use Wi-Fi whenever possible.
 - Use Skype for Business or Microsoft Teams from your laptop whenever possible to make calls.
 - Use your wireless services as if you were paying the bill.
 - Employees are required to pay the bills and request reimbursement only for official calls on a monthly basis.
 - If the bill exceeds the eligibility limits, an employee is required to get approval from their immediate supervisor and department head.

3.2 Laptops & Desktops

- Windows-based laptops and desktops are the standard devices provided to all employee.
- Requests for non-standard devices requests must be approved by the Chief Technology Officer and Chief People Officer.
- Employees are responsible for maintaining current anti-virus definitions and security of the device.
- Employees must safeguard company data by applying strong passwords and automatic locking after periods of inactivity.

3.3 Privacy/Company Access

- No employee using his or her personal device should expect any privacy except that which is governed by law.
- The company has the right, at any time, to monitor and preserve any communications that use company networks in any way, including data, voice mail, telephone logs, and Internet use and network traffic, to determine proper use. Management reserves the right to review or retain personal and company-related data on personal devices or to

release the data to government agencies or third parties during an investigation or litigation.

- Management may review the activity and analyze use patterns and may choose to publicize these data to ensure that company resources in these areas are being use according to this CDWT Policy.
- Furthermore, no employee may knowingly disable any network software or system identified as a monitoring tool.

3.4 Policy Violations

- Employees who have not received authorization from management and who have not provided written consent will not be permitted to use personal devices for work purposes.
- Failure to follow company's policies and procedures may result in disciplinary action, up to and including termination of employment.

3.5 Risks/Liabilities/Disclaimers

- The company reserves the right to disconnect access to company systems or disable services without notification.
- Lost or stolen devices must be reported to the HR Department within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- The company reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this CDWT Policy.

3.6 Security of the Devices

- Employees are responsible for the security of their devices and the information stored on them. Employees must implement a passcode on any device containing or accessing Everise India data. Always carry the device with you; never leave them unattended.
- Lost or stolen devices must be reported immediately.

All company security policies apply regardless if the device is owned by the company or the employee.

3.7 Use of Cell Phones or Similar Devices

3.7.1 General Use at Work

While at work, employees are expected to exercise the same discretion in using cell phones. Excessive personal calls during the workday can interfere with employee productivity and be distracting to other employees. The company is not liable for the loss of personal cell phones brought into the workplace.

3.7.2 Unsafe Work Environment

The company prohibits employee use of cell phone or similar devices while at any work site at which the operation of such device would be a distraction to the work environment and/or create an unsafe work environment. Such work sites must be secured or the device used only by an employee who is out of harm's way

3.7.3 Confidentiality of Customer Information

- To further protect customers' sensitive information, the use of non-company issued cell phone equipment or any personal cell phones and recording devices (including, but not limited to, MP3 players, IPODs, cameras, camcorders, personal computers, PDA's, tablets, smartphones, smartwatches or any item that may store data in video, audio or text form, hereafter referred to collectively as "personal communication devices") during work hours is prohibited.
- All personal communication devices must be concealed and in the "off" mode (a status equivalent to the power supply removed from the device) during work hours and while an employee is logged into company systems.
- Employees who service accounts of the company's healthcare clients may be violating HIPAA if they use personal communication devices during work hours or logged into company systems.
- Employees may not use any cameras, video and audio recording devices, or video or recording features of cell phones, MP3 players or personal digital devices with wireless capabilities that can cause violations of privacy and breaches of confidentiality. Camera phones can present risks to the company by potentially compromising customer information.

3.8 Termination

- Upon termination of employment, whether voluntary or involuntary, all access to company systems and networks will be disconnected. For company-owned devices, services with the mobile carrier will be disconnected and all access will be disabled. All

company devices must be returned to the HR Department within seven days after the employee's termination date.

- Failure to return any company equipment in a timely manner may result in penalties. All access will be disabled and the company stipend will be terminated with respect to any personal communications devices used for company business.

ELECTRONIC MONITORING AND RECORDINGS POLICY

1. Introduction

Everise India is committed to protecting its confidential and proprietary information, as well as that of its clients. In addition, Everise India wants to ensure that its employees can openly communicate with one another and have the freedom to communicate without the fear of being secretly recorded without their consent. The Information Technology Act, 2000 ("IT Act") mandates the secure processing of personal information and prevention of misuse of information. Many clients require that Everise India maintain a cleanroom environment free of any electronic or recording devices to ensure the security and confidentiality of its operations. It is illegal for a person to record calls made to another person without obtaining the consent of such other person.

2. Electronic Recordings

Everise India employees, visitors, clients, vendors, or representatives acting on behalf of the company may not record conversations of another person without his or her prior knowledge and consent. Everise India Human Resources reserves the right to refuse any request to make recordings of any communication or release any authorized recordings, unless otherwise made in accordance with applicable laws or court processes. Recordings may include audio, video, webcam by any means, including smart phones.

3. Electronic Monitoring

All employees, during work shifts, are subject to being recorded by the company in all company locations, including while working at home at their desktops on behalf of company clients, as a condition of their employment. This Electronic Monitoring and Recordings Policy shall not limit the right of Everise India or its clients' right to install and use security cameras or webcams for the purpose of monitoring the employee's safety and work performance subject to limitations provided by data privacy laws, rules and guidelines.

A violation of this Electronic Monitoring and Recordings Policy may result in disciplinary action, up to and including termination of employment.

DRUG-FREE WORKPLACE POLICY

1. Purpose

Everise India intends to maintain a safe, productive, and comfortable drug-free workplace for employees, applicants for employment, clients, and customers. With this in mind, Everise India has established this drug-free workplace policy (“**Drug Free Policy**”).

2. Definitions

For the purposes of this Drug Free Policy, the term restricted substances refer to all abused substances, whether inhaled, injected, or swallowed, including, but not limited to:

- Alcohol, such as beer, wine and hard liquor;
- Illegal drugs, such as marijuana, hallucinogens, cannabis, club drugs (also known as rave or party drugs such as Ketamine, Ecstasy and Rohypnol) and cocaine;
- Non-prescribed prescription medication, such as painkillers and barbiturates; and
- Inhalants, such as glue, paint thinner, petrol and hair spray.

3. Applicant Drug Testing

Applicants will sign a written consent form and submit to a drug testing procedure, free of charge, as a condition of employment. If an applicant tests positive for cannabis, the results will be reviewed by the HR Director of Compliance on a case-by-case basis.

4. Prohibited Behavior

Everise India explicitly prohibits the use, possession, solicitation, offer for sale or being under the influence of restricted substances during work hours, including lunch and breaks, or on company property at any time. Employees are in violation of the Drug Free Policy if they:

- Are impaired or under the influence of restricted substances while working for the company, on or off the premises;
- Report for duty in an altered or impaired condition, as the result of the use of restricted substances; or
- Have impaired reflexes or reaction time or suffer from drowsiness due to adverse side effects from the use of a prescribed drug while working for the company, on or off the premises;

- Are convicted of any local, federal, state or municipal criminal drug statute, and fail to report the conviction to their supervisor within five (5) calendar days of the occurrence.

5. Employee Drug Testing

Everise India reserves the right to set standards for employment and may require employees, as a condition of continued employment, to submit to drug testing under the following circumstances:

Reasonable Suspicion Testing - Where there is a reasonable suspicion that an employee is under the influence of a restricted substance, including but not limited to:

- Direct observation of use of a restricted substance;
- Evidence of drugs or alcohol on or about the employee's person or work area;
- A significant deterioration in work performance that suggests impairment;
- Symptoms of being under the influence of a restricted substance, such as abnormal or erratic behavior or changes in physical appearance.
- A report of use of a restricted substance, provided by a reliable and credible source; or
- Newly discovered evidence that the employee has tampered with a prior drug test result.
- **Post-Accident Testing** - Employees involved in an on-the-job accident, especially those for which the employee is deemed at fault.
- Reasonable suspicion testing needs prior approval from the HR Director of Compliance.

6. Refusal to Test

Any employee who refuses a request to submit to testing under this Drug Free Policy may be subject to disciplinary action, up to and including termination. Attempts to alter, substitute or tamper with the collection of the specimen or failure to appear for testing will be deemed a refusal to take the drug test. A refusal to take a test shall include the following:

- fails to appear for any test within a reasonable time, as determined by Everise India after being directed to do so;
- fails to remain at the collection site until the testing process is complete;
- fails to provide urine specimen when required for a drug test or a breath specimen for an alcohol test;

- fails to provide a sufficient amount of urine or breath when directed, and it has been determined, through a required medical evaluation, that there was no adequate medical explanation for the failure;
- declines to take a second test as directed;
- fails to undergo an evaluation, as directed by the medical personnel and/or management representative as part of the verification process or as directed by Everise India as part of the shy bladder procedures or insufficient breath situation;
- fails to cooperate with any part of the testing process; or
- fails to immediately report a job-related accident for the purpose of avoiding testing.

Inspections

Please review our Search, Inspection, and Investigation Policy in this Employee Handbook.

Confidentiality

The results of any drug test will constitute medical information and will remain confidential in accordance with the IT Act. All information, interviews, reports, and statements received by Everise India as part of this policy are confidential communications. Unless authorized by law, Everise India will not release such information without a signed written consent form signed by the person tested.

Test Results

Everise India will attempt to ensure that all aspects of the testing process are as private and confidential as reasonably practical. Actual test results will be provided to:

- Any medical personnel supervisors and managers who have a need to know such information;
- the associate tested upon written request;
- any person permitted or required by law or regulation to receive such information;
- any individual with an associate's written authorization; to law enforcement;
- the decision maker(s) in a legal action initiated by or on behalf of the employee or placed at issue by the associate in any legal, administrative, or other proceeding; or
- to any governmental agency or contractor as required by the governing laws in India. Non-specified statistical information may be provided upon request to a corporation, which requires its vendors or subcontractors to maintain drug and alcohol testing

programs in accordance with a contract, or to governmental agency in accordance with the law.

7. Disciplinary Action

The severity of the disciplinary action taken against an employee found to violate this Drug Free Policy will depend on the circumstances of each case. However, any violation of this Drug Free Policy may be subject to disciplinary action, up to and including termination.

8. Voluntary Employee Assistance and Rehabilitation

Everise India supports employees in seeking assistance, including counseling and rehabilitation services. Everise India encourages the use of Paid Time Off (PTO) or leave without pay, for purposes of bona fide rehabilitation efforts. Participation in employee assistance and rehabilitation programs is confidential. Everise India will not use the employee's voluntary participation in a program as a basis for corrective action, nor will participation in such a program jeopardize employment or advancement opportunities. However, participation will not protect employees from disciplinary action for continued unacceptable job performance or rule violations.

9. Time Off

An employee with Everise India's medical certification documentation from a licensed health provider may request a leave of absence to obtain treatment for substance abuse if such treatment is required and undertaken. The granting and returning from medical leave are subject to the company's Leave Policy. To discuss an accommodation, please contact Human Resources.

10. Supervisory Responsibility

Supervisors play an important role when it comes to helping employees with substance abuse problems. They are in direct contact with employees and, therefore, are more likely to detect issues such as changes in mood or behavior that may indicate substance abuse. Supervisors who suspect that an employee is under the influence of a restricted substance have the responsibility to:

- Inform employees of the Drug-Free Workplace Policy;
- Investigate reports of dangerous practices or suspicious behavior;
- Observe and document changes and/or problems in employee performance and behavior;
- Counsel employees as to expected performance improvement;
- Clearly state consequences of Drug Free Policy violations; and

- Contact the Human Resources Department for further assistance.

11. Employee Responsibility

While the use of medically prescribed or over-the-counter medications does not necessarily violate this Drug Free Policy, employees should not take prescription or over-the-counter medication that impairs their ability to perform their job or creates a safety hazard. If they must take medication that adversely affects their job performance, they should seek advice from the Human Resources Department about possible time off or accommodation. Additionally, employees aware of substance abuse by another employee should report this information to their immediate supervisor or the Human Resources Department.

12. Discipline for Policy Violations

Everise India employees who violate this Drug Free Policy, will subject the employee to disciplinary action up to and including termination. Employees may not avoid imposition of discipline by first requesting such treatment of a leave of absence after being selected for testing or violating Everise India policies.

- **Refusal to Test.** Additionally, a candidate or employee who refuses to submit to alcohol or drug screening will be considered as having tested positive and may be removed from employment consideration or subject to discipline, up to and including termination.
- **Referral to Law Enforcement.** In addition to imposing discipline discipline, Everise India may refer information and any suspected illegal drugs or illegal drug paraphernalia to law enforcement.
- **Automatic Suspension.** In the event that an employee is suspected of violating this Drug Free Policy or is ordered to submit to a post-accident or reasonable suspicion test, the employee will be suspended from duty without pay until the test result is received. If the test result is positive, then the employee is subject to discipline as described herein.
- **Applicants.** If a pre-employment test result is positive or if the individual refuses to submit to a pre-employment test, then Everise India shall treat the individual as having withdrawn his/her application and it shall withdraw its conditional offer of employment.

13. Employer Right to Amend Policy

Everise India reserves the right to amend, delete or revise parts of this Drug Free Policy at any time.

EQUAL EMPLOYMENT OPPORTUNITY POLICY

1. Objective

To provide equal employment opportunity to all qualified individuals regardless of the individual's race, color, gender, gender identity, sexual orientation, religion, national origin, age, disability, or any other protected class status provided by the respective equal employment opportunity law applicable in the country. It is the company's policy and practice to provide an environment which provides equal opportunities at employment devoid of any form of discrimination. The company shall not discriminate on any ground, including race, caste, religion, colour, ancestry, marital status, gender, sexual orientation, age, nationality, ethnic origin, disability or any other category protected by applicable law.

2. Coverage

All employees of the company and temporary or contractual personnel working in the company premises.

3. Salient Features

All employees & all applicants for employment with the company will be treated equally in all respects. This Equal Employment Opportunity Policy ("EEO Policy") applies to all aspects of employment, including, but not limited to:

- Job advertising, recruiting, and hiring
- Compensation and benefits
- Job assignments, promotions & transfers
- Training activities
- Layoffs, disciplinary procedures, and termination of employment
- Use of all company facilities

3.1 Responsibility

- The HR Department is responsible for compliance with this EEO Policy as overseen by the Chief People Officer.
- Any employee who is aware of any act or allegation of discrimination will report the incident via his/her supervisor or through the 'Complaint Reporting Procedure' mentioned below.
- As an integral part of the supervisor's responsibility, each supervisor shall ensure that there is no discriminatory conduct against a fellow colleague/peer/subordinate/supervisor.

- Any supervisor who is aware of an action or allegation of discriminatory treatment but fails to report the incident is subject to disciplinary action, up to and including termination of employment.

3.2 Complaint Reporting Procedure

- Employees are encouraged to resolve complaints with their immediate supervisor. However, if the employee prefers, he/she may file a verbal or written complaint with the Human Resources Department.
- A description of the offending conduct should be given, including the date of the incident and the name of the person accused, to the Site HR Manager.
- Every complaint will be investigated, and a decision will be made upon assessing the best method of handling the issues raised.
- Disciplinary action may be taken to ensure an effective resolution.
- The complainant will be informed about the results of the investigation.
- In cases when the results of the investigation are inconclusive or when a reasonable doubt remains as to whether the conduct complained of violates this EEO Policy, both employees will receive counselling concerning the appropriate standard of conduct.

3.3 Non – Retaliation Policy

Neither the company nor any employee will retaliate against another employee who has provided information or cooperated with the investigation of discrimination or harassment. If instances of retaliation are proven, management will take appropriate disciplinary action against the offending party.

ANTI-HARASSMENT, DISCRIMINATION, AND RETALIATION PREVENTION POLICY

1. The company is committed to providing all our employees with a work environment free of discrimination, harassment, and/or retaliation of any kind.
2. No employee will be subjected to any harassment because of age, race, religion, color, sex, national origin, disability, military or marital status, sexual orientation, gender identity, or any other category protected by federal, state, or local laws. Any form of discrimination, harassment, and/or retaliation will not be tolerated.
3. Harassment may take several forms, such as degrading comments, intimidation, offensive material, emails, or language, or other verbal, visual, or physical conduct of a sexual, racial, ethnic, religious, disability-related, or age-related nature, which could create a hostile, intimidating, or offensive work environment. Such discrimination, harassment, or retaliation is intolerable, a violation of the company's Anti-Harassment, Discrimination, and Retaliation Prevention Policy, and will result in an appropriate discipline, up to and including termination.

Examples of harassment in violation of this Anti-Harassment, Discrimination, and Retaliation Prevention Policy may include, but are not limited to:

- Degrading or inappropriate comments of a sexual, ethnic, racial, ageist, religious, or disability nature.
 - Unwelcome sexual flirtations, advances, or propositions.
 - Offensive materials, emails, text messages, instant messages, or the language of a sexual, ethnic, racial, age, religious, or disability nature.
 - Touching, hugging, pinching, patting, or brushing against another person's body.
 - A display in the workplace of sexually suggestive objects or pictures.
 - A threat or action that makes the affected individual's employment, work-related opportunities, or benefits subject to the submission of sexual demands.
 - Retaliation, harassment, discrimination, or intimidation against employees who make complaints of harassment.
4. Any sexual advances or personal relationships between a supervisor and subordinate are prohibited.
 5. If you believe you have been harassed, observe incidents of harassment, or believe you have been retaliated against, you should immediately report the alleged incident to the Human Resources Department. Incidents should be reported as soon as possible so we may begin a prompt investigation.

6. All claims of harassment and retaliation will be thoroughly investigated objectively, and all information obtained will be kept as confidential as possible.
7. Please do not assume the company is aware of your problems. Please bring your complaints and concerns to our attention so we may resolve them. Your complaints can be brought to the Internal Complaints Committee (as set out under the Anti-Sexual Harassment Policy below).
8. Violations of this Anti-Harassment, Discrimination, and Retaliation Prevention Policy will not be permitted and will result in discipline up to and including termination.

ANTI-SEXUAL HARASSMENT POLICY

1. Purpose

The purpose of the Everise Anti-Sexual Harassment Policy ("**Prevention of Sexual Harassment Policy**" or "**POSH Policy**") is to ensure all employees understand that Everise has a zero-tolerance policy for sexual harassment in the workplace.

2. Description of conduct that constitutes harassments

Sexual harassment is unwelcome sexual conduct that is a term or condition of employment. Unwelcome sexual advances, requests for sexual favors, & other verbal or physical conduct of a sexual nature constitute sexual harassment when:

- a. Submission to such conduct is made either explicitly or implicitly a term or condition of an individual's employment
- b. Submission to a rejection of such conduct by an individual's employment
- c. Submission to or rejection of such conduct by an individual is used as the basis for employment decisions affecting such individual; or
- d. the conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile, or offensive working environment.

Any of the following could, if part of a pervasive pattern of abuse, constitute sexual harassment:

- Jokes, innuendos or gestures of a sexual nature;
- Sexually-charged computer programs, emails or messages;
- Demeaning language or behavior that is based on sex;
- Compliments about a person's body of a sexual nature;
- Repeated requests for a date despite refusals;
- Unwelcome sexual advances;
- Requests for sexual favors;
- Questions or comments about personal or intimate sexual matters;
- Hugs, kisses, neck rubs, or back rubs;
- Deliberately brushing up against someone else;
- Sexual epithets or name-calling;

- Sexually intimidating behavior or ridicule;
- Objects, pictures, photographs, or cartoons of a sexual nature;
- Other verbal or physical harassment of a sexual nature.
- Requesting sex for something such as better job opportunities, advancement etc... (Quid Pro Quo)

3. Zero Tolerance

Everise is committed to providing a workplace free from sexual harassment. As such, Everise will not tolerate harassment of any of our employees or independent contractors by supervisors, co-workers, customers, vendors, agents and any other third parties.

4. Compliant Procedure

In the course of any such investigation, Everise will take appropriate measures to maintain the confidentiality of the participants to the extent possible. Although it may be necessary to divulge some information to ensure that a fair investigation is conducted, Everise will limit information to only those persons with a need to know of the complaint or of the investigation.

5. No-Retaliation

All parties contacted in the course of a sexual harassment investigation will be expressly reminded that Everise will not tolerate retaliation in any form against any employee who believes or is concerned that sexual harassment has occurred and reports such conduct pursuant to this POSH Policy. Moreover, Everise will protect any employee who participates in any sexual harassment investigation from any resulting retaliatory conduct. If an employee believes that they are experiencing retaliation as a result of having made a complaint pursuant to this policy or having participated in a sexual harassment investigation, the employee must promptly report the facts and names of the individuals involved to their leadership or Human Resources.

6. Discipline for Harassment

If an investigator concludes that conduct in violation of this policy has occurred, the offending individual(s) will be subject to corrective action, including formal discipline, up to and including termination of employment. Please note that POSH Policy may be construed to be more protective of employees than the law requires. Regardless, Everise will discipline any individual who violates this policy even if such conduct does not rise to the level of violation of the law.

7. Formal Training

To ensure that Everise's employee remain unchanged about their obligations under this POSH Policy, Everise will require all employees to periodically receive training regarding our zero-tolerance for sexual harassment at work.

8. Internal Complaints Committee

In furtherance of this POSH Policy, an internal complaints committee ("**Committee**") will be constituted by the company to address all cases/complaints of alleged harassment (including sexual harassment) submitted by an aggrieved employee(s) ("**Complainant**") or take action *suo moto*, in the absence of a Complaint being submitted by the Complainant to prevent harassment within the outlined framework. The company may set up sub-committees or engage external agencies to investigate such Complaints of harassment as the company may deem fit. The Committee shall also have power to direct the transfer of any matter/case from one sub-committee to another or to the Committee itself. The Committee will consist of the following members:

- (a) A presiding officer, who shall be a senior female employee nominated from amongst the employees at the workplace, or in the absence of such an employee within the workplace, from another branch or department of the workplace, or from any other organization or workplace of the same employer;
- (b) In addition to the presiding officer, there shall be at least two (2) members from amongst the employees preferably committed to the cause of equal rights for female employees or who have had previous experience in social work or have legal knowledge; and
- (c) One (i) member from amongst non-governmental organizations or associations committed to equal rights for female employees or a person familiar with the issues relating to sexual harassment in the workplace.

Provided that at least one-half of the total members of the Committee so nominated shall be women.

ANTI-DISCRIMINATION ON THE BASIS OF GENDER, GENDER IDENTITY OR TRANSGENDER STATUS POLICY

Everise India prohibits discrimination against and/or harassment of applicants, employees, and interns based on their actual or perceived gender or actual or perceived status as an individual who is transgender, gender non-conforming or intersex. For purposes of this Anti-Discrimination on the Basis of Gender, Gender Identity or Transgender Status Policy, gender includes gender identity, self-image, appearance, behavior, or expression. Harassment includes, but is not limited to, violence, threats of violence and similar conduct.

The company evaluates all requests for reasonable accommodations, including requests for medical leave or schedule changes, changes to the terms and conditions of employment, program participation or use of a public accommodation in a non-discriminatory manner. The evaluation includes, but is not limited to, treating leave requests for medical or health care needs related to an individual's gender identity in the same manner as requests related to other medical conditions.

Employees who engage with the public as part of their job duties are required to conduct themselves in a respectful, non-discriminatory manner by respecting gender diversity and ensuring that members of the public are not subject to discrimination (including discrimination with respect to single-gender programs and facilities). A transgender person shall have a right to be recognised as such, in accordance with the provisions of The Transgender Persons (Protection of Rights) Act, 2019. A person recognised as transgender shall have a right to self-perceived gender identity. The gender of transgender person shall be recorded in all official documents in accordance with certificate issued by District Magistrate.

Preferred Names, Titles and Pronouns

Everise India allows employees to self-identify their names and genders and will use an individual's preferred name, gendered title (e.g., Mr./Ms.) and pronoun (e.g., he/him/his; she/her/hers; they/them/theirs; or ze/hir). Requests to be addressed by a certain name and/or pronoun do not require supporting documentation. If an employee is unsure what name, title, or pronoun another individual prefers, the employee should not hesitate to ask the person their preferred method of being addressed.

Facilities Designated as Single-Gender

All employees have the right to use restrooms consistent with their gender identity or transgender status.

Dress Code

Everise India's dress code and grooming standards are gender neutral, meaning they do not differentiate or impose restrictions or requirements based on gender or sex. All Everise India employees should dress professionally at Everise India facilities and be aware of any

safety concerns regarding their choices; for example, footwear that may cause injury. This said, the list below will serve as a guide to acceptable business casual dressing at work:

Casual Business Attire	
Acceptable	Not Acceptable
Any item in the business casual list	Clothing that works well for the beach, yard work, dance clubs
T-shirts/Collarless shirt, sweatshirts, Sports shirts, sweatshirts, sport team jackets, and athletic socks.	Clothing that reveals too much cleavage, back, chest, stomach, Haltered or spaghetti-strapped blouses, off-shoulders, backless
Ankle length pants, Jeans/ Denim/Capris	Leggings, sweatpants, spandex and the likes
Athletic shoes and sandals	Hats or caps

Reporting and Anti-Retaliation

Employees with questions or concerns regarding their safety, gender discrimination and/or a request for a reasonable accommodation, or who feel they have been subjected to discrimination or improperly denied an accommodation, should contact their Human Resources representative, or consult the Whistleblower Policy in this Employee Handbook.

Everise India prohibits and does not tolerate retaliation against employees who report issues or concerns of gender discrimination in good faith pursuant to this Anti-Discrimination on the Basis of Gender, Gender Identity or Transgender Status Policy.

DIVERSITY, EQUITY AND INCLUSION POLICY

Everise is committed to fostering, cultivating and preserving a culture of diversity, equity and inclusion.

At Everise, we understand the value diversity has not only in the workplace, but on our ability to empathize with our customers and deliver world-class customer experiences. We celebrate all cultures for their uniqueness and strengths. We believe that great things will happen when we work with people who think differently from us.

We recognize and appreciate the importance of creating an environment in which all of our team members feel valued, included and empowered to do their best work and bring great ideas to the table in service to our culture and way of life. Through thought leadership, we create empowering experiences that results in mutual trust and engagement between our valued employees, our clients, and our customers.

We embrace and encourage our employees' differences in age, color, disability, ethnicity, family or marital status, gender identity or expression, language, national origin, physical and mental ability, political affiliation, race, religion, sexual orientation, socio-economic status, veteran status, and other characteristics that make our employees unique.

Everise diversity initiatives are applicable—but not limited—to our practices and policies on recruitment and selection; compensation and benefits; professional development and training; promotions; transfers; social and recreational programs; layoffs; terminations; and the ongoing development of a work environment built on the premise of gender and diversity equity that encourages and enforces:

- Respectful communication and cooperation between all employees.
- Teamwork and employee participation, permitting the representation of all groups and employee perspectives.
- Work/life balance through flexible work schedules to accommodate employees' varying needs.
- Employer and employee contributions to the communities we serve to promote a greater understanding and respect for the diversity.

All employees of Everise have a responsibility to treat others with dignity and respect at all times. All employees are expected to exhibit conduct that reflects inclusion during work, at work functions on or off the work site, and at all other company-sponsored and participative events. All employees are also required to attend and complete annual diversity awareness training to enhance their knowledge to fulfill this responsibility.

Any employee found to have exhibited any inappropriate conduct or behavior against others may be subject to disciplinary action.

Employees who believe they have been subjected to any kind of discrimination that conflicts with the company's diversity policy and initiatives should seek assistance from a supervisor or an HR representative.

HUMAN RIGHTS POLICY

Everise believes in the principles of equality and non-discrimination. Everise is committed to treating all individuals with respect and dignity, and work to use our influence and business relationships to promote the opportunity for all people throughout our value chain to exercise and enjoy fundamental human rights. This Human Rights Policy (“**HR Policy**”) outlines the Everise commitment to respect the Principles on Business and Human Rights.

Everise aims to act as a role model for the business community. One aspect of this is ethical conduct as expressed through the Business Code of Conduct. The Business Code of Conduct includes our commitments to:

- Follow high standards of ethical conduct;
- Work with clients, suppliers, and subcontractors that live up to Everise’s core ethical standards;
- Act lawfully, ethically, and in the public interest;
- Champion an inclusive and collaborative culture that is free from bullying, discrimination, and harassment, where everyone is treated with respect and dignity.

Respect for Human Rights

Respect for human rights is a fundamental value of Everise. We believe in the principles of equality and non-discrimination, and we are committed to treating all individuals with respect and dignity, and work to use our influence and business relationships to promote the opportunity for all people throughout our value chain to exercise and enjoy their fundamental human rights. We also recognize the interdependence of human rights and the environment – particularly as it relates to land and natural resources and the importance of the people whose livelihoods depend on the ingredients we source.

Fair and Humane Working Environment

Everise provides a workplace free of harassment, discrimination, harsh and inhumane treatment. Any abusive behavior such as sexual harassment, corporal punishment, mental or physical coercion, or verbal abuses or threats among employees shall not be tolerated.

Discrimination for reasons of race, age, gender, gender-orientation, ethnicity, disability, religion, political affiliation, union membership or marital status shall not be condoned.

Safe and Healthy Workplace

The safety and health of our employees is of paramount importance. Our HR Policy is to provide a safe and healthy workplace and comply with all applicable laws and Local safety and health laws, as well as internal requirements. We work to provide and maintain a safe, healthy and productive workplace, in consultation with our employees, by addressing and remediating identified risks of accidents, injury and health impacts.

Freely Chosen Employment

We are committed to ensuring all work is voluntary. We take meaningful steps to prevent the use of forced, bonded or indentured labor, involuntary prison labor, slavery or human trafficking in our workplaces and throughout our supply chain.

Child Labor Inside our organization

Child labor will not be used under any circumstances. All employees must meet the minimum age requirement set by local laws. We intend to continue improving identification of and elimination of child labor in our supply chain.

Minimum Wage, Hours and Benefits

We are committed to compensating our employees competitively relative to the industry and local labor market. We operate in full compliance with applicable wage laws, including those relating to minimum wages, overtime hours and legally mandated benefits. Working hours for our employees shall be limited to what is permitted by local laws.

Privacy and Data Protection

Everise respects individuals in a manner consistent with the rights to privacy and data protection. Information about people, including its employees, shall be used appropriately for necessary business purposes, and shall be protected from misuse to prevent undue harm to individuals such as discrimination, stigmatization or other damage to reputation and personal dignity, impact on physical integrity, fraud, financial loss or identity theft.

Key Responsibilities

Everise leaders, managers and employees have a personal responsibility for the application of this HR Policy on a day-to-day basis. This means they should not undertake any acts of discriminatory practice in the course of their employment. Furthermore, all Everise employees should positively promote high equality standards in the course of their employment wherever possible.

Finally, all staff have a responsibility to bring any potentially discriminatory practice to the attention of either their Line Manager, the Human Resources Department or the Whistle blower Hotline.

Expectations

Everise Team Leaders, Supervisors, Managers, and Executives should be aware that they will be expected to positively promote high equality standards. Everise leadership will ensure that all employees of Everise are accountable for the promotion and implementation of this HR Policy. We will monitor progress on equality and diversity issues and initiatives on a regular basis and will ensure the implementation of any relevant actions points and plans concerning equality and diversity issues.

Everise is committed to fundamental Human Rights in all Everise subsidiaries and communities where we operate. We want to achieve the right results, the right way by:

- having the courage to lead.
- communicating openly and transparently.
- committing to and support each other.
- promoting and protecting quality outcomes.
- honoring our past while we proudly pursue our future.

Everise's commitment to human rights embodies and reflects these values as they influence everything we do and serve as the guiding principles that drive our company every day. Where appropriate, we engage in dialogue with stakeholders on Human Rights issues related to our business and the communities where we operate.

Process for Implementation

Everise and its subsidiaries are expected to follow the spirit and intent of our guiding principles to ensure respect for Human Rights. These principles are an integral part of other related policies, including the Business Code of Conduct.

If any employee believes that someone is violating the Human Rights Policy or the law, they are asked to report it to their Human Resources Department or the Whistleblower Hotline where a formal review will be conducted regarding the concern.

A copy of this policy will be provided internally and externally. It will be communicated to our employees, and suppliers.

DATA PROTECTION & PRIVACY POLICY

(attached separately)

HEALTH, SAFETY & ENVIRONMENT POLICY

1. Objective

To provide quality workplace conditions that foster a safe and secure environment for the company's employees, customers and visitors, and safeguard its facility from intruders, theft, violence or any other danger.

2. Scope

All company employees and temporary or contract personnel working on company premises.

3. General Guidelines

a. *Employee Identification Badge*

- For security purposes, employees are issued an ID/security badge on their first day of employment.
- All employees, regardless of their position, must present their ID/security badge upon entering any company facility. ID/security badges must be worn and clearly visible at all times while on company premises. ID/security badges should be worn above the waist.
- The ID/security badge allows employees to enter secured areas required by their job. All employees should carry authorized ID and access badge to enter the facility and their work areas. Tailgating or piggybacking through a secure entrance behind another employee and not swiping their access badge each time they enter their authorized area is strictly prohibited.
- Employees are responsible for their ID/security badges. There is a replacement cost for lost ID/security badges. Under no circumstances is an employee to use another employee's ID/security badge. If an employee forgets their ID/security badge, a temporary one for use that day may be issued by Security upon receipt of approval from their supervisor or HR. Temporary ID/security badges must be returned by the end of the day. There is a replacement cost for unreturned temporary ID/security badges. The maximum use of a temporary ID/security badge by any employee is three (3) consecutive days, after which the employee will be required to pay the cost for a replacement badge.
- Failure to adhere to the ID/security badge control procedures may be cause for disciplinary action, up to and including termination.

b. ***Security Inspections***

- The company maintains a work environment free of illegal drugs, alcohol, explosives, weapons, and other improper materials. The company prohibits the possession, transfer, sale, or use of such materials on its premises. The company requires the cooperation of all employees in administering this Health, Safety & Environment Policy (“**HSE Policy**”). Desks and other storage devices are provided for the convenience of employees but remain the sole property of the company. A manager with a member of the Human Resources Department present may inspect a storage device, as well as any articles found within, at any time, either with or without notice.
- Theft or unauthorized possession of the property of other employees, visitors, or customers is strictly prohibited. The company will pursue violators to the fullest extent of the law. To enforce this HSE Policy, the company or its representative may inspect desks and storage cabinets, persons entering and/or leaving the premises, and any packages or other belongings.

c. ***Clean Workstation and Operations Floor Policy***

- In general, paper of any kind is not permitted on the production floor including, but not limited to, newspapers, notebooks, loose leaf paper, paperback books, and crossword puzzles.
- Client-specific paper such as logs, downtime forms, flash training notices, etc., or company-specific paper such as timesheets, login/out reports, QA scan forms, etc., may be permitted according to client requirements or at the discretion of management.
- No handwritten notes may be made at the workstation.
- Limited personal belongings are allowed on the workstation desktop.

d. ***Work Related Injuries***

- All employees are protected by the statutory workers' compensation insurance policy while employed by the company. Coverage is available at the prescribed statutory scheduler deducted cost to the employee and covers injury or illness resulting from legitimate work activities while the employee is working on company premises, working from home, traveling on official company business or attending a company activity.
- It is the responsibility of the employee to notify their manager and the HR Department each time they are involved in or witnesses an accident or safety incident.

- An employee injured on the job, even if medical assistance is not sought, must immediately notify a supervisor, regardless of the severity of the injury. A report of the injury will be completed promptly by the employee and supervisor and submitted within twenty-four (24) hours to the Human Resources Department.
- Failure to report an accident or safety incident is a serious matter, the authorities may impose a penalty if such incidence are not reported on time.
- Employees are to receive authorization from the Human Resources Department prior to seeking medical attention for any work-related injury or illness. In emergency situations requiring immediate medical attention, the employee should seek treatment and submit any associated documentation to their Human Resources Department upon their return to work.
- Everise India does not require managers or employees to be first aid responders, but care and concern for an injured employee is very important. When in doubt, please use 999 for emergencies.

e. ***Violence in the Workplace***

- The safety and security of the company's employees, customers, vendors, contractors and visitors are of vital importance. Therefore, acts of violence made by an employee against another person's well-being will not be tolerated. Employees found guilty of acts or threats of violence will be subject to discipline, up to and including termination of employment.
- In accordance with this HSE Policy, employees are required to report to management personnel any behavior that compromises the company's ability to maintain a safe work environment.
- It is everyone's responsibility to prevent violence in the workplace. Employees can help by reporting what they see in the workplace that could indicate that a coworker is in trouble. No one is expected to endanger their own life or health to help others.

f. ***Weapons***

- The possession or use of any, fireworks, explosives, knives or other dangerous weapons of any kind on company premises is prohibited.
- Employees found with such items will be subject to disciplinary action, up to and including immediate termination of employment.

g. ***Workplace Monitoring***

- The company reserves the right to install surveillance cameras for legitimate business purposes, such as ensuring security or preventing theft, except in areas where privacy is necessary, such as restrooms or changing areas. However, employees should not have an expectation of privacy on company premises, especially in common or public areas.
- The unauthorized recording of conversations, meetings, or other interactions without the knowledge of those recorded may be illegal, and anyone who does so may be subject to disciplinary action.

h. ***Inspections and Privacy Expectations***

- The company maintains a work environment which is free of illegal drugs, alcohol, explosives, weapons, and other improper materials. The company prohibits the possession, transfer, sale, or use of such materials on its premises. In addition, theft or the unauthorized possession of the property of other employees, visitors, or customers is strictly prohibited.
- To ensure the safety and confidentiality of the employees, clients, and visitors, the company reserves the right to inspect company-supplied property, including, but not limited to, company-issued cellular phones, offices, desks, file cabinets, computers and software, company vehicles, lockers, and other storage facilities, are subject to inspection by managers at any time, with or without notice. Employees should have no reasonable expectation of privacy in property owned and/or supplied by the company.
- Employees may be permitted to store personal items in company facilities. However, the company is not responsible for loss, damage or theft of employees' personal belongings; employees should exercise discretion in storing any personal items on company premises.
- The company reserves the right to search all packages, containers, purses, briefcases, backpacks, lockers, desks or persons entering or located on company premises. Any violation of this HSE Policy, including refusal to promptly permit a search, will result in disciplinary action, up to and including termination.

i. ***Employee Responsibilities***

- Employees are responsible for the security of their workstation. Any information that needs to be left at the workstation, such as useful telephone numbers, helpful instructions, or tips, will be laminated by operations management.

- Personal belongings may not be accessed from the production floor. Personal items such as backpacks, lunches, purses, etc., must never be placed on the workstation desktop. These items must be stored in a locker or placed underneath the desk. Please be aware some lines of business require all personal possessions be stored in lockers.
- Any client-specific paper must be turned over to the manager at the end of a shift.
- The company may provide lockers for storage of employee personal items but assumes no responsibility for any loss associated with their use. Employees are responsible for securing lockers with their own lock. The company reserves the right to inspect any locker contents at any time, with or without notice to the employee. Employees should have no expectation of privacy with regards to the contents of their lockers. Storage lockers may only be used while an employee is logged in and working at the location. Lockers must be cleared out and the personal lock removed after the employee's shift ends. The company reserves the right to remove locks remaining on lockers after shifts have ended.
- Employees are responsible for parking their vehicle only in designated parking spots. Employees are not allowed to park in any unauthorized spots. Failing to adhere to this rule could result in the employee's vehicle being towed at the employee's cost. With respect to sites that share the building with other tenants, employees should refrain from using their neighbor's property for congregation, smoking, playing or any other activity that could result in disrupting their business.

j. ***Building and Fire Safety***

- To ensure the safety and security of our workforce, the company expects all employees to become familiar with general fire and evacuation procedures.
- Emergency procedures are reviewed as part of an employee's initial training. Such procedures are also available in Emplx. During an emergency that requires an evacuation, all employees should remember the following:
 - Do not panic.
 - Do not use elevators.
 - Always use the nearest exit.
 - Once you have evacuated the center, move as far away from the building as possible following evacuation routes to designated

areas. This allows emergency crews better access and ensures a safe distance from breaking glass.

- Do not smoke.
- Do not leave the company premises.
- The company may have unannounced fire drills to validate the efficiency and effectiveness of its evacuation procedures.
- Employees are encouraged to contact their supervisor or the HR department for additional information.

SEARCH, INSPECTION & INVESTIGATION POLICY

1. Objective

It is company's policy, when deemed necessary by management, for authorized persons to search and inspect both company property and personal items, including vehicles, brought onto company property. An employee's refusal to cooperate in a search, inspection or investigation will result in disciplinary action up to and including termination.

2. Scope

This Search, Inspection & Investigation Policy ("**SII Policy**") applies to employees of the company. Consultants are exempt from this SII Policy.

3. Procedures for Conducting Searches

3.1 *Decision to search*

The Chief People Officer and Chief Legal Officer are required to approve all searches prior to their occurrence.

3.2 *Conducting searches*

3.1.1 A minimum of three management representatives are required to conduct an unannounced search. Two of these representatives should conduct the search, and the third representative should record the inventory. Items found and identifying locations should be noted.

3.1.2 One of the company representatives conducting the search must be of the same gender as the person whose belongings are being searched.

3.1.3 The search should be conducted in the following manner:

- a. The employee involved will be taken to a private location and informed that the company would like to conduct a search and inspection of his or her personal possessions (including his or her vehicle), in accordance with SII Policy. The company representative conducting this meeting should ask the employee if he or she will cooperate with the search.
- b. The search should not begin until the employee gives written consent to the search. An employee who refuses to cooperate with a search request from an authorized management representative should:
 - Not be detained in any way or for any reason but should be informed that his/her refusal to cooperate will be grounds for disciplinary action up to and including termination.

- c. Be immediately relieved of duty and placed on unpaid suspension pending investigation. In the presence of the employee, the designated company representatives will search as necessary through the employee's locker, work area, personal items or vehicle. The designated company representatives should record an inventory of all items found during the search and secure relevant items. The following may be searched:
- Any company property, including lockers, desks and other individually assigned spaces.
 - Any employee personal property on company premises, including:
 - Pockets
 - Purses/wallets
 - Briefcases
 - Cars/trucks
 - Shopping bags/boxes
 - Removable clothing

The employee may be asked to remove a coat, sweater or similar type of outer clothing so that it can be inspected. The employee may be asked to turn his or her pockets inside out. The search should not include any form of body searching.

- d. After the search is completed, the designated company representatives should:
- Conclude the search by either thanking the employee for his or her cooperation or by placing the employee on unpaid suspension pending the outcome of the investigation.
 - Set up a specific time for the employee to meet with his or her supervisor, or other designated company representative.
 - Immediately write a report of the incident, signed by all involved in the search, including the employee(s). The report(s) should be delivered to the Chief People Officer or their designee. The following information must be included in the report:
 - Reason for the search.
 - Who was involved in the search.
 - Where the search was conducted.

- Date and time of the search.
 - What, if anything, was found during the search.
 - What actions were taken with the employee involved. What items were seized and what action was taken with the item(s).
 - What instructions were given to the employee.
- The Chief People Officer or their designee should immediately report to the appropriate authorities any illegal items that are found and should document such notification. These items will be placed in a secure location until the authorities arrive.

COMPENSATION & BENEFITS

1. Objective

To help employees understand the different components of their compensation structure.

2. Scope

All of the company.

3. Compensation Components

3.1. *Base Pay*

Base pay is an independent component of the salary structure. It determines the employee's gross salary & differentiates the compensation of the employees within a band/level. It is fully taxable as per current tax legislation.

3.2. *Bonus/Incentive*

- A bonus or incentive refers to any compensation above the base wage or salary. This includes, but is not limited to, performance bonuses, referral bonuses, sales incentives or any other compensatory cash or prizes.
- A bonus or incentive may vary depending on the employee's specific position and on specified requirements having been satisfied.
- Bonuses or incentives are payable at the sole discretion of the company depending on the employee's and company's performance during the year. Bonuses or incentives are subject to deduction of applicable income and statutory taxes.
- Bonuses or incentives are payable only to employees who are on the payroll of the company on the date of the cash payout.

3.3. *Salary Advances*

- In general, the company does not provide salary advances. In emergency situations, an advance may be granted by the company under certain conditions.
- The employee will be required to demonstrate the urgent need for the advance and provide appropriate documentation when requested prior to the advance being issued.
- In no case will the amount of the advance exceed 65% of the amount already earned in the pay period. Advances are repaid the following payday.
- An employee may not receive more than two advances each rolling twelve-month period.

- All Advances are approved by the Chief People Officer. The company does not provide loans to employees.

4. Pay Period and Direct Deposit

- Our pay period is monthly once on the last working day of each month. Payday will be advanced by a day if it falls on a Sunday or Public Holiday. In the event should the company have technical or banking partner-related challenges, employees will be notified of the delay in crediting the salary.
- The salaries will be paid to employees through their bank account on the last working day of each month.

5. Provident Fund

- Under the Employee Provident Fund (EPF) Act, employees and the company are required to make monthly contributions to the EPF.
- The contribution is based on current legislation rates and shall be deducted from their salary as stated in the EPF Act. The company will contribute EPF at the statutory contribution rate on the employee's income, i.e., annual base salary, bonus as well as any applicable allowances.

6. Gratuity

Gratuity is the monetary amount which is payable to the employee of an organization under the payment of Payment of Gratuity Act, 1972. It is a part of the salary an employee receives and can be viewed as a benefit plan designed to aid an individual in his/her retirement.

7. Payroll Deductions

The company withholds legally required deductions from the total amount an employee earns each pay period. The company will, with the employee's prior written authorization, withhold additional deductions.

8. Salary Confidentiality

The company maintains salary records for each employee on a confidential basis. Some employees, while performing their regular job duties, may come in contact with salary records. Failure by those employees to adhere to the company's policy on maintaining the confidentiality of the company's records of the salaries of other employees may subject him or her to disciplinary action up to and including termination.

9. Everise India Insurance Benefits

The company offers health insurance benefits for employees, spouse & up to two children designed to meet employee needs. For more detailed information, please refer to the specific policy or the Summary Plan Description (SPD) of the specific benefit plan or contact the Human Resource Department for more information.

10. Employee resignation

This benefit is applicable for all active employees excluding employees serving their separation notice period.

INTERNAL JOB POSTING (“IJP”) POLICY

1. Objective

To provide an opportunity to apply for open positions within the organization, for promoting career growth and effective utilization of the skills aligned with the company objectives.

2. Scope

All regular full-time employees of the company who meet the requirements stated in this Internal Job Posting Policy (“IJP Policy”).

3. Eligibility & Requirement

For any open position received by the talent acquisition team, internal employees shall be assessed through IJP prior to assessing external candidates.

The following will be the eligibility guidelines for the IJP movements:

- **Lateral IJPs** – Minimum 6 months in production in the current role, which does not include nesting time, with a performance rating of “Meets Expectations” and above.
- **Vertical IJPs** – Minimum 12 months after production in the current role, with a performance rating of ‘Meets Expectations and above.
- Any employee with any verbal or more than one written warning for behavioral or performance issues will not be eligible for an IJP.
- Completed all the required trainings and development programs.
- In case an employee applies for simultaneous multiple IJPs, and if he/she gets selected in any of these, the employee will automatically not be eligible for the other lateral IJPs that he/she has applied for.

Additional qualifiers can be added over and above the defined IJP Policy depending on the skill requirements for any position by talent acquisition in consultation with the department head.

4. Guidelines

The step-by-step process is as below:

- Talent acquisition will obtain approvals and release the IJP through internal communication emails and other appropriate channels which may include posters, intranet, etc.

- The communication should specify the skillset required, the job description, eligibility criteria in terms of performance scores, tenure, etc. with an end date of submission of applications.
- Upon the release of the IJP, eligible employees shall submit their applications to the Talent Acquisition team, where the applications will be auto-routed to their supervisors and department heads for approval.
- On receipt of recommendations from the respective managers, talent acquisition, in consultation with the Department Head, shall discuss the IJP evaluation process (i.e., written tests, group discussion, personal interview, etc.) along with the supervisor's ratings.
- The final results of the IJP will be based on the evaluation.
- Feedback will be arranged along with talent acquisition and specific lines of business for those employees who do not qualify the evaluation.

5. Selection and Deployment

- On completion of the IJP selection process, the talent acquisition team will announce the results of the evaluation to the employee.
- Selected employees shall be released from their current role on or before a 30-day period from the time an employee is selected.

6. Compensation

- For all lateral movements, there will not be any immediate increase in compensation. However, if an employee is moved to a new department or line of business and the base pay is less than the minimum salary grade of the new department/line of business, the existing base pay shall be brought at par with the minimum grade of the new position.
- For all vertical movements, if the base pay of the selected employee is higher than the minimum salary grade of the promoted level, the existing base pay shall be increased based upon the new role.
- If the base pay of the selected employee is lower than the minimum base pay of the promoted level, the existing base pay shall be brought at par with the minimum grade of the new position.
- IJP movement letters will be issued to the selected employee with the changes in title or compensation along with the corresponding effective date.

Exceptions to this IJP Policy may be made, based on business necessity, with written approval of the Chief People Officer.

PROMOTION POLICY

1. Policy Purpose

The purpose of this Promotion Policy ("**Promotion Policy**") is to outline the principles, requirements, and process for promotions within the company. It also sets out the minimum standards that should be adhered to.

The company is an equal opportunity employer. Promotion decisions are based on merit, experience, and potential, without regard to race, color, national origin, gender/sex, marital status, age, religion, disability, sexual orientation, ethnicity, veteran status or any other characteristic protected from discrimination by applicable federal, state, or local laws.

2. Policy Statement

The company's promotion philosophy is fundamentally based on the concept of "promotability of the candidate." It requires employees to have demonstrated behaviors and capabilities needed to be elevated to the next level of responsibility, over and above being an exceptional contributor.

Recommendations for promotion should be based on the following factors:

- Sustained performance of the candidate
- Potential displayed by the individual for taking on higher responsibilities
- Availability of vacancies

Recommendations may not be based on:

- A managers' subjective opinions unsupported by performance or metrics
- Discrimination
- Fraternization
- Favoritism
- Nepotism

Promotions shall be role-based except in case of the following:

- SVP to EVP (Band 1)
- Director to Senior Director (Band 2)
- Manager to Sr. Manager (Band 3)
- Lead to Assistant Manager (Band 3)

- Assistant to Specialist (Band 4)

This shall not apply to the Sales function, as the roles are completely market-facing.

3. Procedures

3.1. *Eligibility Requirements*

The following requirements must be met for an employee to be considered for a promotion:

- **Job** – The employee must meet the minimum requirements contained in the role's job description. The employee must also be able to perform the essential functions of the position, with or without reasonable accommodation.
- **Good Standing** – The employee must be in good standing (be clear of a Performance Improvement Plan or any disciplinary action for a minimum of one year).
- **Minimum Tenure** – The employee must meet the minimum tenure requirements specified in paragraph 3.2 below.
- **Performance** – A business case will need to be submitted that demonstrates the following during the required tenure period:
 - KPI/Scorecard performance requirements that were met
 - Measurable performance impact in 2 or more of the following areas:
 - Reduced expenditures
 - Increased revenue
 - Improved process efficiencies
 - Enhanced client experience
 - Enhanced employee experience
 - Innovation
 - company values that were demonstrated
 - How the company's diversity initiatives are supported
- **Employee Potential** – The employee must have demonstrated the potential to take on higher roles and responsibilities.

The mere eligibility of these requirements shall not guarantee an automatic promotion. The employee's promotion must also be approved per the requirements specified in section 3.2 below.

Exceptions to these requirements may only be made upon the unanimous approval of the Global CEO and CPO.

3.2. **Process Requirements**

3.2.1. As a rule, all inter-band promotions shall be strictly role-based. It will be mandatory to complete a tenure period of:

- **Band 1 – 2**

2 years with exceptional performance or 3 years if meets minimum performance requirements.

- **Bands 2 & 3**

1 year with exceptional performance or 2 years if meets minimum performance requirements.

- **Band 4**

Lateral IJPs – Minimum 6 months in the current role, which does not include training time, with a performance rating of good & above.

Vertical IJPs – Minimum 12 months in the current role, with a performance rating of good & above.

3.2.2. Promotions must not merely be recommended based on tenure or other factors which are not directly connected with Performance or the elevated role of the employee.

3.2.3. In case of Band changes for the employee and the promotion, there also needs to be a job enlargement for the same employee and the promotion. Job enlargement would mean increasing the scope of a job currently handled by the employee by extending the range of his job duties and responsibilities.

3.2.4. A promotion recommendation is required to be initiated manually. The promotion recommendation, facilitation, and approval matrix are as follows

Band	Titles	Recommended by	Facilitated by	Approved by
Band 1	SVP, EVP, CXO	CEO/CXO	Corporate HR	Promotion Committee consisting of - CEO, President, CPO and CFO
Band 2	VP	Function Head & Country Head	Corporate HR	Promotion Committee consisting of - CEO, President, CPO and CFO

Band	Titles	Recommended by	Facilitated by	Approved by
	Director, Senior Director	Function Head & Country Head	Corporate HR	Promotion Committee consisting of two CXOs and CPO
Band 3	Team Leader, Assistant Manager, Manager, Senior Manager	Function Head	Country HR Head/Location HR Leads	Country HR Head, Country Head
Band 4	CSR, Specialist/SME	Function Head	Country HR Head/Location HR Leads	Country HR Head, Country Head

- 3.2.5. Once promotion process and approval requirements are completed, Human Resources will prepare a promotion letter and provide it to the employee for signature.
- 3.2.6. Upon receipt of the signed promotion letter from the employee, Human Resources will complete final process requirements in Emplx.

4. Enforcement

An employee found to have violated this Promotion Policy may be subject to disciplinary action, up to and including termination of employment. ***No exceptions to this Promotion Policy may be made without the prior written approval of the CPO.***

LEAVE POLICY

1. Objective

This policy provides a framework to standardize and control the relationship between Everise (India) BPO Services Private Limited ("company") and its Employees (as defined herein below). The policy's objectives are as follows:

- a. Ensure Employees have the opportunity to have a healthy relationship between professional and personal time.
- b. Ensure Employees' interests are safeguarded.

2. Scope

This policy is applicable to all employees ("**Employees**") of the company.

3. Guidelines

- a. A calendar month of service will be deemed completed for calculating the annual leave entitlements if the Employees are at work during all normal working days.
- b. A calendar year is the period from 1st January to 31st December of the respective year for which all the leaves are computed.
- c. Employees are granted the annual leave entitled to them after consultation with their reporting manager or supervisor ("**Manager**"). Manager shall have the right to approve or deny the request at their discretion and without assigning any reason whatsoever. Employees waive the right to challenge their Manager's decision.
- d. Employees should ensure they take their full entitlement to annual leave in consultation and agreement with their Manager. Managers should ensure that employees' workloads allow employees to take their full entitlement to annual leaves.
- e. Employees who wish to avail leaves for more than five (5) consecutive days shall discuss the same with their Manager in advance of the desired date. All leave requests for annual leave should be updated in Workday at the earliest reasonable opportunity.
- f. On all occasions (except sick leave in case of emergency), Employees shall obtain prior approval for leave from the Manager to whom they report before taking the leave. If, however, for a valid reason, prior approval cannot be obtained, the Employees shall advise the immediate superior or departmental head by phone, e-mail, Workday or mobile app. The Employees shall ensure that the same

is recorded on the leave module in the Workday within two (2) working days after resuming their duties.

- g. Any misuse of leave shall be treated as misconduct.
- h. Five (5) consecutive days of absence, without notifying a Manager may be considered a voluntary resignation from the company's employment. In such case, Employees shall not be entitled to receive company's benefits, including, but not limited to, a leave encashment benefit.

4. National and Festival Holidays

National and festival holidays are the days on which the company provides Employees time away from work in order to celebrate holidays common to all geographies across India. In view of the Delhi Shops and Establishment Act, 1954, employees of Everise India will be paid three (3) days per calendar year as holidays. The HR department will share the holiday list no later than January of each year.

No substitute holiday shall be allowed if any of the holidays, initially declared, subsequently happens to fall on a weekly off or any other non-working day or in the event of more than one (1) festival falling on the same day.

5. Earned Leaves

- a. Each Employee of the company is entitled to fifteen (15) days of Earned Leaves ("EL") every calendar year after every twelve (12) months of continuous employment. Every month of the calendar year the Employee shall get credit of 1.25 days.
- b. Employees who join mid-way during the year shall be eligible for EL credit for the remaining months on a pro-rata basis.
- c. Any leave taken in excess of the entitled leaves shall be automatically considered as leave without pay.
- d. Employees must ensure that they obtain the necessary approvals from their Manager for EL. If an Employee takes leave without prior approval, the company shall consider it to be an unauthorized absence, and the same may be unpaid.
- e. The Employee has to avail a minimum of four (4) days of EL in the year, for which leave travel allowance is claimed. The employee must be on approved EL of a minimum of four (4) days or longer. Sundays and national holidays falling within this period of four (4) days shall not be included as EL.

6. Sick Leave

- a. All the Employees of the company shall be entitled to fifteen (15) days of sick leave ("SL") in a year which shall be credited at the start of the calendar year.

- b. Employees who join mid-way during the year shall be eligible for SL credit for the remaining months on a pro-rata basis.
- c. If an Employee is prevented from working due to illness, the Employee must notify their Manager and/or the HR department as soon as possible but no later than the first day of illness. Failure to do so may lead to disciplinary action.
- d. There may be exceptional circumstances that prevent notification by the Employee. The company will treat such cases sympathetically, taking into consideration such situations.
- e. If the Employee fails to communicate to their Manager by the third day, the company shall view the absence as desertion. It will be up to the Employee to demonstrate that the absence was due to illness upon their return to work.
- f. All medical leaves of more than two (2) days shall be supported by a medical certificate issued by a registered medical practitioner in India.

7. Maternity Leave

- a. Maternity Leave shall be granted as per the Maternity Benefit Act 1961 and Maternity Benefit (Amendment) Act of 2017. Female employees who have worked for at least eighty (80) days in the company in the twelve (12) months immediately preceding the date of expected delivery shall be entitled to twenty-six (26) weeks (182 days), including weekends and holidays) for two surviving children, of which more than eight (8) weeks shall precede the date of expected delivery.
- b. Mothers giving birth to a third surviving child will be entitled to maximum twelve (12) weeks of maternity leave, of which not more than six (6) weeks shall precede the date of her expected delivery.
- c. The expectant mother can choose to use up to eight (8) weeks of leave before her delivery. The leave structure is left to the mother's discretion; she may also take the entire twenty-six (26) weeks of maternity leave after the birth of the child.
- d. Eligible women employees shall apply for leave on the system by filling out all the relevant details and providing a hard copy of the certificate from the qualified gynaecologist specifying the date of expected delivery.
- e. Maternity Leave can be extended for an additional one (1) month in case of sickness arising out of pregnancy, premature birth of child, medical termination of pregnancy or tubectomy operations, provided the employee submits necessary medical certificates to HR.
- f. Maternity leave may not be accumulated or encashed.

8. Adoptive Mother

A female employee who legally adopts a child who is below the age of three (3) months at the date of adoption is eligible for twelve (12) weeks of leave, which shall be calculated from the date child is handed over to the adopting mother.

9. Commissioning Mothers & Surrogate Mothers

A commissioning mother is a female employee who has opted for the services of another woman to conceive a child. The commissioning can be with or without the provision of genetic material by her and her partner. A surrogate mother is a female employee who chooses to bear a child on behalf of another woman. As per the maternity leave policy in India, both the commissioning mother and the surrogate mother are eligible for the maternity benefit for up to twenty-six (26) weeks.

10. Tubectomy; Miscarriage; Pregnancy Termination

Female employees who have had a tubectomy can opt for two weeks' leave from the date of their operation.

In case of illness arising out of pregnancy, earned leave balance can be combined with maternity leave.

In case of miscarriage or medical termination of pregnancy for any reason, the number of days of paid leave will be limited to forty-five (45) continuous days from the date of such occurrence.

If a female employee needs to use maternity leave for medical termination of pregnancy or a miscarriage, the request for such a leave shall be forwarded to their Manager along with the supporting medical documents.

The female employee shall take active steps to keep her Manager informed about any foreseeable changes in the initial dates communicated.

An Employee on maternity leave is not permitted to take on any other employment, even on a temporary basis, without written authorization from the company. To do so will result in termination of employment.

A female employee who is covered under Employee State Insurance (ESI) Act is not eligible for the maternity benefit as per the Maternity Benefit Act and must use the Maternity benefit provided by the Employee State Insurance Corporation (ESIC) under the provisions laid down under the Employee State Insurance (ESI) Act, 1948.

11. Paternity Leave

A male employee who has completed 90 (ninety) days of service in the organization & whose spouse or partner has given birth to a baby or is under medical supervision

due to a maternity-related emergency is entitled to paternity leave of seven (7) working days, which can be used for up to two (2) children only.

This leave cannot be accumulated or encashed and has to be taken in one go.

12. Compassionate Leave

Employees are eligible for compassionate leave in the event of the death of the following immediate family members:

Relation to Employee	No. of paid compassionate leave
Spouse/Child/Parents/Siblings	Three (3) working days
Grandparents/Parents-in laws	Two (2) working days

Compassionate leaves must be consumed immediately from the date of demise.

13. Unpaid Leave

Unpaid leave may be granted for a period not to exceed seven (7) days during a calendar year and is subject to management's approval on a case-by-case basis. Any unpaid leave exceeding seven (7) days shall only be granted under exceptional circumstances and at the sole discretion of the management, subject to the following:

- a. Business needs;
- b. An employee having consumed their entire year's leave encashment;
- c. Valid and genuine reasons are given for circumstances due to an emergency or on compassionate grounds, such as taking care of a sick family member;
- d. Unpaid leave of more than thirty (30) consecutive days may affect the computation of the following benefits:
 - (i) Annual leave entitlement
 - (ii) Performance/Variable bonus
- e. Employees shall not be entitled to any allowance during unpaid leave.

14. Optional Holiday

- a. Optional holidays are the specific number of days that an Employee can choose as per their choice basis religion, norm, preference and practice. Employees shall

be notified of the optional holiday list along with the annual holiday list at the beginning of the year.

- b. An Employee can opt for optional holidays from the list of annual holidays by informing their Manager at least two (2) weeks in advance.

15. Leave Encashment/Carry Forward

- a. Leave carries forward is allowed only to the extent of maximum forty-five (45) days from the Earned Leave and the balance EL over and above the said forty-five (45) leaves shall get lapsed. Any other leave balance besides Earned Leave shall also get lapsed.
- b. EL can be encashed only at the time when the Employee ceases to be in the company's employment, and in such case leave encashment will be restricted to maximum of fifteen (15) days. Company reserves the right to change the limit of leave encashment at any time.
- c. EL encashment will be calculated on (current monthly basic salary per month*12 months/365days=per day amount*days of paid leave left) and will be subject to income tax.

16. Leave during Notice Period

An Employee shall not be eligible for leave during their notice period.

17. Unauthorized Absence

- a. In case an Employee is absent from work without the prior approval from their Manager or is absent, even though the leave is rejected by the approving authority, no salary shall be paid to the Employee for the duration of their unauthorized absence.
- b. The HR team shall issue a memo to the Employee specifying the details of days of absence and the penalty levied if the same exceeds more than five (5) consecutive days. In case of unauthorised absence, the company shall have the sole discretion to decide whether an employee shall be penalised or terminated from the employment or with both.

18. Half Day

To be entitled for half a day's pay, an employee must work for minimum of 4.5 hours (excluding lunch time) within their designated work hours.

19. Policy Owner

HR is the policy owner. For any clarifications regarding Leave policy, please contact your reporting manager or Human Resources.

Any deviation from the leave policy will need the approval of the Chief People Officer and Global CEO

Rehire & Reinstatement

Eligibility is determined based on how the Employee left Everise India, skills, performance and attendance.

1. **Layoffs / Closure / Program Ended** – Employees who have demonstrated good performance are eligible for rehire. There is no waiting period to apply for available openings based upon qualifications, attendance, and performance.
2. **Voluntary Termination with Full Notice** – Employees who work through their full notice and meet overall good performance and behavioral standards are eligible for rehire. There is no waiting period to apply for available openings based upon qualifications, attendance, and performance.
3. **Involuntary Terminations** – Employees who were terminated for misconduct, violation of company's policies, unsatisfactory performance, excessive absenteeism or lateness, or any other for-cause terminations are generally not eligible for rehire.

GLOBAL TRAVEL POLICY

1. Policy

- To provide guidelines through which Domestic & International business travel should be arranged and the parameters that must be adhered to for accommodation and other incidental expenses.
- It is Everise's Global Travel Policy ("**Global Travel Policy**") to reimburse employees for necessary and authorized travel expenses when directly connected with or pertaining to the transaction of Everise business.
- All travel must be done in accordance with this Global Travel Policy. Those traveling on Everise business are asked to exercise prudent business judgment regarding expenses covered by this Global Travel Policy.

2. Purpose

- This Global Travel Policy shall provide guidelines on the accurate documentation of all travel business transactions.

3. Scope

- All employees across all locations of the company, who need to travel both Internationally & Domestically for business purposes.

4. Guidelines

- For domestic travel, the President's approval is required. For international travel, the department head's approval and global CEO's approval is also required.
- Employees must only undertake international business travel if the nature of the work cannot be completed through telecom/video-conference alternatives.
- All travel must be booked only through our travel partner, Vikas Chopra at Fly Premier Class & using our automated Travel Requests process in NetSuite for:
 - Air travel
 - Hotel
 - Car Rentals

All travel must be planned as far in advance as possible and scheduled so as to minimize the impact on the workday.

5. Procedure

5.1. *Mode of Travel*

The mode of travel as applicable to different categories of employees is as below:

International Travel	
Band	Class of Travel
Band 1 – SVP/EVP/CXO	Economy Class
	Business-class if one-way travel time exceeds 5 hours
Band 2 – VP/Senior Director/Director	Economy Class
	Premium economy if one-way travel time exceeds 7 hours
Band 3, 4 – Senior Manager & below	Economy Class

Domestic Travel	
Band	Class of Travel
Band 1 – SVP/EVP/CXO	Economy Class
Band 2 – VP/Senior Director/Director	Economy Class
Band 3, 4– Senior Manager & below	Economy Class

5.2. *Expenditure Entitlements*

International travel entitlements (in USD) as applicable to different categories of employees are listed below:

Band	Daily Lodging Entitlement	Daily Allowance Entitlement
Band 1 – SVP/EVP/CXO	\$250	\$75
Band 2 – VP/Senior Director/Director	\$175	\$60
Band 3, 4 – Senior Manager and below	\$150	\$50

5.3. ***Travel Accommodations***

Travel Requisition Approvals and Procedures

- Employees who need to travel for business purposes must E-mail the travel request to our travel partner, Vikas Chopra, at Fly Premier Class
- Vikas Chopra provides various options, including rates to employees via E-mail. Employee to confirm the travel options by sending an E-mail to Vikas
- Employee to initiate travel form on NetSuite with complete details including costs and submit for approval.
- Upon approval from Department Head/CPO/President/CEO, Vikas sends an E-mail with an itinerary for travel.
- Should a new hire not yet be set up in NetSuite, they will need to contact the Global Service Desk. The GSD will provide the necessary form to be completed, and they will submit the request for approval and completion.

5.4. ***General Travel Policy***

- Cash advances will not be provided except in special circumstances and will require the prior approval of the Country HR Head, CPO, and Chief Financial Officer (CFO).
- Expenditures incurred on commuting from residence to airport and airport to hotel and back locally and at an international location shall be reimbursed additionally only on submission of bills.
- The daily allowance will cover all boarding expenses, including basic laundry, meals, etc.
- The company will not reimburse tips greater than 20%.
- Other reasonable travel expenses may be considered, such as emergency business calls received while overseas. This would, however, need to be justified in an itemized bill during the reimbursement process and need to be approved by the head of department.
- Luggage, briefcases, magazines, newspapers, books, airline club dues and/or initiation fees, traffic fines, toiletries, hair-cuts, shoe shines, in-flight movies/headsets, excessive personal phone calls, parties, personal recreation, and alcoholic beverages are all considered personal in nature and will not be reimbursed.
- While on international trips, employees shall use the local sim card of the country being visited, which shall be facilitated by the IT and Administration leads of that country. As an alternative, the employee will be allowed the use of a data roaming package from the local telco company (in lieu of obtaining local sim card) and the amount is capped

at USD \$50.00 per two-week trip. Any excess claimed requires additional approval from Head of Department.

- Expenses incurred on local transport should be supported by receipts. In case of non-availability of receipts, exception approval of the Head of Department should be taken.
- Any payment greater than what is allotted shall require approval from the head of department and Chief Financial Officer (CFO).

5.5. *Lodging Policy*

It is the company's policy for all employees to stay with our preferred and negotiated rate properties. When requesting lodging arrangements, employees should observe the following:

- All reservations must be made through NetSuite Travel Requisition Form. Please note that hotel rooms are NOT automatically paid for by Everise. All hotel rooms must be pre-approved prior to trip, otherwise they will not be reimbursable. This does not include incidentals.
- Employees must utilize Airbnb services whenever the length of stay is more than 5 days.
- Hotel reservations that are not going to be used, must be cancelled 24 hours prior so that guarantee charges are not incurred. Employees who do not cancel reservations may not have such expenses reimbursed. Mini-bar and room service charges will be included as part of daily allowance calculation. Other charges (e.g., in-room movie or spa or other luxury services) will be considered personal in nature.
- Each employee must include the itemized hotel receipt with the expense report to be reimbursed. Cancellations should be handled by the employee contacting our Travel Coordinator.

5.6. *Car Rental Policy*

When renting automobiles, employees should observe the following:

- All reservations must be made through NetSuite travel requisition form. Please note that the car rentals are not automatically paid for by Everise. All car rentals must be pre-approved prior to trip, otherwise they will not be reimbursable.
- All cars rented should be of compact or intermediate size (based upon the number of employees traveling together). The company will not reimburse luxury automobiles. It is encouraged to use UBER.
- Employees are not to purchase additional insurance when picking up a rental vehicle.

- In case of accident, processing of insurance varies from country to country. The employee should coordinate with someone in the recipient country for the processing of required documents.
 - No extras will be reimbursed by Everise (GPS, etc.).
 - Employees should return the rental vehicle with a full gas tank (or if the trip will exhaust a tank of gas, the employee may pre-purchase the gas from the auto rental company as often this is less expensive than buying the gas yourself).
 - The Everise Car Rental Policy covers rental cars for business-related travel only.
 - Report the accident to:

Liberty Mutual – 800-362-0000
Everise CustomerContactChannels
Everise Policy # AS6-Z91-468870-018
Please put your supervisor on notice of the incident to report to:
Helen Franco
Helen.Franco@weareeverise.com
Jordan Parnell
Jordan.Parnell@hubinternational.com
225-218-2492

5.7. ***Travel Time Policy for Non-Exempt/Hourly Employees***

- Business trips involving non-exempt employees must be pre-approved by the Country HR Head, the department head and the President.
- In general, time spent traveling during a non-exempt employee's regularly scheduled hours is considered compensable. Time spent traveling outside of the non-exempt employee's regularly scheduled hours is not considered compensable.
- Working time spent on an out-of-town business trip should be recorded and is considered time worked except for normal time spent in transit from home and the regular mealtime of 30 to 60 minutes.
- Business-related travel time of non-exempt employees is also credited as time worked when calculating eligibility for overtime, as defined in the local area (daily/weekly). The Champion's manager should review non-exempt employees daily logged hours to ensure accuracy and compliance with applicable State and Federal laws.

5.8. *Expense Reimbursement Process*

It is Everise's policy that all employees shall record in a timely fashion all expenses incurred in the conduct of authorized company business on the electronic employee expense report.

- Expense reports must be submitted during the same month in which you travelled. Any expenses submitted later than 30 days post travel completion will run the risk of not being reimbursed. Itemized and fully legible receipts (business name, amount, date, etc.) must be presented.
- Signed credit card slips should be included but are not considered sufficient support without an itemized receipt. All T & E's are paid out bi-weekly on non-payroll Fridays.
- In order to be reimbursed timely, all T & E's must be completed in NetSuite by EOD Monday following that Friday so that supervisors and accounting have enough time to view and approve. All expense reports should have itemized receipts included for each expense line item and mileage should have the number of miles included. Bank statements without support are not sufficient documentation of expenses and do not qualify for reimbursement.
- The only exceptions to this are bank fees incurred as a result of currency exchange which may appear on a bank statement and cash tips as reflected in the statement with date, vendor, and amount. Any expense reimbursement that does not adhere to this Global Travel Policy will be rejected by Finance.

5.9. *Authorized Travel Agent – Travel Partner at Fly Premier Class*

- Travel Partner at Fly Premier Class is the only authorized travel agency authorized for all Everise employees.
- Travel Partner at Fly Premier Class will follow and enforce the Global Travel Policy.
- All travel arrangements for Everise employees will be processed through the SSC travel services support team.

Travel Partner at Fly Premier Class is not authorized to book or issue travel tickets when directly contacted by a Everise employee.

5.10. *Travel Services Support Contact Information*

Contact Name	Contact number	Contact Email
Authorized Travel Agent: Vikas Chopra, Travel Partner at Fly Premier Class	Toll Free 877.477.3326 Cell 240.472.4502 WhatsApp# 240.472.4502	Vikas@ flypremierclass.com
Kopal Rana, Travel Partner at Fly Premier Class	US-703.740.0216 India # +91 95992 32500	Kopal@ flypremierclass.com

Any deviation from this Global Travel Policy will need approval of the Chief People Officer and Global CEO.

EMPLOYEE RESOURCES

1. Communications

- We believe all employees should be kept fully informed about Everise India and any current events. Your supervisor is always your best source of information. Workday, the company's website, and the bulletin boards are also excellent sources to access information of general interest.
- company information may also be dispersed by company email. If you have any questions or suggestions, please feel free to discuss them with your supervisor, any member of the management team, or a representative from the Human Resources Department.

2. The Immediate Supervisor

- Supervisors perform a key role at Everise India in helping employees understand their specific role within our organization while excelling in their job requirements. Supervisors are responsible for working with employees to plan future career goals, discuss pertinent activities and projects and participate in ongoing and annual evaluations of job performance.
- We realize in the normal course of business that questions, issues, or concerns will sometimes arise. It is important we resolve any of these issues and concerns in a timely manner to avoid escalation and loss of focus on our goals. For this reason, we strongly encourage any employee to meet with his or her immediate supervisor regarding any concern or issue which may arise.
- Please do not assume the company is aware of any questions, issues, or concerns. We encourage you to bring any questions, issues, or concerns to our attention, so we can make every effort to resolve them. If you feel it would be inappropriate to discuss an issue with your direct supervisor, you should bring it to the Human Resources Department.

3. Human Resources (HR) Department

- The HR Department may provide information regarding policies, procedures, pay and benefits, as well as assist in other areas of support and service.
- HR representatives are also available to confidentially discuss and assist with matters that are personal or private in nature, providing resources and answering questions in addition to the support provided by the department management.

4. Open Door Policy

- The company believes that open communication within an atmosphere of mutual trust is of prime importance to its employees. Realizing that effective communication is

always a two-way street, the company values employees' feedback, input and suggestions on any matter.

- In most cases, talking with one's supervisor is the most effective way to share your feedback or suggestion. However, an employee may discuss problems or suggestions with a higher-level manager, executive or the HR Department instead of, or in addition to, their supervisor.
- The company will attempt to keep expressions of concern, their investigation, and the terms of their resolution confidential. However, in the course of investigating and resolving concerns, some dissemination of information to others may be necessary.

WHISTLEBLOWER POLICY

1. Rationale

Everise is committed to ensuring the highest possible standards of ethical, moral and legal business conduct and practices including openness and accountability in all aspects of its business. With the establishment of this Whistleblower Policy ("Whistleblower Policy"), employees, advisors, contractors and vendors are encouraged to raise genuine concerns regarding Detrimental Actions and Improper Conduct occurring within Everise globally. The purpose of this Whistleblower Policy is to:

- Provide a consistent, systematic, corporate-wide process for managing any suspected detrimental action and improper conduct;
- Provide a mechanism for employees and others to report their concerns freely and without fear of reprisal or intimidation if they act in good faith;
- Protect individuals who in good faith report detrimental actions or improper conduct on a confidential basis; and
- Assist in ensuring that improper conduct and detrimental actions are identified and dealt with appropriately.

This Whistleblower Policy supplements (and does not replace) any and all existing policies and procedures of Everise relating to the treatment of wrongful or improper conduct.

2. Coverage

This Whistleblower Policy applies to all Whistleblowers as defined below.

3. Policy

- A Whistleblower as defined by this Whistleblower Policy may be an employee, advisor, contractor or vendor of Everise who reports an activity that he/she considers to be illegal or dishonest to one or more of the parties specified in this Whistleblower Policy.
- The Whistleblower is not responsible for investigating the activity or for determining fault or corrective measures; appropriate management officials are charged with these responsibilities.

Examples of illegal or dishonest activities include violations of federal, state or local laws; billing for services not performed or for goods not delivered; and fraudulent financial reporting.

- If an individual has knowledge of or a concern that illegal or dishonest fraudulent activity has occurred, the mediums for reporting are:

- Open Door Policy (Face-to-face meetings)
 - Email
 - Mail
 - Phone
 - Toll-free Hotline
 - Or via the Corporate Website (if applicable)
- Employees are expected to immediately report any wrongdoing by reaching out to his/her immediate supervisor, others in management, Human Resources or the country Human Resources head. The employee must exercise sound judgment to avoid baseless allegations. An employee who intentionally files a knowingly false report of wrongdoing will be subject to discipline which may include termination.
 - Whistleblower protections include maintaining confidentiality of the Whistleblower and against Retaliation. Insofar as possible, the confidentiality of the Whistleblower will be maintained. However, identity may have to be disclosed to conduct a thorough investigation, to comply with the law and to provide accused individuals with their legal rights of defense.
 - Everise will not retaliate against a Whistleblower in any manner, including retaliation in the form of an adverse employment action such as termination, compensation decreases, poor work assignments and threats of physical harm. Any Whistleblower who believes he/she is being retaliated against must contact the Human Resources head immediately. The right of a Whistleblower for protection against retaliation does not include immunity for any personal wrongdoing that is alleged and investigated.
 - All reports of illegal and dishonest activities will be promptly submitted to the country Human Resources head who is responsible for investigating and coordinating corrective action for each country. Employees with any questions regarding this Whistleblower Policy should contact Human Resources or Helen Franco, Chief Legal Officer.
 - Local references to this for your geography are available in the Annexure provided herein.

4. Procedural Guidelines

4.1. Definitions

Complaint	A disclosure of improper conduct made by a Whistleblower
Confidential Information	Includes:

	Information about the identity, occupation, residential address, work address or whereabouts of (i) the whistleblower; and (ii) the person against whom the Whistleblower has made a complaint; information disclosed by the Whistleblower; and information that, if disclosed, may cause detriment to any person.
Retaliation/Detriment Action	Any reprisal action against a Whistleblower which shall include: Action causing injury, loss or damage; Intimidation or harassment; Interference with the lawful employment or livelihood of the Whistleblower including discrimination, harassment, discharge, demotion, suspension, disadvantage, termination, adverse treatment in relation to the Whistleblower's employment or the taking of disciplinary action; and a threat to take any of the above actions
Improper Conduct	Any unethical behavior, malpractices, illegal act or any other wrongful or improper conduct within Everise which, if proved, constitutes disciplinary offense or a criminal offense.
Whistleblower	Any employee, advisor, contractor or vendor of Everise making a complaint and/or a report under this Whistleblower Policy or to any compliance officer.
CMS	Case Management System

5. The Whistleblower Hotline

- The toll-free Whistleblower Hotline has been created to encourage employees, advisors, contractors or vendors of Everise to speak up when they have legitimate concerns about misconduct. The hotline number is available 24 hours a day and 7 days a week.
- Confidentiality and anonymity are critical factors in a properly managed ethics hotline. As such, all hotline information, including CMS (Case Management System) passwords and copies of reports, are managed by the Primary Contact in a secure environment and that access to this information is limited only to those individuals who have a "need to know."

6. Roles

Below are the various functions performed by individuals involved with our hotline program. One person may perform multiple roles at any given time. Provided below are the descriptions and persons assigned to each role:

Whistleblower Committee (WBC)	<ul style="list-style-type: none"> • A committee formed for the purpose of receiving, processing investigating, • and determining the genuineness of any Complaint or Report received • from a Whistleblower or a Recommendation received from the Compliance Officer • in order that appropriate action can be taken to address the Complaint, Report • or Recommendation. The WBC shall also be responsible for dealing / liaising with • the Compliance Officer in respect of any matters pursuant to the Recommendation.
Compliance Officer	<ul style="list-style-type: none"> • Responsible for ensuring that all complaints about unethical or illegal conduct • are investigated and resolved. The Compliance Officer will advise the Board of Directors on all complaints and the resolution and will report at least annually on any compliance activity relating to accounting or alleged financial improprieties. • The Compliance Officer is empowered to conduct the investigations in isolation of the Board in order to maintain independence but are free to involve members of • the Board as necessary. It is solely the Compliance Officer's charge to determine whether or not a complaint can be considered valid for investigation though any individual may submit a complaint as noted above. • This role is taken on by our Chief Legal Officer, Helen Franco
Investigation Team	<ul style="list-style-type: none"> • A team made up of members nominated by the WBC on an ad-hoc basis for the purpose of investigating any Complaint Report or Recommendation as directed • by the WBC. • This must be comprised of the following: • Investigation Team Lead

	<ul style="list-style-type: none"> Representative from Management (preferably Sr. Manager up) who may or may not be from the same Department Representative from HRBP who will also be responsible for taking the minutes of meetings.
Investigation Team Lead	<ul style="list-style-type: none"> Usually the Country HR Head or the person designated by the WBC as the leader of the Investigation team
Primary Contact	<ul style="list-style-type: none"> The individual with primary responsibility for the hotline program. By emailing reports@lighthouse-services.com, the Primary Contact will manage who the designated recipient for reports are and inform the vendor of any changes to a DBA (Doing Business As) names. She will also receive email notification of any upgrades to our services, administrative matters and program correspondence. There can only be one primary contact.
Designated Recipient	<ul style="list-style-type: none"> All reports are sent via email to our designated recipients. The hotline agreement provides Everise with the opportunity to specify who will receive reports for Fraud, Ethics, Compliance and Human Resource cases. To ensure appropriate immediate action is taken, the mailboxes are segregated below: Fraud, Compliance & Ethics: Helen Franco, Chief Legal Officer & Sheena Ponnappan, Chief People Officer Human Resource Concerns (includes Harassment): Helen Franco, Chief Legal Officer, Sheena Ponnappan, Chief People Officer and Country Human Resource Heads
Case Management System (CMS) Administrator	<ul style="list-style-type: none"> Helen Franco, Chief Legal Officer & Sheena Ponnappan, Chief People Officer The CMS Administrator has unrestricted access to our entire online database and is responsible for updating information related to the database. In addition, they also assign reports to CMS Investigators and add new users. There is no limit to the number of CMS Administrators we can have.
Case Management System (CMS) Investigator	<ul style="list-style-type: none"> Legal Team and Country Human Resource Heads Investigators have limited access to the CMS and can investigate, track progress, dialog, and upload files to reports they have been assigned by the Administrator. There is no limit to the number of CMS Investigators we can have.

7. Hotline Details

Below are the International Calling Instructions for employees (Worldwide Toll-Free Number) for countries that do not use a direct dial toll-free.

7.1. *For Employee:*

- Make sure you have an outside line.
- Enter the Access Code for the country and/or the telephone system you are calling from.
- An English-language voice prompt will ask for the number you are calling.
- *Enter our toll-free number: 800-603-2869. There is no need to dial '1' before the toll-free number. You are now connected to the hotline.*
- A Lighthouse greeting will be played in multiple languages. Make a choice from the prompts or press 0 and tell the English operator the language you speak. An interpreter will then join the call in 2 – 3 minutes. The Lighthouse operator will interview you, aided by the interpreter.
- A report in English is then sent to the designated recipient(s) of your company.
- Access codes are subject to change

Calling Instructions

1. Make sure you have an outside line.
2. Enter the Access Code for the country and/or telephone system you are calling from. You will then hear a 'bong'.
3. An English-language voice prompt will ask for the number you are calling.
4. Enter our toll-free number: 800-603-2869. There is no need to dial "1" before the toll-free number.
5. You are now connected to the hotline.
6. A Lighthouse greeting will be played in languages Make a choice from the pre-recorded language prompts* or press 000 and tell the English operator the language you speak (preferably in English). An interpreter will then join the call in 2 ± 3 minutes. The Lighthouse operator will interview you, aided by the interpreter.
7. A report in English is then sent to the designated recipient(s) of your company.
8. Access codes are subject to change.

The following automated in-language greetings are provided to the caller:

English	press 1	Hungarian	press 01	Finnish	press 001
Spanish	press 2	Polish	press 02	Russian	press 002
French	press 3	Dutch	press 03	Hind	press 003
Mandarin	press 4. wait for greeting, then press 1	Czech	press 04	Hebrew	press 004
Cantonese	press 4, wait for greeting, then press 2	Taiwanese	press 05	Turkish	press 005
German	Press 5	Korean	press 06	Other	press 000
Italian	press 6	Tagalog	press 07		
Portuguese	press 7	Vietnamese	press 08		
Japanese	press 8	Indonesian	press 09		
Arabic	press 9				

Website

Employees also have the option to file a complaint online by going to: [whistleblower Submission](#)

8. Case Management Guidelines

- Reports received via the Hotline are sorted by the designated recipient(s) and, where appropriate, provided to the Chief People Officer or her designee, for appropriate action.
- Once a case is turned over to the country Human Resource head, discipline management procedures must be followed.
- Where necessary, such as for grave ethics concerns (e.g., discrimination or harassment) an Investigation Team is created and usually led by an investigation team lead.
- The Investigation Team shall provide the necessary Investigation inputs upon which the disciplinary action or non-action, where applicable, shall be based.
- All cases must be recorded in the Case Management System (CMS). The following accesses are provided to the roles below:

CMS Administrator	View reports online at your convenience Assign incidents to the appropriate party for investigation
--------------------------	--

	Set the risk level, priority and status of reports Record follow-up and outcome notes Anonymously dialog with reporter if enabled Create reports and charts to help track activity and analyze trends Review an audit trail for added internal control Upload digital files and documents to a record Search the database using keywords and date filters Create multiple user levels Add customized fields Send messages to system users Integrate system data using API
CMS Investigator	Assign incidents to the appropriate party for investigation Set the risk level, priority and status of reports Record follow-up and outcome notes Anonymously dialog with reporter if enabled Create reports and charts to help track activity and analyze trends Upload digital files and documents to a record Search the database using keywords and date filters.

- The Compliance Officer is responsible for providing progress updates and reports of closure, aside from the regularly released Compliance Reports, to shareholders and Executive Leadership as necessary.

9. Protection for Whistleblowers

9.1. *Non-Disclosure of confidential information*

Confidential information is defined as:

- Information about the identity, occupation, residential address, work address or whereabouts of (i) the Whistleblower; and (ii) the person against whom the Whistleblower has made a Complaint;
- Information disclosed by the Whistleblower; and
- Information that, if disclosed, may cause detriment to any person.
- Should the Complainant, or the person who is reported as the policy violator, request for the above, the Investigation Team or must seek approval from the Complainant for the same to be released. Without such consent, the Complainant shall remain under the blanket of anonymity.

9.2. *Non- Retaliation*

- If proven true, the company shall impose the necessary Disciplinary Actions for any retaliation or detrimental action taken against a Whistleblower.
- Such retaliation actions shall include:
 - Action causing injury, loss or damage;
 - Intimidation or harassment;
 - Interference with the lawful employment or livelihood of the Whistleblower, including discrimination, discharge, demotion, suspension, disadvantage, termination, adverse treatment in relation to the Whistleblower's employment or the taking of disciplinary action;
 - Threatening to take any of the above actions.

ENTERPRISE INFORMATION SECURITY POLICY

1. Objective

The objective of the security program is to ensure the availability, confidentiality, and integrity of information/data and systems across the entire organization. Security is an enterprise-wide risk management issue.

- Senior executives at each operating business have full accountability on securing information and systems across their business and operation.
- All employees and authorized users, including 3rd party vendors and contractors, are responsible for protection of information and systems against threats and risks.

2. Access

All requests for logical access must be defined within a Service Request in the ticketing system. Access to information and application systems and functions are restricted to the minimum necessary to perform your job function. Privileges are formally authorized and controlled, allocated to users on a need to use and event by event basis for the functional role.

Each user of the system is granted a unique User ID. There is no shared access or accounts. No guest or anonymous accounts are created.

Upon termination, either voluntary or involuntary, logical, and physical access is removed.

3. Password policy

Rules govern the creation and maintenance of passwords for the User IDs. Passwords are never set to not expire. The expiration duration is forty – two (42) days. After this, the password must be changed by the user.

Passwords should be changed whenever there is any indication of possible system or password compromise. Default passwords are never permitted.

3.1. *General Standards*

- You may not use the previous 24 passwords
- Passwords expire in 42 days
- Password must be in affect a minimum of 1 a day
- Minimum password length 8 characters
- Passwords may not contain the user's entire account name or full name.

- Passwords must contain characters from three of the following five categories:
- Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
- Lowercase characters of European languages (a through z, sharp s, with diacritic marks, Greek and Cyrillic characters)
- Base 10 digits (0 through 9)
- Non-alphanumeric characters: ~!@#\$%^&* -+=\(){}[];:'"<>.,?/
- Passwords should not contain the company name in any form

A passphrase is suggested to provide for a higher level of security. A passphrase is a sequence of words or text used instead of a password. It may be easier for you to remember but harder for hackers to crack.

A password dictionary is utilized to enforce strong passwords and block any change requests that matches a password on the banned password list.

After 6 repeated unsuccessful password attempts, your User ID will be locked. The lockout duration is 30 minutes or until an administrator enables your User ID. Idle sessions of more than 15 minutes require you to re-enter your password.

Your workstation may be protected with a number of security protocols. Anti-virus software, intrusion detection, firewall, operating system updates, restricted ability to save, copy, print, download or install software. Full and quick anti-virus scans will run at scheduled intervals as well as update virus definitions. Security patches are delivered on a pre-determined schedule. Security protocols are centrally managed and should not be tampered with, disabled or bypassed.

Only approved software should be installed. The use of removable media devices is not permitted.

3.2. ***Security Awareness Training***

The Security Awareness program provides a general overview of the common-sense techniques to keep data safe. Training may cover topics such as privacy and key security policies and procedures, legal and regulatory considerations, and fraud related issues staff should know to prevent, detect and respond to information security incidents. Security Awareness Training is required of all staff members upon hire. Training is repeated at least annually. The frequency and content of training may change based on emerging threats and technology.

4. Incident Response

The company seeks to ensure that all personnel react appropriately to any actual or suspected security incident relating to Information Systems and Data. Incidents should be reported to the Global Service Desk (through any channel). A ticket will be created and routed to the appropriate group for handling. Reports should include, where possible, a description of the event, the date of the occurrence or discovery, a description of the types of information involved. Reporting should be done without reasonable delay.

Any concerns regarding security policies, procedures, or compliance with them, may be reported to the Security Officer at InfoSec@weareeverise.com.

NON-SOLICITATION & NON-DISPARAGEMENT POLICY

1. Non-Solicitation

Prior to employee's termination date with the company and for the 12-month period following termination, employee agrees not to, directly or indirectly, whether for his/her own account or for the account of any other individual or entity, (a) solicit, induce, enter into any agreement with, or attempt to influence any individual who was an employee, consultant or contractor of the company at any time during the preceding twelve (12) month period to terminate his/her employment relationship with the company, or interfere in any other way with the employment or other relationship of any employee, consultant or contractor of the company, or (b) solicit any customer (including any prospective customer with respect to which the company had taken any material steps toward establishing a business relationship at any time on, or within the nine (9) months prior to, the Termination Date (a "Prospective Customer")) or vendor of the company, induce any of the company's customers or vendors to terminate its existing business relationship with the company, diminish the amount of business a customer or vendor is doing with the company or interfere in any other manner with any existing business relationship between the company and any customer, vendor or third party or any potential business relationship between the company and any Prospective Customer.

2. Non-Disparagement

During and after his/her employment with the company, the employee agrees not to make any disparaging statements about the company or to engage in disparaging conduct directed at the company that is an intentional public attack on the company's products and/or services in a manner that a reasonable person would perceive as calculated to harm the company's business and is unrelated to any employee concern involving the terms and conditions of employment.

The employee agrees to refrain from engaging in any type of communication, electronic, written or verbal, with third parties in an effort to directly or indirectly disparage or injure the company, or from assisting others in doing so, or from otherwise engaging in or assisting others in negative activities with respect to the company, including in the commercial marketplace, financial marketplace and broadcast media, including print, television, radio and Internet. However, this Non-Solicitation & Non-Disparagement Policy does not prohibit an employee from engaging in such communications that are intended to address employee concerns involving the terms and conditions of employment. This non-disparagement provision does not prohibit or restrict the Employee from communicating with any government agencies or otherwise participating in any investigation or proceeding that may be conducted by any government agency, including by providing documents or other information, without notice to the company, and without waiving any right to receive an award for providing any such documents or information.

3. Enforceability

The employee hereby acknowledges and agrees that the restrictions contained in this Non-Solicitation & Non-Disparagement Policy are necessary for the reasonable protection of the company. The employee agrees that, in the event of any breach or threatened breach of any provision contained in this Non-Solicitation & Non-Disparagement Policy, the company shall have the right, in addition to any other rights or remedies it may have: (a) to a temporary, preliminary or permanent injunction or injunctions and temporary restraining order or orders to prevent breaches of such provisions and to specifically enforce the terms and provisions thereof without having to post bond or other security and without having to prove special damages or the inadequacy of the available remedies at law; and (b) to require the employee to account for and pay over to the company all compensation, profits, monies, accruals, increments or other benefits derived or received by him or her as a result of any transaction constituting a breach of any of the provisions of this Non-Solicitation & Non-Disparagement Policy.

POSITIVE WORK ENVIRONMENT POLICY

1. Overview of the positive work environment policy

Everise is committed to maintaining an environment that is safe and respectful; our shared success depends on it. Accordingly, we do not tolerate workplace discrimination, violence, or harassment.

All directors, officers and employees have a duty to ensure a safe and respectful workplace environment where high value is placed on integrity, fairness, and respect. In order to achieve this goal, Everise has established this Positive Work Environment Policy (“**PWE Policy**”) which relies on everyone in our workplace not only to refrain from these behaviors, but also to identify and report workplace discrimination, violence and harassment as it occurs.

If you experience or become aware of what you believe to be discrimination, violence, or harassment in the workplace, as defined in this policy, you are expected to report it either to your supervisor, Human Resources, or to Everise reporting hotline. If you or someone you know at Everise is in immediate danger of serious bodily harm, first call local law enforcement authorities and then report the incident following the process explained herein.

Complaints of workplace discrimination, violence or harassment will be taken seriously. If you are found to be discriminating against, acting, or threatening to act violently towards, or harassing any individual at Everise, or if you knowingly condone the discrimination of, violence towards, or harassment of another individual at Everise, depending on the seriousness of the case, you will face corrective action up to and including termination shall be considered.

A culture of reporting when it comes to workplace discrimination, violence and harassment is essential for us as a company to maintain a safe and respectful workplace. While we reserve the right to take corrective action if you knowingly make a false accusation about an innocent party, you will not face retaliation for making a good faith report or assisting in the investigation of a complaint.

2. Commitment to a positive work environment

Integrity, fairness, and respect are hallmarks of our culture, and we are committed to a positive, open and inclusive work environment free from discrimination, violence and harassment. Each of us has a personal responsibility to our colleagues and to Everise to take an active role in achieving a safe and respectful work environment.

3. Scope of the policy

This PWE Policy applies to all directors, officers, employees and temporary workers (collectively, “you” or “Employees”) of Everise.

All Employees are required to comply with the personal behavior and positive work environment requirements set out in the company's Business Code of Conduct. This PWE Policy supplements and expands on those provisions and is intended to raise awareness of our approach to fostering a positive work environment among Employees. You must also comply with applicable laws, rules and regulations governing the subject matter of this PWE Policy. In the event that a local law, rule or regulation (collectively, "Local Laws") in a jurisdiction in which we conduct business is more restrictive than this PWE Policy, or where this PWE Policy is inconsistent with Local Laws, the Local Laws will apply. For further guidance, please refer to any country-specific appendices attached to this PWE Policy which are applicable to you.

This PWE Policy reflects the standards that Everise expects its business associates, partners, agents, contractors, third-party service providers and consultants (collectively, "Third Parties") to adhere to when interacting with Everise and its Employees.

For the purposes of this PWE Policy, a "business associate," "partner," "agent," "contractor," "third party service provider" or "consultant" means an individual or entity, including a subcontractor, that provides and receives payments for services or goods related to any aspect of our business.

For the purposes of this PWE Policy, "Work Environment" or "Workplace" means Everise places of business and business-related electronic communications, and outside Everise places of business when conducting business (for example, all places where Employees perform their duties (including but not limited to company buildings and company grounds), company-sponsored functions, recreational or social events, and travel, or company business over the telephone and internet/intranet or any other form of communication).

4. No tolerance for workplace discrimination, violence & harassment

Everise strictly prohibits Workplace Discrimination, Violence and Harassment (as defined below). This PWE Policy outlines our commitment to providing a Workplace free of Discrimination, Violence and Harassment and summarizes the responsibilities of Employees to understand: (i) what constitutes Workplace Discrimination, Violence and Harassment, respectively; (ii) their obligations to maintain an environment where these behaviors are not tolerated; and (iii) how to report incidents following proper procedures. If you contravene this PWE Policy, you will face corrective action up to and including the termination of your employment with Everise.

4.1. Definitions of workplace discrimination, violence & harassment

Workplace Discrimination means the differential treatment of an individual or group, such as the denial of an opportunity, based on any characteristic protected by applicable law, including, without limitation:

- Race

- Color
- Sex, gender (including pregnancy) or gender identity
- Marital status
- National origin
- Religion
- Age
- Physical or mental disability
- Sexual orientation

In some circumstances, Discrimination may be unintentional. Regardless of intent, such conduct is not acceptable, violates this PWE Policy and may also constitute a violation of applicable law.

Workplace Violence means an action (oral, written or physical) which causes, is intended to cause, is capable of causing, or could reasonably be interpreted as a threat to cause death or bodily injury to oneself or others, or property damage. Workplace Violence includes, but is not limited to, the following behaviors:

- The use of physical force against or by a person that causes or could cause physical injury, including physical acts such as punching, hitting, kicking, pushing, damaging property or throwing objects;
- The attempted use of physical force against or by a person that could have caused physical injury; and
- An action, statement or behavior (or series of actions, statements or behaviors) reasonably believed to be a threat of physical harm or a threat to safety or security in the Workplace. This can include:
 - Bringing or threatening to bring a weapon of any kind into the Workplace.
 - The potential for domestic violence to have an impact on the Workplace.²

Where required by Local Law, risk assessments regarding Workplace Violence will be conducted in accordance with the process outlined in the attached [Appendix B](#).

Domestic violence is an act of violence committed against an individual by that individual's spouse or family member. If you become aware that domestic violence may occur in the Workplace, you must report your concern using this PWE Policy.

Workplace Harassment means conduct which a reasonable person ought to know is unwelcome and includes conduct (e.g., comments and actions) which would be

perceived by a reasonable person as being hostile, humiliating or abusive or cause him/her torment. Harassment covers a wide range of conduct, and includes Sexual Harassment, Bullying and Psychological Harassment (as defined below). It may be targeted at a person or group of people because of a personal dislike or personality conflict, and not solely because of race, religion, color, sexual orientation, or any other prohibited grounds.

Workplace Harassment may be expressed through offensive oral, written or physical conduct that singles out a person to the detriment or objection of that person. Workplace Harassment includes Sexual Harassment, bullying, teasing, offensive jokes, innuendos, displaying or circulating offensive pictures or materials, offensive or intimidating conversations, making fun of or defaming a member of a particular religion, race, gender, etc. or similar forms of behavior.

Workplace Harassment does not include reasonable actions taken by the company relating to the management and direction of Employees or the Workplace. Indeed, Workplace Harassment is not to be confused with the normal exercise of the company's rights with respect to its Employees, in particular its right to assign tasks, do a follow-up and/or monitor the work of an Employee whose output is unsatisfactory, conduct performance reviews and appraisals, reprimand or impose disciplinary sanctions, and/or investigate alleged misconduct.

Insofar as the company does not exercise these rights in an arbitrary, abusive or discriminatory manner, or outside the normal conditions of employment, the company's actions and those of its Employees do not constitute Workplace Harassment. Workplace Harassment does not include differences of opinion or minor disagreements between co-workers.

In some circumstances, Workplace Harassment may be unintentional. Regardless of intent, such conduct is not acceptable, violates this PWE Policy and may also constitute a violation of applicable law.

For clarity, the following are three specific types of Workplace Harassment included under this PWE Policy:

(a) *Sexual Harassment*

Sexual Harassment is unwelcome sexual behavior (physical, spoken or written) which could reasonably be expected to make a person feel offended, humiliated, or intimidated and includes:

- engaging in a course of hostile, humiliating or abusive behavior against a person in the Workplace because of sex, sexual orientation, gender identity or gender expression; or
- making a sexual solicitation of or advance toward an Employee where the person making the solicitation or advance is in a position to confer,

grant or deny a benefit or advancement to such Employee and the person making the solicitation or advance knows or ought reasonably to have known that the solicitation or advance is unwelcome.

Sexual Harassment, by definition, is coercive and one-sided, and persons of any gender can be victims of it.

(b) *Psychological Harassment*

Psychological Harassment includes hostile, humiliating or abusive behavior that manifests itself in the form of conduct, verbal comments, actions, or gestures characterized by the following four criteria:

- Repetitive;
- Hostile or unwanted;
- Affects the person's dignity or psychological integrity; and
- Results in a harmful work environment.

Psychological Harassment may come from a superior, colleague, a group of colleagues, a client or a supplier. A single serious incident of such behavior may also constitute Psychological Harassment if it undermines the person's dignity or psychological or physical integrity and if it has a lasting harmful effect.

(c) *Bullying*

Bullying includes repeated, malicious, severe or pervasive oral, written or physical mistreatment that a reasonable person would consider offensive, degrading or humiliating to one or more individual(s) in the Workplace. A bully need not be in a position of authority and, unlike Discrimination, the Bullying conduct need not relate to the targeted individual's status as a member of a legally protected group. Bullying is characterized by willfully targeting another person or persons and socially degrading the person(s), or engaging in similar behavior, that causes or reasonably ought to have been expected to cause another person(s) to develop deep seated fears and/or adverse health effects that would affect a reasonable person's ability to function normally.

Bullying may include, by way of example:

- Physical or psychological threats;
- Exclusion or social isolation, or the encouragement of others to turn against the targeted person;

- Unreasonable interference with a person's ability to do his or her work; or
- Personal attacks.

5. Employee, Supervisor & Senior Management Responsibilities

5.1. *Employee Responsibilities*

- Understand and comply with this PWE Policy;
- Behave in a manner consistent with creating a positive Work Environment and maintain positive interactions at work;
- Report incidents of Workplace Discrimination, Violence or Harassment experienced directly or witnessed;
- Immediately report any violent or potentially violent incident as outlined in this PWE Policy;³
- Participate and cooperate in any investigations of Workplace Discrimination, Violence or Harassment if, and to the extent required, by the circumstances of the investigation; and
- Understand and follow organizational procedures to prevent Discrimination, Violence and Harassment, including addressing it as soon as you are aware.

5.2. *Supervisor Responsibilities*

All supervisors and managers (i.e., Employees to whom other Employees report) should strive to create a work environment in which Employees feel comfortable reporting incidents and raising concerns or questions about Everise policies. This includes:

- Understanding how to recognize and handle a workplace Discrimination, Violence or Harassment incident or complaint so that it does not go unaddressed;
- Managing interpersonal conflicts within the team before they escalate;
- Encouraging Employees to report incidents or complaints of Discrimination, Violence or Harassment, or escalate all complaints to Human Resources (even those about his/her own behavior); and
- Participating and cooperating in any investigations of Workplace Discrimination, Violence and Harassment if, and to the extent required, by the circumstances of the investigation.

³ In the event of an extreme or imminent threat of physical harm to themselves or any person, you should contact law enforcement (e.g., Police) using emergency procedures.

5.3. *Senior Management Responsibilities*

The senior executives of Everise (the “Senior Executives”) are responsible for taking reasonable measures to:

- Establish a “tone from the top” reflective of a positive Work Environment;
- Protect Employees from Workplace Discrimination, Violence and Harassment;
- Promote a Work Environment where Employees are comfortable reporting violations;
- Implement a program where complaints are dealt with in an appropriate and timely manner, as required; and
- Provide training as deemed appropriate or where required by law.

6. **Reporting Incident & Complaints**

Internal reporting is important to Everise and it is both expected and valued. If you experience or witness behavior that you believe may violate this PWE Policy, you are expected to promptly report it.

Reports should in the first instance be made to your supervisor or manager, who will ensure that the information is properly handled and escalated as necessary. If you are unsure about the appropriate avenue for reporting because of the nature or the content of the report, or otherwise, reports should be made to your local Human Resources (HR) contact. If you are not comfortable reporting an incident to your supervisor or manager, or to HR, you can report through our reporting hotline (the “Reporting Hotline”). The Reporting Hotline is managed by an independent third party and allows for anonymous reporting in English and other languages. The Reporting Hotline is available toll-free; 24 hours per day, 7 days per week. Please see [Appendix A](#) for the Reporting Hotline phone numbers by jurisdiction.

7. **Responding to reported incidents & complaints**

7.1. *Handling of Incidents and Complaints*

Everise takes all incidents and complaints of Workplace Discrimination, Violence and Harassment seriously. Incidents or threats of Workplace Violence may be reported to law enforcement, as appropriate.

Every report of Workplace Discrimination, Violence or Harassment will be assessed and, where appropriate or as required by law, an investigation, including discussions with all applicable parties, will be undertaken. The company will determine who will conduct the investigation depending on the circumstances. In some circumstances, the company may, at its discretion, retain an independent third party to conduct the investigation.

When an investigation has taken place, if appropriate and as required by law, the complainant and respondent will be informed of the results of the investigation and any corrective action that has been or will be taken as a result of the investigation. In such cases, the results of the investigation will be provided within a reasonable period of time after completion of the investigation.

Confidentiality and privacy will be respected to the extent possible, subject to the need to conduct a full, fair and respectful investigation and to ensure the safety of Employees and comply with applicable law. Everise will take any reasonable action deemed necessary for the protection of Employees and of the Workplace. It is expected that anyone participating in an investigation keep that fact and any details discussed during the investigation confidential. A breach of this requirement for confidentiality will be dealt with and may lead to serious consequences, up to and including termination of employment.

7.2. *Precautions During Investigations*

The company will also take every precaution reasonable to protect the involved Employees during the investigation, including but not limited to moving involved Employees to different locations, floors or offices during the investigation. Precautionary measures, if warranted, may be in place until an ultimate determination is made related to the investigation, and if required, corrective actions are applied.

7.3. *Workplace Discrimination, Violence or Harassment Involving a Third Party*

If an incident of Workplace Discrimination, Violence or Harassment involves a Third Party in the Workplace (e.g. client, contractor, visitor, etc.), the above process will apply. Where deemed appropriate, the company will report the incident to that person's employer and any other parties which the company believes it is appropriate to report to under the circumstances. The company will take reasonable steps, including removing the individual from its property and/or involving law enforcement as appropriate, to ensure the safety and protection of all Employees and the Workplace.

7.4. *False Claims of Workplace Discrimination, Violence or Harassment*

Allegations made in bad faith may lead to corrective action, up to and including termination of employment.

7.5. *No Reprisal or Retaliation*

Everise will not tolerate retaliation against anyone who has made a complaint or report based on the reasonable good faith belief that a violation of this PWE Policy has occurred or may occur in the future, or has cooperated honestly and completely with an investigation regarding a violation or possible violation of this PWE Policy. Any such person will be protected from any form of retaliation. No documentation

whatsoever will be placed in the personnel file of anyone who has made a complaint or report in good faith, whether the claim is upheld or not.

A reprisal or retaliation can include a demotion, an unwanted transfer or a denial of opportunities within the company. Any person who believes that they have been reprimanded or retaliated against should immediately contact their local HR representative or the Reporting Hotline.

Employees who engage in reprisals or threats of reprisals, or who knowingly make a false complaint or otherwise abuse this PWE Policy, and depending on the seriousness of the case, may be disciplined up to and including immediate termination of employment shall be considered and, if warranted, legal proceedings may be undertaken. Such discipline is not a reprisal or breach of this PWE Policy.

7.6. ***Record Keeping***

At the conclusion of an investigation, a written report of the findings may be prepared as appropriate or where required by law. The report or its findings will not be disclosed to any person unless the disclosure is necessary for the purposes of investigating or taking corrective action with respect to the incident or complaint, is determined appropriate by Everise or is required by law.

Where required by law, records of the investigation will be kept, including a copy of the complaint or details of the incident, a record of the investigation (including notes taken), a copy of the investigation report, a summary of any communications of the results of the investigation to the parties involved, and, if applicable and/or appropriate, a copy of the corrective action taken to address the complaint or incident of Workplace Discrimination, Violence or Harassment and the steps taken to protect Employees and prevent a recurrence. Records will also be kept in accordance with applicable laws.

8. Enforcement & Corrective Action

Everise will take corrective action with respect to any Employee found to have breached this PWE Policy in a manner that is fair, consistent and that reflects the nature and facts of the violation. Anyone subject to this PWE Policy who violates it may face corrective action. Corrective action may include counselling, training, a written warning, transfer, demotion, reductions in short-term or long-term compensation, suspension with or without pay, and depending on the seriousness of the case or termination of employment or the business relationship. The incident will, if substantiated, be documented in the offending person's file.

If we discover a violation of any applicable laws, we may refer the matter to the appropriate authorities, which could lead to penalties, fines, imprisonment or other liability.

This PWE Policy does not limit the company's authority or ability to discipline or take other action for Workplace conduct that is found to be inappropriate, regardless of whether that conduct meets the definition of Workplace Discrimination, Violence or Harassment as documented in this PWE Policy.

9. Approval & Amendments

The Board of Directors of Everise and the Senior Executives have reviewed and approved this PWE Policy. The Senior Executives are responsible for monitoring compliance with this PWE Policy's provisions.

At a minimum, this PWE Policy will be reviewed annually by the company. Everise reserves the right, in its absolute discretion, to supplement, change, discontinue or amend its policies and procedures at any time without consultation with any Employee.

Any amendments to this PWE Policy must be approved by the Senior Executives, together with any other procedures required by Local Law.

PRIVACY POLICY

1. Objective

The objective of this Privacy Policy is to outline various guidelines pertaining to the privacy of personal data in conjunction with applicable central and state law.

2. Scope

This Privacy Policy is applicable to all company employees or contract personnel.

3. Guidelines

3.1. *Company Personnel Files*

The company maintains accurate and complete employee files regarding all employees. Personnel files are confidential records that contain employment records and belong to the company. These files for the most part are maintained in Emplx. Where historical data is not in Emplx there may be paper files in the Human Resources Department. In accordance with company's policies, supervisors may retain copies of some employee records, such as performance evaluations, non-medically related requests for time off, and/or disciplinary records in departmental files. However, the supervisor is responsible for maintaining the confidentiality of these records, limiting access to them and ensuring that the department does not keep the originals of any records. Supervisors may keep only copies of documents that they have sent to the Human Resources Department. After a supervisor has used a document for its intended purpose, he must promptly send the original to the human resources department. In maintaining its personnel files, the company will comply with all applicable local, state and federal laws.

- The company also keeps all employees' health-related information, including but not limited to pre-employment physicals, drug screen results, in a separate set of confidential files.
- Only designated classes of employees, Human Resources managers, have access to records related to health plan administration. Except for those records that indicate whether or not an employee is participating in the health plan, records used for health plan administration purposes will not be filed in either an employee's personnel file or his confidential medical file. All other information related to health plan administration will be kept in files that are separate and distinct from the company's personnel files. No information used for health plan administration purposes will be used for any other purposes or considered in any employment-related decisions.
- Only designated individuals and the HR Department have access to employee personnel files. Supervisors may request access to the personnel files of the individuals who report to them, but they will not have access to confidential medical files. Supervisors must request access to their team's files by contacting the HR Manager at their site.

- Employees may have access to their files in accordance with company's policies and applicable law. Unless approved in advance by the Country HR Head, no employee can remove personnel files from the area designated for file review. If an individual is granted the authority to view a file in another location, he/she must complete the appropriate form to "check out" the file and must promise to protect its confidentiality and return the file completely intact by the due date indicated on the "check out" slip.

3.2. *Authorization for Release of Medical Information*

The company recognizes and respects its employees' rights to privacy, including the right to maintain the confidentiality of their personal medical information. However, under certain circumstances, the company may require employees either to provide specified medical information to a company representative directly or provide the company with an executed authorization form that directs a health care provider to disclose specified information to the company. The company will require such releases when they are necessary to comply relevant applicable laws or company policies. Examples of the types of medical records the company may require or situations when the company may require employee medical information include, but are not limited to:

- Records related to workers' compensation, occupational injury and/or workplace medical surveillance.
- Records related to sick leave requests and/or justifications for sick leave.
- Records obtained for the purpose of determining disability and/or life insurance eligibility.
- Pre-employment physicals.(if applicable/available)
- The results of drug screens. (if applicable/available)
- Fitness for duty test results. (if applicable/available)

When the company asks an employee to execute an authorization for a health care provider to release medical information, it will provide the employee with an authorization form that sets forth the parameters of the requested use and disclosure of information. The authorization will identify the information to be disclosed, the party to whom the information should be disclosed and the purpose of the requested disclosure. The company will keep all employees' health-related information in set of confidential files that are maintained separately from employee personnel files. Employees may have access to their files in accordance with company's policies and applicable law.

3.3. *Duty to Report Violations*

Each employee has a duty to report suspected violations of this Privacy Policy either through a phone call or a letter. There will be no retribution against any employee

reporting violations in good faith. Violations can be reported to an employee's supervisor, the Human Resources Department or Country HR Head.

3.4. *Client Notifications*

Should a request for information or a violation of this Privacy Policy be submitted, the below steps must be followed:

- Immediate escalation to Leadership by the appropriate Client Services Person In Charge
- The Client Services Person in Charge with the consent of the Site Head will communicate directly with the client within a reasonable time frame;
- All client policies and procedures will be strictly adhered to with the company's full cooperation; and
- The company will partner with a client to track and monitor a potential privacy breach until closure of the issue is mutually reached with the client.

Violations of this Privacy Policy may result in suspension of work duties, removal of responsibilities, demotion, termination and/or criminal and financial penalties. Self-reporting a violation will not excuse the violation itself. However, the extent and quickness of reporting will be considered in determining appropriate actions.

EVERISE DATA PRIVACY STATEMENT FOR EMPLOYEES

Everise (India) BPO Services Limited, a member of the Everise group of companies ("Everise India," "company," "us," "our," and "we") is committed to the protection of personal and sensitive personal information of its employees, clients, client's customers, vendors, and other third parties whose information it holds or in its possession from unauthorized or illicit use and processing in accordance with privacy regulations.

To ensure that you can make informed decisions and feel confident about supplying your personal and sensitive personal information to us and in processing personal information of our clients, customers, vendors and other persons whose personal information you hold, process or encounter during your employment with the company, we are providing you this Data Privacy Statement ("Privacy Statement") which outlines our data collection, usage, retention, disclosure and disposal practices in respect of your personal information, your rights as data subject and your obligations towards any data you process in the course of your work. This Privacy Statement is effective as of 04 September 2020.

This Privacy Statement also aims to explain how Everise India and its affiliated entities process your personal information, who has access to it, for how long the information is kept and how it is kept secure.

1. What is Personal Information?

When we refer to personal information we mean information that identifies or can identify a specific individual. We may collect personal information about you, your working relationship with the company, and where necessary, references to information about third parties such as your spouse, children (if any) and/or dependents (collectively, "Dependents"). In the course of your work, you will also find yourself dealing with personal information of others, particularly of your fellow employees, our clients and their customers, vendors, subcontractors and even guests. Thus, in the employment context, personal information may refer to any of the following:

- (a) *Personal details:* name, email, phone numbers, residential address, gender, status, photograph, Viber, WhatsApp, WeChat or similar accounts.
- (b) *Immigration information:* citizenship, passport data, details of residency, work permits, visa.
- (c) *Compensation and payroll:* remuneration or salary details (including base pay, bonus, incentives, etc.), overtime, compensation type, frequency,
- (d) *salary reviews, performance appraisals, bank details, time records* (including vacation and other absence records, leave status, hours worked and shift hours), pay data and termination date, compensation details.
- (e) *Position:* description of current position, job title, corporate status, management category, job code, job functions, legal employer entity,

location, employee identification number, terms of employment, work history, hire/rehire and termination date(s) and reason, length of services, retirement eligibility, promotions, disciplinary records, transfer dates, reporting managers information.

- (f) *Talent Management Information: details contained in letters of application and resumes (previous employment background, school or education history, professional qualifications, language and other relevant skills, certification, certification dates and expiry dates), information to complete or initiate background check, details on performance management, ratings, learning and training programs, training scores, performance reviews, relocation information and other information which may be necessary to populate employee's work biographies.*
- (g) *Management Records: details of any stock ownership, dividend information or directorships.*
- (h) *System and Application Access Data: information required to access company systems and applications such as system ID, LAN ID, email account, instant messaging account, system passwords, access logs, activity logs, employee status, and other electronic content which may be necessary to use company systems.*

Depending on the urgency of the vacancy, the company may employ different means to gather your Personal Information, which includes but not limited to:

- (i) Email (Outlook Mail)
 - (ii) Postal Mail
 - (iii) Telephone Calls
 - (iv) Text Messages
 - (v) Fax
 - (vi) Accomplishing Forms (Both for Internal and External Purposes)
 - (vii) Logging in and Out of the company's Systems
- (i) Other Sensitive Personal Information: date of birth, ethnic origin, marital status, sexual orientation, age, color and religious, philosophical or political affiliations, physical, physiological and mental health condition, medical record and history, biometric information, passwords, genetic or sexual life, any proceedings for any offense committed or alleged to have been committed, disposal of such proceeding or sentence of any court, financial information such as bank a/c or credit card or debit card or other payment

instrument details, those issued by any government agency peculiar to an individual which includes, but is not limited to social security numbers.

2. How do we use Personal Information

Your personal information will be collected, used, accessed, transferred or otherwise processed before and during your employment with the company to establish, maintain and manage the employment relationship between you and the company and for other legitimate business reasons (e.g., conducting investigations, audits, managing talent or diversity programs, process improvements, comply with contractual obligations). We also process your personal information for:

- (a) **Managing workforce:** Managing work activities and personnel generally (including recruitment, appraisals, performance management, client projects onboarding or roll offs, promotions, succession planning, rehiring, salary administration, performance or wage reviews, awards and incentives, healthcare, pension plan, training, leave management, promotions, transfers, engagement and recreational activities); providing employment references; managing company or government loans; performing workforce analysis and planning; performing employee surveys or background checks; managing coaching actions; disciplinary matters; grievances and terminations; reviewing employment decisions; making business travel arrangements; managing business expenses and reimbursements; planning and monitoring of training requirements and career/skill development activities; and creating and maintaining internal employee directories.
- (b) **Communications and Emergencies:** facilitating communication to employees and their nominated contacts in emergency situations; ensuring business continuity, providing references and recommendations; protecting the health and safety of employees; and safeguarding IT infrastructure and other assets.
- (c) **Business Operations:** operations and managing IT and communications systems; IT security operations and related support; development and maintenance services; managing products and service development; improving products and services; managing company assets; allocating assets to human resources; strategic planning; project management; business continuity and disaster recovery; compilation of audit trails and other reporting tools; maintaining records relating to business activities; budgeting; financial management and reporting; and managing mergers, acquisitions, sales, reorganizations and integrations.
- (d) **Compliance:** complying with legal and other requirements such as incometax, recordkeeping and reporting obligations to government agencies; conducting audit or government inspections and other request from government or local authorities; protecting legal rights and pursuing remedies; defending litigation and managing internal claims or complaints,

conducting investigations and complying with internal policies and procedures; protecting privacy, safety of people and property of the company; protecting against fraud or crime; or for risk management purposes.

- (e) Corporate Investigations and Asset or Resources Management: monitoring activities of employees to the extent allowed by law (including monitoring of email, internet and resource use of employees) and conducting internal investigations, inspections, and audits.
- (f) Data Analytics: analyzing data to describe and improve business performance; create and drive marketing and recruitment campaigns; create promotional and engagement activities and employee or customer experience; and improve talent or employment management.

In the course of your work, you may be processing personal information of other employees, clients, client customers, vendors, and others whose information we hold or is in our possession pursuant to a contractual relationship or any other legitimate purpose. When you do handle such information, you must only do so for business purposes in accordance with company policies and pursuant to reasonable instructions for processing and sharing.

3. How do we transfer Personal Information

Since the company is part of a global organization with global IT systems, any personal information we collect may be routed, stored or transferred internationally throughout the worldwide organization¹ and sometimes, to third parties for our business purpose. We have internal policies to ensure an equivalent level of protection is in place across our global organization. The company only shares personal data within the organization if and as far as necessary for the purposes specified in this Privacy Statement.

Access within the company and across entities shall only be limited to those who have a need to know the information for the above-mentioned purposes, and may include your managers and their designees, global or local personnel in HR, IT, Legal & Compliance, Facilities, Finance, Marketing & Communications, and Internal Audit. Thus, we made sure that any employee processing personal information is bound by confidentiality under their Employment Contracts.

The company does not usually share personal data with any third party outside of the organization unless one of the following circumstances applies:

- (a) When it is necessary for the purposes. We may share personal data with third parties to the extent that a vendor's services or access or a client's requirements foresee or require such disclosure, and your personal data was submitted for such purpose. We may share personal data with our parent

company and affiliated companies and other service providers that support us in the realization of the purposes specified in this Privacy Statement.

- (b) When required by law or for legal reasons. We may share personal data with third parties if we have good-faith belief that their access to and use of the personal data is necessary: (a) to meet any applicable law and/or court order, (b) to detect, prevent or otherwise address fraud, security or technical issues, and/or (c) to protect the interests, properties or safety of us, our employees, clients and guests, or the public, in accordance with the law. We will notify you about such disclosure, as far as reasonably possible
- (c) In relation to corporate restructuring. If we are in a process of merger, acquisition or asset sale, we may transfer personal data to the involved third party. We continue to ensure the confidentiality of all personal data.
- (d) Upon your consent, we may share personal data with third parties for reasons other than the above-mentioned if we obtained your explicit consent to do so. You have the right to withdraw this consent at any time.

Third parties are also expected and required to protect the security of your personal information and to only use such information for the provision of services to the company and in compliance with applicable laws. Any third party who may come in contact with your personal data is also obliged to keep and treat your personal data confidential

Third parties who may obtain your Personal Data for the abovementioned purposes are vendors, subcontractors and clients who will need to know your Personal Information for legitimate business purposes. Vendor or subcontractors such as providers for health and life insurance, background checks, clinic management, external payroll, banks (payroll), engagement partners, data analytics, actuarial studies, financial audits, and other similar services which are utilized by the company to manage your employment, administer your benefits, conduct business activities and perform other employment-related functions.

The following companies (with corresponding location) are affiliated with C3: [THIS LIST WILL CHANGE DEPENDING ON WHAT ENTITY THE STATEMENT APPLIES TO.]

- (1) C3/Customer Contact Channels Inc., USA
- (2) C3/Customer Contact Channels Philippines Ltd.
- (3) Trusource Labs, LLC, USA
- (4) C3/Customer Contact Channels Guatemala Limitada., Guatemala
- (5) Everise Holdings Pte. Ltd., Singapore ("Everise")
- (6) Trusource Labs Ireland Limited, Ireland

- (7) Other companies that may be controlled by Everise or under common control with Everise or that control Everise now or in the future

4. How do we keep Personal Information secure?

The company will take appropriate measures to protect personal information consistent with applicable privacy and data security laws and regulations, including requiring service providers to use appropriate measures to protect the confidentiality and security of personal information.

To keep your personal data secure, we have implemented the following security measures:

- (a) Secure operating environments. We store your data in secure operating environments and only accessible to the company's employees, agents and contractors on a need-to-know basis. The company also follows generally accepted industry standards in this respect.
- (b) Encryption. We use industry-standard encryption to provide protection for information that is transmitted to us.
- (c) Prior authentication for IT access and access to premises. We require our employees and contractors to verify their identity (e.g. through login ID and badges) before they can access IT resources and business premises to prevent unauthorized access.
- (d) Audit. We audit the application of our security measures and ask third party experts to review our security controls against international standards to help us to further improve our security level.

Should despite of our security measures, a security breach occur that is likely to result in a risk to your privacy, we will inform you and other affected parties, as well as relevant authorities, when required by applicable data protection law, about the security breach as soon as reasonably possible.

5. How do we ensure data integrity?

The company will take reasonable measures to establish that the personal information processed is relevant for its intended use and is accurate and complete for carrying out the purposes described in this Privacy Statement. It will retain personal information as long as it has a relationship with you. After the contractual relationship ends, the company shall keep it for a period of 4 or 10 years depending on the data in accordance with the statutory period of limitations imposed by law or mandated by the company's contractual relationships with third parties. (Please refer to the company's Record Retention Matrix for the details.) On the other hand, images captured by CCTV or security cameras in and around the company premises are kept for three (3) months from date of recording, except when otherwise requested by enforcement authorities and / or the Legal Department in cases where

the recorded images show possible policy violation, criminal activity or incidents that require investigation.

6. What are your rights?

The company acknowledges your rights as data subjects. Hence, as an employee, you have the following rights over your Personal Data:

- (a) Right to be informed. You have the right to be informed that your personal data will be, are being or were collected and processed by the company. You may also contact us to get confirmation that we are processing your personal data.
- (b) *Right to access.* You may request that we provide you with a written description of information that we have about you as well as the purpose for holding or processing them. You may also request for a copy of your information which the company will provide in a commonly portable format (e.g. a printed copy of any soft copy files you have requested, or a photocopy of the document you are requesting) within a month from date the request was made.

However, the company is not generally required to undertake endless and disproportionate searches for information in order to respond to a request and the company may refuse your request if:

- The relevant personal data is not in the company's possession or control;
- The request is identical or similar to the one you have recently requested;
- The request is obviously unfounded or frivolous;
- Harm would arise or likely arise from disclosure (for example, if disclosure would be likely to prejudice a criminal investigation or unduly prejudice someone's commercial interests); or
- Other cases allowed by law.

In case your request is declined, we will provide you a formal notification indicating the grounds for declining your request.

- (c) Right to withdraw consent. In case our processing is based on consent, you may withdraw the consent at any time by contacting us. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal data conducted in reliance on lawful processing grounds other than consent.
- (d) Right to rectification or correction. You have the right to have inaccurate or incomplete personal data we store about you rectified or completed,

provided that the information is/are not necessary for compliance with a regulatory obligation and it is not necessary to establish, exercise or defend legal claims. If such personal data has been disclosed to a third party in accordance with this Privacy Statement, then we shall also ask them to rectify or update your personal data.

- (e) Right to object to or restrict processing. In case our processing is based on our legitimate interest to run, maintain and develop our business, you have the right to object at any time to our processing. We shall then no longer process your personal data unless there are other compelling legitimate grounds for our processing that override your interests, rights and freedoms, or it is necessary to establish, exercise or defend the company's legal claims or support our obligations. This right may be exercised upon discovery and substantial proof that personal data was obtained or processed unlawfully.
- (f) Right to data portability. As mentioned above, you have the right to receive your personal data from the company in a structured, commonly used and machine-readable format and to independently transmit those data to a third party, in case our processing is based on User's consent and carried out by automated means.
- (g) Right to erasure. You have the right to have personal data we process about you erased from our systems if the personal data are no longer necessary for the purposes specified in this Privacy Statement. Upon your request, we will also erase data when you withdraw your consent or object to our processing, unless we have a legitimate ground to retain the data. We may not immediately be able to erase all residual copies from our servers and backup systems after the active data have been erased. Such copies shall be erased as soon as reasonably possible.

To exercise any of the above-mentioned rights, please send us a letter or email to the address set out below, including the following information: name, address, phone number, email address and a copy of a valid proof of identity. We may request additional information necessary to confirm your identity. We may also reject requests that are unreasonably repetitive, excessive or manifestly unfounded.

Data Protection Officer
C3/Customer Contact Channels Philippines Ltd.
20th Floor Bonifacio One Technology Tower
Rizal Drive corner 31st Street, Bonifacio Global City Taguig City,
Philippines 1634
Tel. No.: +632 5534671
Email: dataprivacy@weareeverise.com

What are your obligations?

In conjunction with your rights, you have a responsibility to keep your personal details accurate and up to date, which can be done through Emplx, HR Files and other office systems. You should notify the appropriate channels of any changes to your personal information.

In the course of doing your work, you may have access to personal information about other individuals. You are expected to treat any such personal data in a responsible and professional manner consistent with the company's Privacy Policy. This responsibility is in addition to any obligations arising from professional / business ethics or our Code of Conduct.

Any third-party personal information which was obtained in the expectation of a duty of confidentiality should be treated in the strictest confidence and cannot be disclosed without proper authorization. As an employee, you are also expected to comply with data protection and security clauses that were executed as part of our standard terms of business and/or service contract(s) with our clients, vendors and other third parties with whom we partner or do business.

Finally, you have the responsibility to report any breaches of data security (including but not limited to, unauthorized use, sharing, access or disclosure, malicious or unintentional disclosure, and other policy violations) immediately to the Data Protection Officer (DPO)

7. Any Updates?

We may amend this Privacy Statement from time to time and the updated version shall apply and supersede any and all previous versions. We will inform you through email or other mode of communication to keep you up to-date of the changes in our Privacy Policy.

8. Where do I go if I have questions about this Privacy Statement?

If you have concerns about how the Company processes personal information or if you have any questions about this Privacy Statement, please contact the Company's DPO as provided in the above-mentioned Section 6

9. Where do I go if I have questions about this Privacy Statement?

If you have concerns about how the company processes personal information or if you have any questions about this Privacy Statement, please contact the company's DPO as provided in the above-mentioned Section 6

PROGRESSIVE COACHING PROCESS

To ensure compliance with company policies and sustained performance expectations, Everise India has in place a coaching and counseling process that is intended to improve performance when, in the opinion of management, improvement is warranted. Employees at all levels should be open to feedback and respond accordingly.

The disciplinary action process is subject to the severity of the offense but could commence at any of the following steps.

1. First Warning / Coaching Statement

If undesirable action or performance occurs, this warning is issued to make the employee aware of any gap in behavior or performance and create awareness for immediate corrective action.

2. Second Warning

If an undesirable action or performance is repeated, the employee is given a written warning and a documented coaching session with up to a 30-day corrective action plan by his/her Supervisor. The purpose of this meeting is to discuss the behavior or performance gap in more detail and collaborate on a solution with the employee.

3. Final Warning

The employee is given a final written warning and documented counseling session with up to a 30-day corrective action plan by his/her Supervisor. Termination of employment may occur if immediate corrective action is not taken.

4. If similar action continues, pending the circumstances, termination of employment may occur. Termination as a result of disciplinary action must be approved by the Chief People Officer or their designee.

5. An employee may also be placed on a Performance Improvement Plan (PIP). The PIP process may run concurrently with the coaching and counseling process or in place of it. During the PIP period, regular meetings and feedback between the employee and his or her Supervisor are required.

6. Suspension

At Everise India, suspension is not used as a form of disciplinary action. An employee is suspended when, in order to thoroughly investigate an issue, management determines it is best that the employee not be at the workplace. The employee should contact the Human Resources Department to find out the status of their employment at the designated time. If the employee is reinstated, the time away is paid based upon the employee's normal work schedule. If the employee is not reinstated, the employee is paid through their last hour of work. Employees who do not call as requested are considered to have voluntarily resigned.

EMPLOYEE ACCEPTABLE USE POLICY

The company possesses information that is sensitive and valuable. Some information is protected by federal and state laws or contractual obligations that prohibit its unauthorized use or disclosure. The exposure of sensitive information to unauthorized individuals could cause irreparable harm to the company or our clients and could also subject the company to fines or other government sanctions. Additionally, if company information were tampered with or made unavailable, it could impair the company's ability to do business. The company therefore requires all employees to diligently protect information as appropriate for its sensitivity level.

Failure to comply with this Employee Acceptable Use Policy may subject personnel to disciplinary measures. Failure to comply could result in termination.

Explicit management approval is required to use the company technology and resources.

1. Employees and Contractors

- You may only access information needed to perform your legitimate duties as an employee and only when authorized by the appropriate management.
 - You may only access acceptable network locations for the technologies on the company network for which you have been approved access.
 - You may only store company data in company-approved systems and/or locations. Client data should only reside within client systems.
- You are expected to ascertain and understand the sensitivity level of information to which you have access through training, other resources or by consultation with your manager.
- You may not in any way divulge, copy, release, sell, loan, alter or destroy any information except as authorized by management within the scope of your professional activities.
- You must understand and comply with the company's requirements related to personally identifiable information (PII), protected health information (PHI) and payment card information (PCI).
 - You may not engage in inappropriate access to PHI, PCI or PII of neighbors, colleagues and relatives.
 - Covered data (PII, PHI, PCI) is prohibited from being stored onto local hard drives, floppy disks, and other external media.
 - Covered data is prohibited from being placed in any system within the company network or cloud-based systems. This includes but not limited to email, Office 365, the Service Desk portal, nanoRep, LivePerson,

SugarCRM, Emplx, etc. Covered data should only be used within the client system it originated or was intended for.

- Workstations must be locked when away.
- You must adhere to the company's requirements for protecting any computer used to conduct the company business and for any computers used to transact the company business regardless of the sensitivity level of the information held on that system.
- You must protect the confidentiality, integrity and availability of company information as appropriate for the information's sensitivity level wherever the information is located, e.g., held on physical documents, stored on computer media, communicated over voice or data networks, exchanged in conversation, etc.
- You must safeguard any physical key, ID card or computer/network account that allows you to access company information. This includes creating difficult-to-guess computer passwords. You should not share your login and password for any system with anyone else, regardless of the circumstances.
- You must destroy or render unusable any confidential or highly confidential information contained in any physical document (e.g., memos, reports, microfilm, microfiche) or any electronic, magnetic or optical storage medium (e.g., USB key, CD, hard disk, magnetic tape, diskette) before it is discarded.
- You must report any activities that you suspect may compromise sensitive information to your supervisor or to the company IT Security Officer.
- Your obligation to protect sensitive information continues after you leave the company.
- While many federal and state laws create exceptions allowing for the disclosure of confidential information in order to comply with investigative subpoenas, court orders and other compulsory requests from law enforcement agencies, anyone who receives such compulsory requests should contact the Legal Department before taking any action.
- If you are performing work in an office that handles information subject to specific security regulations, you will be required to acknowledge that you have read, understand and agree to comply with the terms of this Employee Acceptable Use Policy annually.

2. Managers and Supervisors

In addition to complying with the requirements listed above for all employees and contractors, managers and supervisors must:

- Ensure that departmental procedures support the objectives of confidentiality, integrity and availability defined by the security manager and designees, and that those procedures are followed.

- Ensure that restrictions are effectively communicated to those who use, administer, capture, store, process or transfer the information in any form, physical or electronic.
- Ensure that each staff member understands their information security-related responsibilities.

3. Technology Staff

In addition to complying with the Employee Acceptable Use Policy requirements defined for all employees and contractors, and managers and supervisors, those who manage computing and network environments that capture, store, process and/or transmit company information, are responsible for ensuring that the requirements for confidentiality, integrity and availability, as defined by the appropriate management, are being satisfied within their environments. This includes:

- Understanding the sensitivity level of the information that will be captured by, stored within, processed by, and/or transmitted through their technologies.
- Developing, implementing, operating and maintaining a secure technology environment that includes:
 - A cohesive architectural policy.
 - Product implementation and configuration standards.
 - Procedures and guidelines for administering network and system accounts and access privileges in a manner that satisfies the security requirements defined by the Information Guardians.
 - An effective strategy for protecting information against generic threats posed by computer hackers that adheres to industry-accepted "best practices" for the technology.
- Ensuring that staff members understand the sensitivity levels of the data being handled and the measures used to secure it.

4. Information Definitions

The confidentiality requirement for an information collection will be expressed in the following terms:

- "Public" information can be freely shared with individuals on or off campus without any further authorization by the appropriate the company Management.
- "Internal" information can be freely shared with members of the company community. Sharing such information with individuals outside of the company community requires authorization by the appropriate the company Management.

- “Departmental” information can be freely shared with members of the owning department. Sharing such information with individuals outside of the owning department requires authorization by the appropriate the company Management.
- “Confidential” information can only be shared on a “need to know” basis with individuals who have been authorized by the appropriate the company Management, either by job function or by name.
- “Highly confidential” information can only be shared on a “need to know” basis with a limited number of individuals who have been identified by the appropriate Information the company Management.

The integrity/availability requirement for an information collection will be expressed as follows:

- Information is “non-critical” if its unauthorized modification, loss or destruction would cause little more than temporary inconvenience to the user community and support staff and incur limited recovery costs. Reasonable measures to protect information deemed “non-critical”
- include storing physical information in locked cabinets and/or office space, using standard access control mechanisms that prevent unauthorized individuals from updating computer-based information, and making regular backup copies.
- Information is “critical” if its unauthorized modification, loss, or destruction through malicious activity, accident or irresponsible management could potentially cause the company to:
 - Suffer significant financial loss or damage to its reputation.
 - Be out of compliance with legal/regulatory or contractual requirements.
 - Adversely impact its clients.
- Additional safeguards for critical information:
 - Critical information must be verified either visually or against other sources on a regular basis.
 - A business continuity plan to recover critical information that has been lost or damaged must be developed, documented, deployed and tested annually.

Any noncompliance with these requirements will constitute a security violation and will be reported to the management of the company user and the company CIO and will result in short-term or permanent loss of access to the company computing systems. Serious violations may result in termination, civil prosecution or criminal prosecution.

SOCIAL MEDIA POLICY

This Social Media Policy governs employee use of social media, including any tools used to share content and profiles, including but not limited to social networking websites, apps, and blogs. The lack of explicit reference to a specific site or type of social media does not limit the application of this Social Media Policy.

Social media can be an interesting and rewarding way to share your life and opinions with family, friends, colleagues, and people all over the world, even with strangers. The company respects the rights of all employees to use social media. However, because communications by company employees on social media could, in certain situations, negatively impact business operations or create legal liability, it is necessary for the company to provide these guidelines. These guidelines are intended to ensure employees understand the types of conduct that are prohibited and to assist you in making responsible decisions about your use of social media. This Social Media Policy will not be interpreted or applied so as to interfere with the rights of employees to discuss or share information related to their wages, hours, or other terms and conditions of employment. Employees have the right to engage in or refrain from such activities.

Employees engaging in use of social media are subject to all of the company's policies and procedures, including, but not limited to, the company's policies: (1) protecting trade secrets and confidential information related to the company's operation; (2) safeguarding company property; (3) prohibiting unlawful discrimination, harassment and retaliation; and (4) governing the use of company IT.

1. Scope & Coverage

- This Social Media Policy applies to all employees of the company and its affiliates and subsidiaries globally, regardless of rank, position, or nature of employment.
- As the world of electronic communication and technology is rapidly evolving, social media can mean many things. For purpose of this Social Media Policy, "social media" includes all means of communicating and posting information or content of any sort on the Internet or on any web or mobile based applications (including your own or someone else's sites), whether or not these sites are associated or affiliated with Everise India. The lack of an explicit reference to a specific site or type of social media does not limit the application of this Social Media Policy. Social media shall include, but is not limited to, the following:
 - Web, mobile, multi-media and social networking websites such as Facebook, Yahoo! Groups, Twitter, Instagram, Google+, LinkedIn or any other similar sites.
 - Content communities like YouTube, Skype, or similar platforms.
 - Blogs (both Everise India blogs and personal blogs), online journal or diary, personal website, web bulletin boards or chat rooms.

- Advertising content applications like Google.
- Collaborative content sites such as Wikipedia and any other site where text can be posted.
- To be clear, social media also includes new and emerging applications; thus, you should be aware that this Social Media Policy is intended to apply to sites or services that exist now or come into existence while this Social Media Policy is in effect.

2. Principle of Accountability

- You are ultimately responsible for what you post online in any social media application. Before creating and posting content, consider the reward and even more carefully the risks in your statements or postings. Bear in mind that your conduct in social media may adversely affect your work or work performance or that of your fellow employees, clients, customers, vendors, people who work on behalf of Everise India, or Everise India's legitimate business interests, or may otherwise violate this Social Media Policy or other Everise India policies and may result in disciplinary action up to and including termination.
- The company standards allow use of its IT Resources only for conducting company business. ***If you access social media using your own machines or devices, you should never use company time, property or IT networks for such communications.*** If you do so outside of work using non-company resources, you must:
 - use your personal email address and internet connection;
 - state that these are your personal views and not the views of Everise; and
 - ensure that your statements, postings, and communications do not violate any laws (including but not limited to libel or other defamation, stalking, harassment, intimidation, unauthorized use of intellectual property, fraud, misrepresentation, etc.) or Everise India policies (e.g., disclose confidential or proprietary information or speak on behalf of Everise India without authority, etc.).

3. Guidelines

You must observe these basic principles in your use of social media.

3.1. ***Know and Follow the Standards and Employee Handbook***

You are expected to carefully read this Social Media Policy, the company standards and this Employee Handbook, which includes policies on harassment. You must ensure that your statements, declarations and postings in social media are consistent with all of these policies. Inappropriate postings that include discriminatory remarks, harassment, intimidation, threats of violence, or any inappropriate or unlawful conduct are prohibited.

3.2. ***Be Respectful***

- You are expected to respect your audience and avoid inappropriate subject matters while communicating in your personal blogs or commenting and posting in social media. Ethnic, religious, gender, sexual orientation, and racial slurs, personal insults, obscenity, and similar postings are disrespectful and should be absolutely avoided.
- You should exercise your best judgment when expressing your views and opinions in social media. Although you represent your own self in public and do not always represent Everise India's official views, your acts, communications and behavior may be considered reflective of the Everise India culture and values. In this regard, you are considered an ambassador of Everise in any public setting.
- It is understood that there may be times when you disagree with co-workers about work or management issues. Everise India employees are encouraged to address such issues and concerns using the internal channels.
- You should always be respectful and courteous to fellow employees and other people in your writings and communications. Also, bear in mind that you are more likely to resolve work-related complaints by speaking directly with your co-workers, managers, or Human Resources, or by emailing COOInsight@weareeverise.com than by posting complaints to a social media outlet.

3.3. ***Be Honest and Accurate***

You must make sure that you are always honest and accurate when posting information and news, and if you make a mistake in your posting, you should take steps to correct it immediately. You must be open about any previous posts you have changed or corrected. It is good to remember that the Internet and social media applications record everything; so, even when you delete posts or comments, those can still be searched and appear in searches. You should never post any information that you know to be false or spread rumors about Everise India, fellow employees, customers, vendors, and people working on behalf of Everise India or its competitors.

3.4. ***Post Only Appropriate Content***

You should always be mindful of the laws, regulations and company's policies that may apply to your postings in social media. Thus, you are advised:

- Not to create a link from your blog, website, page or posting to any Everise websites without specific prior permission from Everise Brand Marketing and Communications Department.
- Not to represent yourself as a spokesperson for Everise India. When you express opinions, they should be your personal opinions, and identified as your personal opinions.

- Not to use social media to post or to display comments about co-workers, supervisors, customers, vendors, suppliers, or members of management that are obscene, physically.
- threatening or intimidating, or otherwise constitute a violation of the company's workplace policies against discrimination, retaliation, or harassment. If you have been harassed, intimidated or abused by a co-worker via social media, you should report the conduct to your immediate supervisor or contact Human Resources.
- Not to use social media to post or display content that is an intentional public attack on the company's products and/or services in a manner that a reasonable person would perceive as calculated to harm the company's business and is unrelated to any employee concern involving the terms and conditions of employment.
- Not to post a photograph or video of a vendor, supplier, or customer on social media without that individual's express permission.
- Not to misrepresent on social media an employee's title or position with the company.
- You should use your personal email address when using Social Media. You are not allowed to use your Everise India email address to register on Social Media sites or for social networks, blogs or other online tools utilized for personal use. You should respect the intellectual property rights of others. You should not post or share material that is protected by copyright or trademark.
- You should refrain from discussing non-public as well as sensitive topics related to Everise India even if a disclaimer is being used. For example, comments and speculations on the organization's business performance (including both past performance and anticipated performance for upcoming quarters or future periods), business plans, unannounced strategies or prospects (including information about partnerships or joint ventures), potential acquisitions or divestitures, similar matters involving the company's competitors, legal or regulatory matters, and other similar subjects could negatively affect the company.

3.5. ***Do Not Disclose Confidential and Proprietary Information***

- You are required to strictly maintain the confidentiality of Everise India business information (including Trade Secrets and other Confidential Information, as previously defined) and other confidential information. Trade secrets include, but are not limited to, information regarding the development of systems, processes, products, service offerings, call flows, scripts, customer lists, software, pricing information, work flows, financial metrics, financial forecasts and other financial information, technology, and other matters relating to Everise India business operations. Beware of congratulating co-workers online and referencing significant Everise India achievements that have not been publicly disclosed (i.e. successful development of a new product or launch of a new partnership, acquisition of a significant new customer, and achievement of a key financial metric.)

- The company has well established means of communicating publicly to the marketplace or to the general public; hence only officially designated employees have the authorization to speak on behalf of the company. You are also not allowed to post internal reports, policies, procedures or other internal business-related confidential communications in any social media platform.

3.6. ***Do Not Let Social Media Interfere with Your Work***

You should not allow social media activity to interfere with your job responsibilities. You are expected to devote your full time and attention to your work during your work hours.

3.7. ***Social Media Monitoring***

- You should be aware that the company may observe and monitor the content and information posted by employees on social media when, to the extent allowed by applicable privacy regulations, there is a legitimate business interest in doing so, such as an investigation into whether there has been a violation of this Social Media Policy and other company policies.
- You may also be subject to disciplinary actions where you have:
 - violated local laws by making threats of physical harm, libeling, slandering or defaming customers, clients, co-workers, officers or directors, or other persons;
 - violated copyright laws, such as illegal downloading of music videos or movies where the downloads are loaded to or accessible from company systems;
 - disclosed company confidential information or the confidential information of our clients, customers, partners or vendors;
 - disclosed personal information of customers, clients, co-workers, officers or directors, or other persons such as social security numbers or government ID numbers, credit card or banking information, address, or other personal information;
 - used social media in violation of company policies, including anti-harassment and anti-discrimination policies, such as inappropriate or sexually suggestive comments and graphics, or any demeaning or disparaging jokes and comments;
 - Where your postings violate this Social Media Policy, the company may also require you or the relevant social media application to remove the applicable posting or thread.

3.8. *Reservation of Rights*

The company reserves its right to institute civil and criminal proceedings against you for violation of this Social Media Policy, and to recover payment for fines, penalties or damages to its business and reputation, and to claim and file for other legal relief and remedies to protect its interests.

3.9. *Retaliation is Absolutely Prohibited*

Taking negative action against any employee for reporting a possible violation of this Social Media Policy or for cooperating with an investigation is prohibited.

3.10. *Dealing with Media*

- You should not speak to the media on behalf of Everise.
- All media inquiries should be directed via email to the Corporate Communications Department: corporate.communications@weareeverise.com
- If you have questions about this Social Media Policy or need additional information or guidance, please contact your local Human Resources representative.

SEPARATION AND TERMINATION PROCESS

1. Separation from the company is classified as voluntary (employee initiated) or involuntary (company initiated).
2. Employees voluntarily leaving the company are expected to give a minimum notice as per the Employment Contract calendar days. Failure to give proper notice may result in ineligibility for re-hire.
3. Unused earned paid leave is paid at the time of exit as per the Leave Policy.
4. Employees who fail to work all of their scheduled shifts during the notice period will be subjected to a reduction in hours.
5. **Layoffs / Closure / Program Ended:** Employees who have demonstrated good performance are eligible for rehire. There is no waiting period to apply for available openings based upon qualifications, attendance, and performance.
6. **Involuntary Terminations** – Employees who were terminated for misconduct, violation of company's policies, unsatisfactory performance, excessive absenteeism or lateness, or any other for-cause terminations are generally not eligible for rehire.
7. **Rehire Eligibility:** Eligibility is determined based on how the employee left Everise India, skills, performance and attendance.
8. **Rehire:** Employee rehired will be treated as a new hire
9. **Retirement:** The retirement age for all employees shall be 60 years old or by the prevailing Indian regulation on retirement age

ACKNOWLEDGEMENT OF EMPLOYEE HANDBOOK

I understand it is my responsibility to read and abide by the Employee Handbook. The Employee Handbook may be revised periodically. It is my responsibility to check the online Employee Handbook which is found on the Intranet. I acknowledge my obligation to read and understand its contents, and further acknowledge and agree that:

- The Employee Handbook is only intended to provide a general overview of the company's personnel policies and does not necessarily represent all such policies or practices in force at any particular time.
- The current version of the Employee Handbook supersedes any previous version of the Employee Handbook that may have been issued by the company.
- My signature below or electronic signature in Emplx also attests to the fact that I have read, understand, and agree to be legally bound by the contents of the Employee Handbook.
- My signature below or acceptance in Emplx also attests to the fact that, in addition to acknowledging and accepting the Employee Handbook, I have read, understand and agree to be legally bound by the Business Code of Conduct, and will abide by any other policy duly adopted by Everise India

Employee Name (please sign and print)
Date

Employee Signature
Date

Annexure I
IJP Application Form

Position Applying To		
Position Title:	Hiring Manager:	
Program / Account:	Date:	
Employee Information		
Employee Name:	Hire Date / Emp ID	
Current Position / Program	Immediate Supervisor:	
Length of time in Position	Shift Schedule / Rest Day	
<p>Qualifications for this position: <i>Include relevant prior job experience gained outside or inside Everise India.</i></p> <p><i>You may complete this section on a separate sheet of paper. Please do not forget to attach your MOST UPDATED resume.</i></p>		
Employee Signature:	Contact #	
Current Supervisor Section		
Please check the appropriate boxes below:		
1. Is on active corrective action?	Yes	No
2. Met all requirements for his/her current position as of the last performance review?	Yes	No
3. Currently meeting the requirements for his/her current position?	Yes	No
Comments / Recommendation:		
Supervisor's Signature:	Date:	
Recruiter Section		
1. Meets minimum qualifications for the position to which he/she has applied?	Yes	No
2. Have been with the company for 6 months and above?	Yes	No
3. Eligible to apply?	Yes	No

Comments/ Recommendation:		
Recruiter's Signature:		Date:
Hiring Manager Section (Interviewer)		
Comments / Recommendation: <i>Please put your notes here.</i>		
Transfer Date		Program:
HM Signature:		Date today:
RELEASING MANAGER SECTION		
Comments / Recommendation:		
Signature:		Date:
HR Section		
1. SCF Received	Yes No	Date Received:
2. Masterfile Updated	Yes No	Date Updated:
Comments / Recommendation:		
Signature:		Date:

*** Everise India is an equal opportunity employer. All recruiting and hiring activities will be administered without regard to race, religion, sex, age, national origin, or disability.*

APPENDIX A
CONTACT INFORMATION FOR POLICY

Reporting Hotline:

North America – 800-665-0831

South Africa – 0800-000501

Mexico – 01800-436-0065

France – 0800-91-2964

Australia – 1800-152-863

South Korea – 0809-080-895

New Zealand – 0800-443-938

Germany – 0800-000-6649

Brazil – 0800-891-3867

Spain – 900-810-305

Portugal – 0800-78-4717

Hong Kong – 800-960-631

Chile – 1230-020-0517

Switzerland – 0800-225-163

Qatar – 800-0249

Ireland – 1800-946-551

China – 400-880-1042

United Kingdom – 0808-234-2210

Singapore – 1800-622-7248

Japan – 012-099-3307

Colombia – 01800-011-0149

Two-Stage Dialing:

India – 000-117, then 800-795-2716

Peru – 0-800-70-088, 0-800-50-000 or 0-800-50-288, then 800-795-2716

United Arab Emirates – 8000-021, 8000-051 or 8000-061, then 800-795-2716

Collect Worldwide – 770-613-6339

Online – <http://brookfield.tnwreports.com/>