TresVista
Catalyzing Your Impact

UK Employee Handbook

Disclaimer

Welcome to the TresVista family! We are thrilled to have you join our vibrant, talented team as we strive to provide exceptional services while empowering our Employees to grow and succeed together.

Employees are required to abide by this Handbook and the policies herein, and any other rules, regulations, policies that may be released by the Management from time to time. Unless expressly stated otherwise, the policies and procedures set out in this Handbook do not form part of the terms of your contract with us, which are provided to you separately.

In order for the policies to remain current and relevant, the Handbook is revisited at regular intervals and necessary modifications, or additions are made. In such cases, the eligible Employees are informed of any change. Further, each Employee is bound to observe and uphold all of the Company's policies and procedures as implemented or varied from time to time.

The provisions mentioned are indicative and in case of any conflict with the provisions of the Employment Agreement, Offer Letter, or subsequent Promotion Letters, the terms of the most recent of Employment Agreement, Offer Letter or Promotion Letter prevail. Further, subject to law, all representations and undertakings related to any and all benefits being or to be extended to Employees pursuant to this Handbook are on a best effort basis and may be rolled back at discretion of the Management. This document is intended for the internal use of recipients only and may not be distributed externally. Any reproduction for external distribution in any form without written permission from TresVista may amount to a breach of confidentiality resulting in disciplinary action.

Table of Contents

(A) About TresVista

1. History

TresVista along with its list of entities situated in India, Singapore, United States and United Kingdom, started in November 2006. It is a unique high-end financial service provider that meets client needs by offering a diverse and in-depth suite of services. It provides financial advisory and consulting services to institutional clientele across asset classes and industries with a reach that spreads across the globe. Financial sector clients include private and public equity, hedge funds, investment banking, equity research, and fixed income firms. TresVista has also worked across multiple sectors such as banking, logistics, telecommunication, solar power, media, manufacturing, and many more. Through its unique services model and culture, TresVista delivers excellence to clients and opportunity to Employees, both with an aspiration to exceed expectations.
This Handbook is applicable to all the Employees of TresVista's entity incorporated in the United Kingdom – TresVista (UK) Limited.

2. Mission Statement

To be recognized as the highest quality financial and consulting services provider through:

- Building a team of industry leading talent
- Consistent dedication to excellence and quality
- Active participation in the growth and success of its clients

3. PACT

The culture of TresVista is built on the founding pillars of the PACT.

People

'We recognize and value that people are unique and multifaceted. We give people the freedom to contribute to the Improvement of the organization. We encourage creativity and support enthusiasm.'

Action

'We encourage active decision making and getting the job done. We act rather than react.'

Clients

'We strive to be close to the customer. We learn from the people we serve in order to continuously improve our quality.'

Team

'We succeed together.'

4. CSR

"We make a living by what we get, but we make a life by what we give"

Winston Churchill

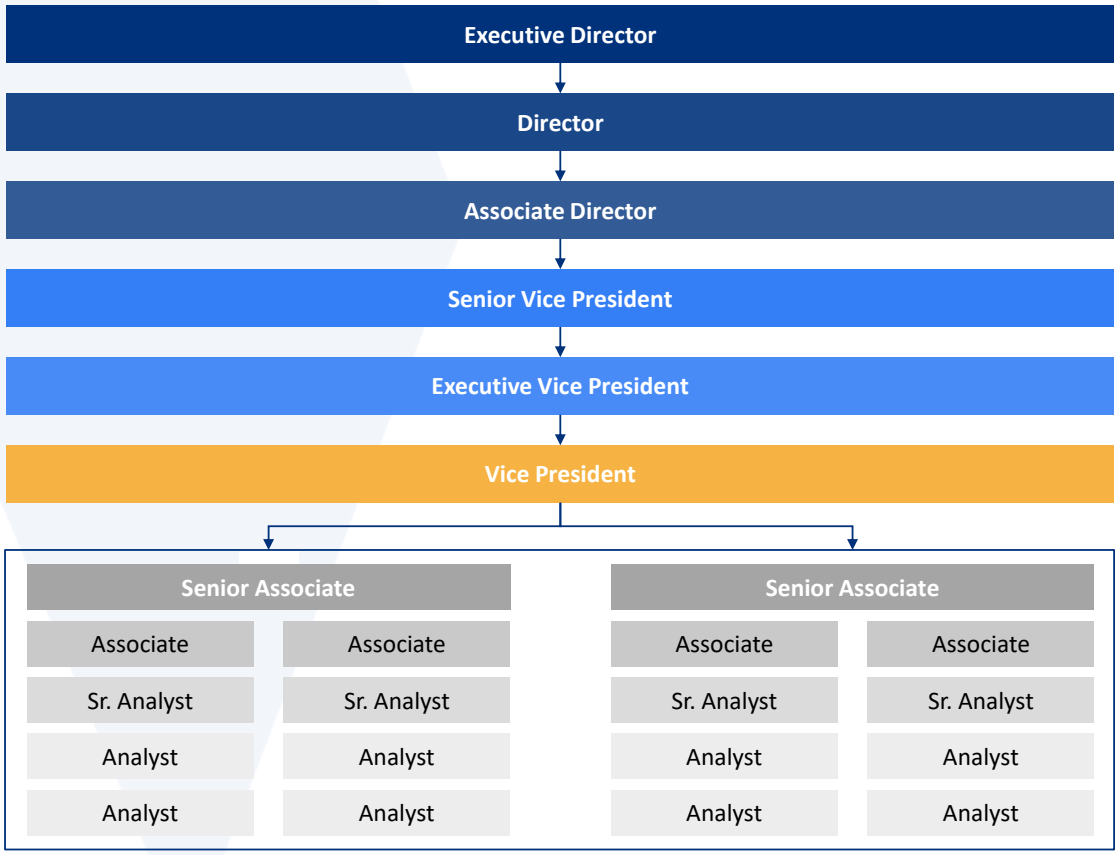
Since its inception, TresVista has been committed to serving the community to which it belongs. The founders appreciate that the proper functioning and improvement of a society requires its Employees, both as individuals and as corporate citizens to take not only responsibility but also action.

The Company periodically organizes community service events at the Company level, where in all Employees are encouraged to participate. Besides this, Employees are encouraged to promote causes they are passionate about. The founders often participate in service events with individual champions of causes. TresVista also actively partners with organizations that promote social investment and entrepreneurship, whereby TresVista's team members can leverage their financial skills for the benefit of NGOs and social entrepreneurs.

The small changes that can be made and witnessed, allow TresVista's Employees to become more engaged and committed towards donating time and money for socially valuable causes. As a team, everyone at TresVista is encouraged to continue contributing to the community by putting in their best efforts.

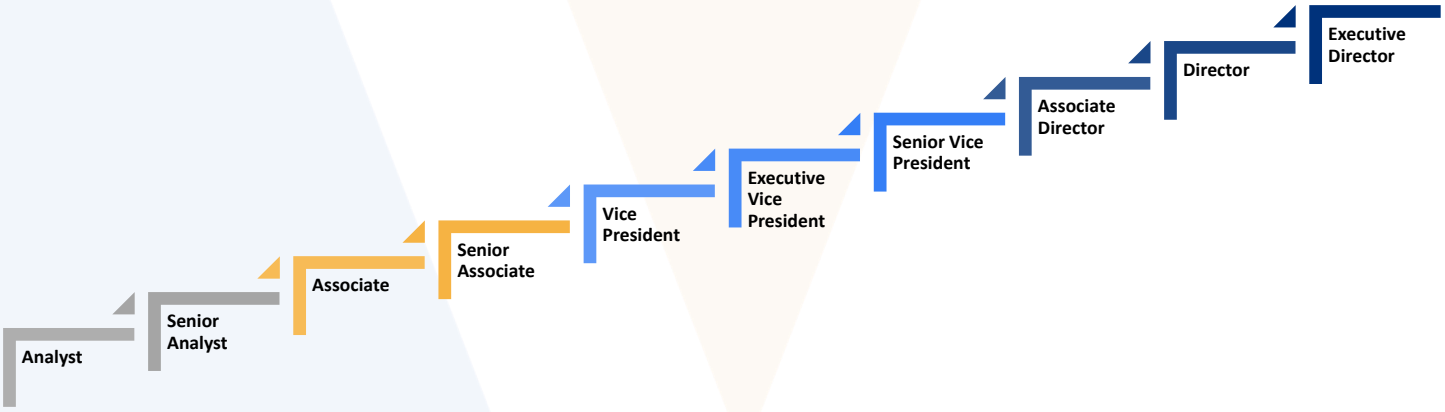
5. Organizational Structure

TresVista has multiple teams, each headed by a Vice President (VP). Employees may get rotated between teams during their tenure.



6. Career Progression

At every level, an Employee has the opportunity to grow. The diagram below summarizes the initial career progression at TresVista (some departments may have a slightly different path). There also exists the opportunities to move within departments of the Company over time.



7. Training

TresVista takes responsibility for the growth of its Employees, by providing enriching and valuable opportunities to learn at every stage of their career. Training at TresVista plays a pivotal role in Employee learning and development, knowledge sharing and skill enhancement. The aim is to create a supportive and engaging learning environment which is not only limited to technical upskilling but also ensures holistic development. The training modules are carefully tailored to contribute to the success of the organization through focused learning that is strategic, measurable, and effective for every Employee.

New Hire Training

TresVista has a structured onboarding program to impart technical and process understanding and disseminate the culture of TresVista among the new joiners. New hire training is a platform that prepares new joiners for the tasks they will be expected to perform once they hit the floor.

- All new hires undergo intensive induction training facilitated by the Training department
- Such training sessions may be conducted off-site or in the office premises
- The duration of the training ranges from two to five (2-5) weeks depending on the team/department and includes a mix of instructor lead induction/soft skill sessions, team/department/function-specific sessions, and technical sessions

On the Job Training

TresVista has a structured year-wise training calendar that consists of training sessions organized for Employees across various levels. The objective of the programme is to provide each Employee with the opportunity to hone their creative, non-technical, and on-the-job skills in order to maximize their productivity at the workplace. The Training department will notify Employees of these training sessions in advance. It is mandatory to attend these training sessions and it should be noted that:

- Employees are required to plan their holidays accordingly
- It is the Employee's responsibility to notify the Manager in advance to manage work and training sessions
- In case an Employee misses training, they must notify the Training department or their Managers of the reason for not attending the trainingf

Points to Note

- Team/department/function-specific training manuals are provided to the Employees prior to each session
- Employees are encouraged to refer to these manuals whenever required. All accesses given to refer to the training material are revoked at the time of the Employee's exit, since it is Company property

8. Work Ethics

TresVista aims at enhancing its reputation as a quality service provider and an enjoyable, stimulating, and challenging place to work. It expects its Employees to achieve and maintain a high standard of ethics, professional conduct, and work performance to ensure that TresVista maintains its reputation with all internal and external stakeholders.

All Employees should note that:

- High ethical standards must be recognized and valued
- Any unethical or illegal behavior must be reported by the Employees to the Ethics Committee
- An environment of honesty, trust and integrity must be maintained
- TresVista's property must be maintained and not be damaged intentionally
- In all dealings with Third Parties, the policies and directions of this Handbook must be complied with
- Any behavior or collective action which harms or could harm the integrity and/or interests of TresVista must be avoided

Use of any Resources in connection with any illegal activity is strictly prohibited, and TresVista will cooperate with any legitimate law enforcement investigation of potential criminal activity.

9. Personal Information

The 'Personal Information' module under the 'Profile' section on Darwinbox records each Employee's personal details such as educational qualifications, past work experience, contact information, etc. The Employee is required to fill in this page upon joining. At any given time, the 'Profile' page must remain updated. If there is a change in any details, the responsibility lies with the Employee to update the page immediately. The Management, respective Managers, and the HR Department have access to this page. An Employee is required to submit personal documents, as mentioned in the offer letter, before they join the Company.

The Employee is responsible to ensure the personal information page on DarwinBox is updated; for instance, change in address or certification received. These documents are uploaded on DarwinBox and will reflect in the 'Personal Documents' page of an Employee. The documents include but are not limited to the Employee's passport, mark sheets, driving license, and experience letters. The Management, the Corporate Finance department Team, and HR Departments have access to these documents.

All personal information is kept strictly confidential.

In the course of employment with the Company, the Company may obtain or have access to certain information about the Employee or his/her employment with any previous employers, including but not limited to information about the job and performance, health, education, contact details, absence from work and information obtained from background verification checks (collectively, "Personal Information"). The Company will use personal information in connection with employment with the Company, to provide the Employee with health and other benefits, and in order to fulfill its legal and regulatory obligations.

Due to the global nature of the Company's business and need to centralize the Company's information and technology storage systems, the Company may transfer, use or store an Employee's personal information in a country or continent outside the United Kingdom, and may also transfer an Employee's personal information to its other group companies, insurers, and third-party service providers, as necessary or appropriate , and to any party that it merges with or which purchases all or a substantial portion of its assets, shares, or business (any of which may be located outside the country or continent the Employee works or lives).

The Company may also disclose an Employee's personal information when it is legally required to do so or to governmental, fiscal, or regulatory authorities (e.g., to tax authorities in order to calculate appropriate taxation, compensation, or salary payments). The Company may disclose personal information as noted above, including to any of the third parties and for any of the reasons listed above, without further notice to the Employee. By receiving the Handbook, the employee consents to TresVista collecting, retaining, disclosing, and using personal information as outlined above and to transfer such information internationally and/or to third parties for these purposes.

10. Communication

Given TresVista's diverse team and client base, communication is integral to its success. For the sake of smooth and effective flow of communication, English will be the official language for all purposes.

The following communication channels are widely used:

- **Direct Communication:** Employees are encouraged to speak directly to their Managers regarding any day-to-day concerns/queries they may have (E.g., Functioning of the team, work related queries, etc.)
- **Helpdesk:** For any operational concerns/queries/requests, Employees should raise a Helpdesk ticket with the respective departments. If Employees are dissatisfied with the resolution, they may escalate it in accordance with the defined SLA matrix, saved on SharePoint
- **Viva Engage:** Viva Engage is the internal social networking platform of the Company with the aim of bringing together Employees across locations and teams. Employees can participate in events, share their thoughts/achievements/ milestones, and engage with other Employees through this platform

TresVista prides itself on a culture based on openness and transparency. Any feedback or suggestions to improve the workplace are welcome.

11. Company ERPs

The Company has two enterprise resource planning (ERP) systems – DarwinBox and Microsoft Dynamics 365 to manage day-to-day internal activities of the Employees.

- A login ID and password will be provided to each Employee upon joining
- Employees can log-in to ERPs using the single sign-on (SSO) feature
- Manuals with detailed guidelines on how to use the below ERPs are available on the SharePoint
- It is recommended that Employees log-in to the below ERPs through Microsoft Edge to avoid any bugs that may arise in other browsers
- **DarwinBox:**
  - DarwinBox allows Employees to record and manage their personal information, attendance, etc.
  - The system can be accessed through: https://tresvista.darwinbox.in/
- **Microsoft Dynamics 365:** Microsoft Dynamics 365 allows interns to record their expense reimbursements and to access project hours, etc.

12. Personal Use of Company Resources

The use of Company resources for personal use is strictly prohibited. Employees using Company resources including but not limited to equipment, office supplies, technology, software, and internet access, for personal purposes or activities unrelated to their job responsibilities maybe subject to disciplinary action, up to and including termination of employment.

The Management and staff have the right to track usage of Company resources to determine whether usage or involvement is excessive or inappropriate.

13. Phone Etiquettes

All Employees are expected to be reachable on their cell phones even when not in office. It should be noted that:

- Employees must not have any caller tunes and/or disruptive ring tones as it is unprofessional
- While at work, the volume on the cell phone must not disturb people around. It is advised that Employees keep their phones on silent, while working from the office
- Messaging during meetings and discussions should be avoided as much as possible as it is ill-mannered and disruptive
- Phone games should be restricted to the recreation room or outside the office

We understand that personal communication is inevitable and sometimes necessary. However, it is expected that such communication will be kept to appropriate and reasonable levels.

14. IDs and Passwords

User IDs and passwords help maintain individual accountability for the internet, intranet, and email resource usage, and Employees are responsible for keeping them confidential and not sharing them with anyone.

Employees must change their system passwords once every 30 days. Employees must be connected to the authorized VPN client before changing the system password. Employees can raise a ticket with the Software Department for issues related to Microsoft Dynamics 365 and with the IT Department for issues related to system password.

15. Data Usage

- All Employees are responsible for managing their use of information resources and are accountable for their actions relating to information resource security
- Employees can access their respective network drives/share point sites on Company laptops when they are connected to the authorized VPN client

- Network drives/share point sites are backed up per the pre-defined Backup Policy

- Employees are allowed to store their personal data (e.g., documents, MP3, etc.) on the hard drive of their local system, however, it cannot not be stored on the network server
  - Employees can raise a ticket with the IT department to upload their personal files on the drive
  - Data stored on the laptop's local storage will not be backed up, and lost data is not recoverable
  - Any such violations/incidents must be reported immediately so that appropriate action can be taken in a timely manner
- Employees using Company laptops should not leave the device unattended keeping in mind TresVista's Data Security Policy

16. Software and Hardware

Software includes purchased or licensed business software applications, Company-written applications, Employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on TresVista-owned equipment. All equipment, including desktop computers (PCs), laptops, tablets, terminals, workstations, wireless computing devices, USB flash drives, telecom equipment, networks, databases, printers, servers, shared computers, and all networks and hardware to which this equipment is connected, are covered under hardware. Employees must use TresVista's computers and networks only for legal and authorized purposes.

- For computers dedicated for use by a single Employee end-user
- At the end of each workday or if an Employee plans to leave the computers unattended for a few minutes or longer, lock or power off the computer to prevent unauthorized access. In case the Employee wishes to log on to the system remotely, they should log off and switch off the monitor
- For a computer shared by multiple Employee end-users (e.g., database terminals):
  - Not leave their computer sessions unattended, and instead, log-off if they must leave the immediate vicinity of the computer, then log in again upon return
  - Disconnect from network-accessible resources, log-off the computer, and make it available for another Employee immediately upon completion of their computer session
- Employees are responsible for the laptops provided to them by TresVista. In case of theft or damage, the Employee must notify the IT and Compliance Department immediately through an email
- In case of damage, Employees have the responsibility to raise a case with the OEM for repair and replacement
  - Any loss or damage to Company-issued laptops will be borne by the Employee to whom the assets are assigned

17. Email

Email facility is provided to Employees in order to assist them in the performance of their work duties. Email is subject to regulations covering libel, freedom of information, breach of confidence, copyright, obscenity, fraudulent misrepresentation, data protection and unlawful discrimination. Email has legal status as a document and may be accepted as evidence in a court of Law. Access to both, personal and work related emails may be demanded as part of legal action in some circumstances. Some forms of email conduct may also be open to criminal prosecution.

- TresVista emails can be accessible by all Employees using the following applications:
  - Microsoft Outlook available from within TresVista premises and on Company-issued laptops
  - Mobile device management application installed on Employees' compatible personal Smartphones (Android/iOS)

Employees must:

- Not expect privacy, as the IT Department and Management may review any emails at any point in time to ensure compliance with policies, procedures and legal obligations, and for legitimate business purposes
- Set up out-of-office replies as per their Manager's guidance, in case they are out of office for some reason and not able to check emails
- Note that even when it is used for purposes outside the scope of employment of the Employee, TresVista can be held responsible for the contents of email messages, including any attachments
- Not delete emails, including personal messages from the 'Sent Items', 'Inbox' or any other folder
- Not configure their personal mailbox using Outlook or any other applications on Company issued devices such as desktops, laptops, MS Surface, iPads, and smartphones
- Not configure their official TresVista mailbox themselves using any email applications on personal devices such as desktops, laptops, MS Surface, iPads, and smartphones
- Not try to use webmail to access their official mailbox as it is prohibited and blocked through policy by the IT Department

18. Telecommunication

Smartphones

It is mandatory for all Employees to have a smartphone with a valid voice and data plan at all possible times. The data plan on an Employee's personal phone must allow at least email communication. Internet browsing is optional.

19. Wi-Fi

Apart from the wired LAN, there is a Wi-Fi network in place wherein access to Wi-Fi-enabled devices like a laptop, a tablet PC, or a smartphone can be configured. To seamlessly configure Wi-Fi with restricted internet access on all the Employee's smartphones, it is pushed through MDM application which is a secure platform managed centrally by the IT Department.

(B) People Policies

1. Working at TresVista

The purpose of this section is to educate Employees on general office policies and guidelines pertaining to their day-to-day operations.

1.1 Work Hours and Attendance

This policy is to inform Employees about the guidelines concerning office hours, shifts, and attendance.

Work Hours

- **Office Hours:**
  - The timings shall be decided by the Company from time to time, subject to work commitments and responsibilities of the Employee. The Employee:
    - Shall be required to adhere to the office hours as may be intimated from time to time
    - Understands and agrees that no compensatory time off in lieu are provided by the Company for working late and/or on weekends
    - Understands and agrees that the compensation payable as part of his/her employment includes wages and overtime payments, if eligible, and no separate payments would be paid to the Employee
  - The Company may, at its discretion, vary its working hours for any specific Employee to meet its requirements on giving the Employee reasonable notice. If requested to do so by the Company or their Manager, the Employee must keep such records and permit such monitoring or restrictions of the working time as the Company requires
- **Flexibility:** Employees shall be required to obtain prior consent from their Manager for all situations when reporting after or leaving before office hours, otherwise, the day may be treated as a personal day at the discretion of the Manager.

- **Emergency Work Requests:** If an Employee knows they will be unavailable on a weekend or a holiday or will take more than usual time to reach office, they must inform their Manager in advance so that the Manager can plan any last minute or emergency work demands accordingly. Consistent unavailability outside office hours must be avoided

Attendance

- Attendance is managed through DarwinBox and Employees are expected to clock-in on Darwinbox, to mark their attendance for the day
- In case Employees are unable to record their attendance for the day, they may regularize it on Darwinbox the next day
- Employees must ensure that any attendance request is applied for and approved on Darwinbox per the timeline decided by the Corporate Finance department
- Employees must apply for leaves availed by them on DarwinBox under the 'Leaves and Flexwork' module, within the monthly leave and attendance timeline defined by the Corporate Finance department
- Employees must notify their Managers when they are away from their desk for an extended period of time
- Absence due to contingencies:
  - In case of any unforeseen situation, Employees are expected to inform their Manager before 9:00 AM if they will be delayed or absent. Tardiness may result in the Manager marking the day as a personal day
  - In case of unforeseen situations, such as public transportation strikes, Employees are expected to work from home. In case they are unable to work from home, this day(s) will be deducted from the Employee's leave balance unless such a day is declared to be a holiday
- An Employee is not permitted to be absent for more than eighty (80) working days in any twelve (12) month period for any reason other than reasons permitted by law and/or with the prior written permission of the Company

1.2 Hybrid Guidelines

The purpose of this policy is to provide a framework to Employees on working from the office/home in the hybrid model.

Applicability

This policy is applicable to all Employees.

Particulars

- **Working from Office:**

- Employees across departments/team are required to work from the office 20% of the time in a given review period
- The defined guidelines on working from the office are applicable only on working days and not weekends/holidays
- Work from office days are pro-rated in accordance with the firm-wide holidays, leaves/flexwork availed by Employees, and out of office days in that review period given that the intention is to work from the office per the defined frequency matrix, subject to Manager availability/guidelines
- **New Joiners:** Employees are required to work from the office until their training period is completed
- **Employees serving Notice Period:** Employees are required to work from the office per the hybrid model while serving their notice period, and should mandatorily work from office on their last working day (deviation process does not apply on the last working day), subject to any period of garden leave

- **Working from Home:** When working from home, it is recommended that Employees are based out of their respective base locations
- **Deviation Process:** In case Employees are unable to meet the defined hybrid guidelines due to health or unforeseen emergencies, they may work from home at the discretion of the firm/Manager
- **Team Management in Hybrid Setup:**
  - It is recommended that Employees, line Managers and their respective VPs based out of the same office location work together from the office at least two-three (2-3) times a month
  - It is recommended that formal and sensitive conversations (e.g., promotions, review discussions, structured feedback, etc.) are done in person, to the extent possible

1.3 Flexwork

Eligibility

This policy is applicable to all confirmed, permanent Employees, not serving their notice period.

Particulars

- Employees can avail of this benefit for two (2) weeks (i.e., ten (10) working days) in their annual leave cycle
- The benefit can be availed in a maximum of two (2) parts, i.e., five (5) or ten (10) working days at a stretch
  - However, if an Employee has to take a leave during the flexwork period due to medical or unforeseen emergencies, the original flexwork period is split into vacation/personal days and flexwork, accordingly
  - The balance flexwork days from the original flexwork period can be utilized separately in one stretch in the next flexwork request, but cannot be split any further

- E.g., In a five (5) day flexwork request, an Employee was unwell and took two (2) days of leaves. The five (5) days are then split as three (3) days of flexwork and two (2) days of leave
- The remaining seven (7) days can be taken as one (1) flexwork request

- Managers should be mindful when approving these requests and applications not meeting the defined criteria should be rejected

Procedure of Application

Employees can apply for this benefit under 'Leaves and Flexwork' module on DarwinBox.

Approval Mechanism

Employees may avail of this benefit at Manager approval.

Points to Note

- It is encouraged that Employees plan this benefit at least a month in advance
- All requests for flexwork must be applied for and approved within the monthly leave/attendance timeline defined by the Corporate Finance department
- Flexwork cannot be carried forward or encashed and any unused days lapse at the end of the annual leave cycle
- Employees can club this benefit with their leaves, at Manager's discretion
  - However, it is recommended that Employees are not out of the office for more than two (2) weeks at a stretch (inclusive of leaves and flexwork)
- For the days that Employees avail of flexwork, they are mandatorily required to clock-in on DarwinBox
  - Any miss in clocking-in leads to a direct impact on the utilization calculation
- The number of days an Employee works from the office in a week are pro-rated to the flexwork availed in that week
  - Detailed guidelines on the hybrid model can be referred to in Section 1.2 of this Handbook, under the header of people policies
- Flexwork cannot be availed of during the below-mentioned days and Employees are expected to be present in the office on these days:
  - TresVista Day (3rd week of November)
  - Review Delivery Period (3rd and 4th weeks of January/July, as applicable)
- Work timings and other guidelines (such as attendance, availability, responsiveness, etc.) remain as is
- Please note that the Flexwork Policy is in addition to the Flexible Working Policy. Refer to section 1 under the header of people policies of the UK Addendum

1.4 Working from Out of Office

The purpose of working out of office is to enable Employees to attend business activities outside the office on behalf of TresVista.

Eligibility

This policy is applicable to all permanent Employees.

Particulars

- **Attending Business Activities on Behalf of TresVista:** Employees may work from outside the office on specific days wherein they attend activities on behalf of the Company (e.g., meetings outside the office, recruitment, conducting/attending trainings, business trips, etc.)
  - Working from out of office is subject to Manager approval
  - These days are considered as working from the office, per the hybrid model. Employees must clock-in on DarwinBox and mark such days as 'Present – Field Duty'
    - Detailed guidelines on regularizing attendance when working from out of office can be referred to in the User Manual, saved on SharePoint
  - When working from out of the office, it is expected that Employees are available and are productive
- **Working From Another Office Location:** Confirmed Employees, not serving their notice period, may opt to work out of other office locations once for up to one (1) week at a stretch (i.e., from Monday to Friday) in a given month, at their own personal expense, subject to Manager approval
- **Seating Guidelines:**
  - When approving requests to work from other office locations, it is the Manager's responsibility to check and ensure that seats are available
  - **General Guidelines:**
    - Each team has been allocated a defined number of seats, EVPs and below can utilize one of the seats allocated to their team
      - The detailed floor plan can be referred to on the SharePoint
      - If a team/department does not have seats allocated in a particular location, Employees can check with the FMS department on the availability of inter-city seats and accordingly raise a ticket to block them
    - SVPs and equivalents can block a cabin by reaching out to FMS department
      - If no cabins are available, FMS department will block a seat on the floor or an inter-city seat
    - If no inter-city seats are available, Employees can check with the FMS department and leverage Management seats

- **Location Specific Seat Booking Guidelines: -**
  - **Pune and Bengaluru:** Open floor seating plan is followed, wherein Employees do not need to book a seat and can directly utilize one of the seats allocated to their team (e.g.: An HR Employee travelling from Mumbai to Pune can directly occupy one of the empty seats in the HR cabin)
  - **Mumbai:** Seating is managed via the Condeco App and Employees can reach out to the FMS department to book a seat on their behalf
    - In case seats are not available, Managers must reject these requests and Employees are required to shift their travel dates accordingly

1.5 Dressing Guidelines and Personal Grooming

Eligibility

This policy is applicable to all Employees.

Particulars

- Employees are required to adhere to the dressing guidelines set by the Company and it is Manager's responsibility to ensure that their teams adhere to these guidelines
- A summary of the guidelines is mentioned below, and the detailed manuals should be referred to on SharePoint
- **Working from the Office:**
  - Monday to Thursday: Business casuals/formals
  - Friday: Smart casuals
- **Working from Home:** Smart casuals
- **Client Meetings/Networking Events:** Business formals
- **Weekend:** No dresscode

Points to Note

- Employees are encouraged to maintain an appropriate standard of dressing and personal appearance at work. The purpose of the above dress code is to establish basic guidelines on appropriate clothing and appearance at the workplace to:
  - Promote a positive and professional image
  - Respect the needs of Employees from all cultures and religions
  - Make any adjustments that may be needed because of disability
  - Take account of health and safety requirements
  - Help Employees and Managers decide what clothing it is appropriate to wear to work

- Managers are responsible for ensuring that this dress code is observed by their reportees and that a common sense approach is taken to any issues that may arise. Any enquiries regarding the operation of our dress code (including whether an article of clothing is suitable to wear to work) should be made to the Manager
- Failure to comply with the dress code may result in disciplinary actions
- Dress code is reviewed periodically to ensure that it reflects appropriate standards and continues to meet organizational needs. This policy does not form part of any Employee's contract of employment and may be amended at any time
- Employees represent the Company while working with the Clients and engaging in the public. Employee's appearance contributes to the Company's reputation and the development of its business
- **Religious and Cultural Dressing:**
  - Employees may wear appropriate religious and cultural dress (including but not limited to clerical collars, head scarves, skullcaps, and turbans) unless it creates a health and safety risk to them or any other person or otherwise breaches this policy
  - Employees may consult with their Manager regarding further information and guidance on cultural and religious dress in the workplace
  - Priority is always given to health and safety requirements. Where necessary, advice will be taken from the HR Compensation and Benefits 2 team (compensation2@tresvista.com)

1.6 Business Cards

The purpose of this policy is to provide Employees with business cards, for work-related purposes, upon request.

Eligibility

This policy is applicable to all Employees effective their date of joining.

Particulars

- Employees requiring business cards must raise a Helpdesk ticket to the FMS department under the subcategory 'Business Cards'
  - The FMS department will share the final template of the business cards with Employees
  - Employees can get the business cards printed and reimburse the expenses at actuals, subject to submission of the relevant bills and receipts
- It is recommended that Employees carry sufficient number of business cards at all times, for networking purposes such as work-related meetings or trips

1.7 Personal Relationships

Employees must notify the firm in case they have a personal relationship with another Employee, intern, third-party resource, or Partner. Such information is collected by the Company to avoid and handle any probable conflict of interest, complaints of harassment (sexual or otherwise), favouritism, discrimination, etc. resulting out of any personal relationships.

Definition

Personal relationships with another Employee, intern, third-party resource, or Partner include but are not limited to:

- Romantic relationships and/or,
- Family relationships (including but not limited to, parents/in-laws, children/grandchildren, grandparents/in-laws, siblings/in-laws, spouse, biological uncles/aunts, cousins, stepparents, stepsiblings, step-grandparents, step-children)

Points to Note

- Employees must avoid any circumstances that could be viewed as a conflict of interest or act as a cause of potential sexual harassment
- Employees should be mindful of maintaining data confidentiality (such as not sharing trade secrets, confidential and sensitive information, etc.) with whom they have a personal relationship in the workplace
- Employees must immediately notify their respective Managers and HR Compensation and Benefits 2 team (compensation2@tresvista.com) in case of personal relationship with another Employee, intern, third-party resource, or Partner:
  - Within one's team/department
  - Reporting directly or indirectly to the Employee
  - Belonging to a different team/department
- Public display of affection in the office is strictly prohibited
- TresVista does not take any disciplinary action simply because an Employee is in a personal relationship with a colleague. However, it may take necessary actions in case such personal relationship poses a risk to Company's business or culture

1.8 Anti-Sexual Harassment Policy

Overview

The Company is committed to maintaining a workplace free from sexual harassment. Sexual harassment is a form of workplace discrimination. The Company has a zero-tolerance policy for any form of sexual harassment, and all

Employees are required to work in a manner that prevents sexual harassment in the workplace. This policy is one component of the Company's commitment to a discrimination-free work environment. Additionally, Employees should also refer to the Diversity, Equity, and Inclusion Policy and Anti-harassment and Bullying Policy under the header of people policies of this handbook Employee

Particulars

- The Company's sexual harassment policy applies to all Employees, applicants for employment, interns, whether paid or unpaid, contractors and persons conducting business with the Company
- Sexual harassment will not be tolerated in the organization, irrespective of the designation of the Employee. Any Employee or individual covered by this policy who engages in sexual harassment or retaliation will be subject to remedial and/or disciplinary action, up to and including dismissal
- **Retaliation Prohibition:** No person covered by this policy shall be subject to adverse employment action including being discharged, disciplined, discriminated against, or otherwise subject to adverse employment action because the Employee reports an incident of sexual harassment, provides information, or otherwise assists in any investigation of a sexual harassment complaint. The Company has a zero-tolerance policy for such retaliation against anyone who, in good faith complains or provides information about suspected sexual harassment. Any Employee of the Company who retaliates against anyone involved in a sexual harassment investigation will be subjected to disciplinary action, up to and including termination. Any Employee, intern (paid or unpaid), or non-Employee working in the workplace who believes they have been subject to such retaliation should inform a supervisor, Manager, or Human Resources. Any Employee, intern (paid or unpaid) or non-Employee who believes they have been a victim of such retaliation may also seek compensation in other available forums, as explained below in the section on Redressal Mechanisms
- Sexual harassment is a violation of TresVista's policies, is offensive and unlawful, and subjects the Company to liability for harm to victims of sexual harassment. Harassers may also be individually subject to liability. Employees of every level who engage in sexual harassment, including Managers and supervisors who engage in sexual harassment or who knowingly allow such behavior to continue, will be penalized for such misconduct
- This policy applies to all Employees, interns (paid or unpaid), and non-Employees and all must follow and uphold this policy. This policy must be posted prominently in all work locations and be provided to Employees upon hiring

Redressal Mechanism

- Sexual harassment is against the law. All Employees have a legal right to a workplace free from sexual harassment, and Employees can enforce this right by filing a complaint internally with the Company via Grievance Procedure, or through the Employment Tribunals. In the first instance, Employees are requested to raise such concerns internally through the Grievance Procedure

- The Employee can either contact the Human Resources department or their Managers, if they believe they have been subjected to sexual harassment or know of an incident involving sexual harassment. Managers and supervisors are required to report any complaint that they receive, or any harassment that they observe to the Human Resources department
- All Employees are encouraged to report any harassment or behaviour that violate this policy. The Company will provide all Employees a complaint form for Employees to report harassment and file complaints
- The Company will conduct a prompt, thorough and confidential investigation that ensures due process for all parties, whenever management receives a complaint about sexual harassment, or otherwise knows of possible sexual harassment occurring. Effective corrective action will be taken whenever sexual harassment is found to have occurred. All Employees, including Managers and supervisors, are required to cooperate with any internal investigation of sexual harassment

1.9 Proof of Employment

Eligibility

TresVista provides an employment verification proof to all Employees, on request.

Particulars

Proof of employment may be required by Employees for various purposes, including but not limited to the ones mentioned below:

- **Visa Application:** An Employee who is applying for a foreign visa may request for an employment verification letter by the Company. TresVista has a set template for such letters, which includes information such as the Employee's designation and tenure, travel dates and destinations, name and address of the consulate, and salary (if required). In case, an Employee wants the letter in a particular format, they must draft the letter and send it to the HR Operations team (ops@tresvista.com). The letter is then signed by an authorised signatory
- **Bank Application:** An Employee applying for a bank loan, or a credit card may require an employment verification letter from the Company. In certain cases, an Employee may also need to get some of their personal documents attested by the Company

Procedure for Application

- The Employee may raise a ticket to the HR Operations team (ops@tresvista.com) for a letter and/or attestation. Employees can expect to receive the documents within two (2) working days after raising a ticket with the required information
- The letters only specify the Employee's total gross compensation. Details on bonus are not shared

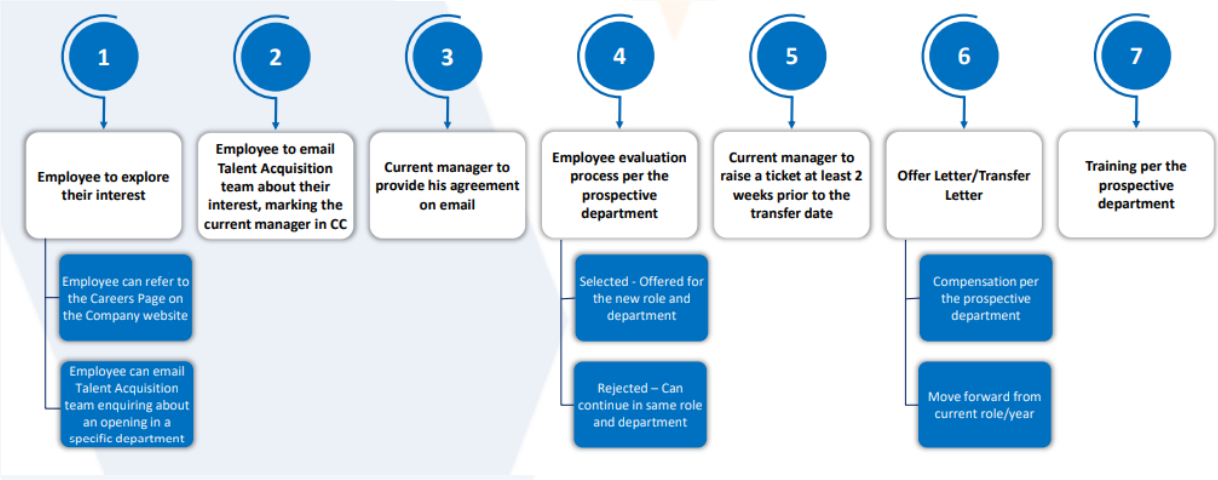
1.10 Inter-Department Transfer Policy

The purpose of this policy is to allow Employees to explore, pursue their interests, develop skill sets, and create a long-term career progression, by encouraging movements within the Company. The intention is to boost Employee morale, simplify the transition process and create an engaging work environment.

Eligibility

- Employees should have completed at least one (1) annual review period in the organization from their date of joining/promotion, at the time of application
  - For example, if an Employee was promoted to Associate w.e.f. July 01 2021, they are not eligible for an inter-department transfer until June 30, 2022

Particulars



Manager

- Employees are required to reach out to the Talent Acquisition team at (recruitment@tresvista.com), expressing their interest for an inter-department transfer, marking their current Manager
  - The current Manager should be aware of the transfer and share approval over email to initiate the process
- All processes (approvals, evaluation, communication, etc.) concerning the transfer, which approximately takes three-four (3-4) weeks, must be completed before a transfer ticket is raised by the current Manager
- The Employee would continue to proceed in the Company per the career progression established by TresVista unless a change in level or role, or designation is required based on suitability, role availability, and business requirement
- The compensation of the Employee is aligned to the prospective department's compensation structure
- The Employee is required to undergo training as required by the prospective department

Points to Note

- Consideration of transfer requests is contingent upon there being a relevant opening in the prospective department the Employee is interested in
- All transfers are subject to completion of any obligations of the previous role at the time of movement (e.g., training credits)
- Transfer are effective only with the annual review period (i.e., January 01/July 01, as applicable)
- In case the inter-department transfer also includes an entity transfer, the Employee is required to co-operate in following the defined process for entity movement, this may include transferring employment from one group entity to the other or secondment to the other entity (at TresVista's discretion), with no impact on the continuity of employment
- The eligibility criteria and transfer timelines mentioned above are **not** applicable for movements intended to address contractual client requirements, and any transfers required by the firm for restructuring purposes

1.11 Performance Appraisal

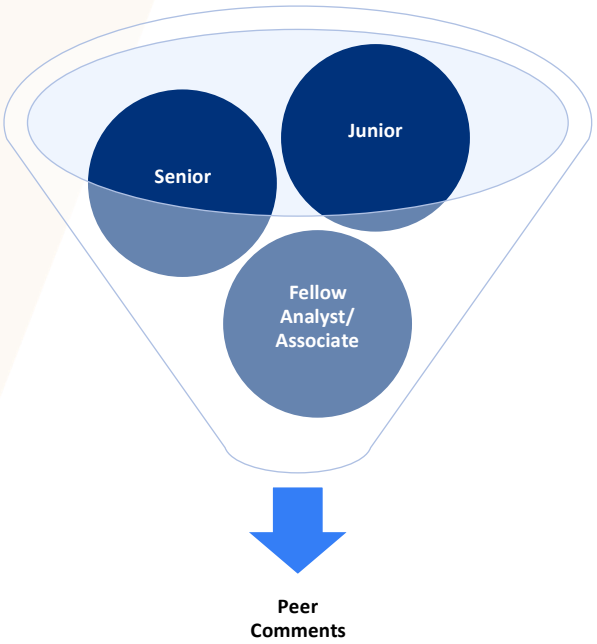
"A Company's Employees are its greatest asset and your people are your product."

Richard Branson

In keeping with this mantra, TresVista is committed toward the success of its Employees and to this end, aims to provide a holistic review process based on constant performance monitoring and regular, objective feedback.

Overview

Everyone values both honest criticism as well as the praise that is due for their effort. The review process at TresVista is 360°, where an Employee is given feedback from multiple sources including peers, seniors, juniors, Manager, and themselves. All Employees have their own learning curve, and must accept feedback in a constructive way.



Eligibility

An Employee is eligible to write and receive reviews if:

- Their date of joining is as follows (For first mid-year review):
  - June Review Period: On or before March 15
  - December Review Period: On or before September 15
- They are not serving notice

Timelines

Performance reviews are conducted semi-annually at TresVista. An Employee will get a mid-year review and a year-end review in an annual review period.

Objectives

The aim of performance appraisals is to:

- Encapsulate the reviewee's performance over the review period
- Provide constructive criticism on areas of development
- Provide a basis for coaching to improve Employee performance
- Assist in setting goals for Employee development
- Assist in making systematic judgments

- Provide feedback to the reviewee from multiple sources
- Assist in realigning the culture of a team and/or the Company
- Provide the Company with performance measures to be used in making promotion and compensation decisions

Points of Evaluation

Parameters

A performance review assesses the reviewees' ability to achieve results across various parameters. The principal categories include:

- Business Results
- Strategic Thinking
- Personal Effectiveness

The 'Self-Appraisal Form' will also have a section on 'Areas of Interest for Development and 'Suggestions for Improving Your Experience at TresVista' and a tabular summary of the projects worked on during the review period.

Ratings

Performance will be rated on a scale of 1 to 5 with the latter demonstrating the highest level of performance.

Rating	Meaning	Description
NA	Not Applicable	Not tested
1	Major Improvement Required	Lack of effort, knowledge, and ability
2	Some Improvement Required	Obvious and repeated mistakes, but shows effort/sincerity
3	Consistent Average Performance	Meets expectations
4	Often Exceeds Performance Expectations	Exceeds expectations
5	Consistently Exceeds Performance Expectations	Displays ability to achieve results at the next level

It should be noted that:

- The individual ratings depend on the perspective of the reviewer, and hence, any serious accreditation/allegation by self or peer reviewer as evidenced by the extreme ratings, has to be backed by credible examples. If one has no opinion on a particular sub-category, rating "NA" is the best option. The Manager comments will not be based on singular incidents or examples
- The category ratings on the review are meant to disclose where the person stands on the date of the review,

whereas an overall rating for the review period describes the reviewee's performance over that entire review period

- The expected level of performance is benchmarked against the expectation of the specific year of the title/role
- The overall rating in the year-end review will be a function of the full year's performance and determines performance bonus
- In order to achieve an overall rating of 5, one has to get a rating of 4 and 5 in all categories. Likewise, an overall rating of 1 means, that an Employee would have got a rating of 1 or 2 in most categories

Process

The review process is important for each Employee and a thorough, accurate, and sincere effort is deserved in recognition of the reviewee's efforts. The HR Department will notify all eligible Employees regarding the initiation of the review process, and communicate important dates.

Solicitation

The solicitation period is the time during which the reviewee sends requests to all those Employees who they have worked with. A reviewee is expected to solicit at least two other Employees in order for the Manager to get holistic feedback about an Employee's performance. Employees may accept or reject solicitation requests.

Writing Reviews

An Employee has to write and submit the self and peer reviews within the given deadlines. Reviews have to written and submitted on Review Portal. For reference, an Employee can also access his previous reviews, if any, under 'My Review Reports'. During this period, Review Portal can be accessed from outside the office.

Employees are encouraged to write an unsolicited review, positive or negative, for any reviewee for whom they feel they have comments that would add value to the review process. The identity of unsolicited reviewers is not known to the reviewee.

An Employee is responsible to ensure that Employees who have accepted their solicitation request, submit reviews in a timely manner. Once the process is closed, no submissions will be accepted on Review Portal. It will be up to the Manager whether they want to consider any review provided to them outside of Review Portal.

Review with Manager

The Manager consolidates all the peer comments and evaluates the reviewee themselves. The 'Peer Comments' section includes comments from all reviewers except those of the Manager. Peer comments are provided to the reviewee without revealing the identification of the specific reviewer. A review document is handed out to the reviewee, after which the Manager or HR has a one on one conversation with them. Managers should avoid taking any holidays during this time.

Outcome

The performance review may result into the following:

- **Probation or Confirmation:** An Employee shall be kept under probation, for the period specified in their Company issued offer letter, subsequent to which they will either be confirmed or their probation period will be extended for a duration of two months, at Manager's discretion. Confirmed Employees will receive relevant communication to this effect
- **Promotion:** An Employee may receive a promotion during a mid-year or year-end review. The promotion may take effect immediately or following the completion of the next review period as stated in their promotion offer

1.12 Organizational Hygiene

The purpose of this policy is to ensure that the perception of TresVista is standardized across all platforms and provide guidelines to Employees on how to communicate with internal and external stakeholders.

Eligibility

This policy is applicable to all Employees.

Particulars

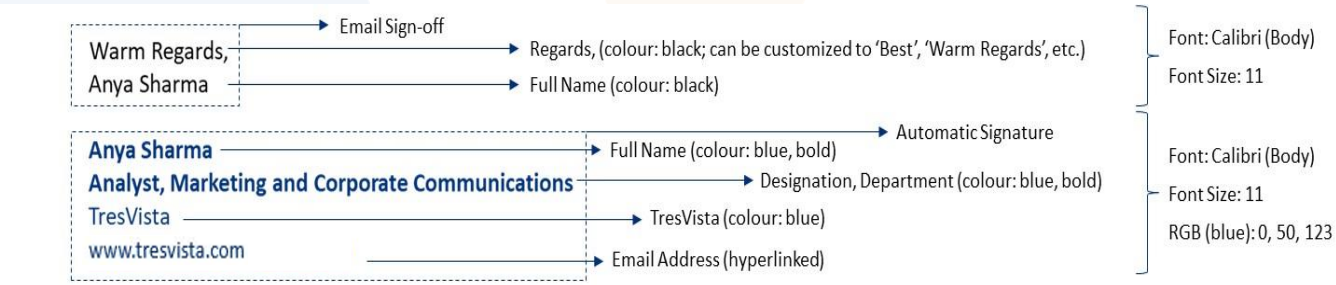
Organizational Information and Materials

- Organizational information talks about the organization, its values, culture, Employees, services, clients, business operations, partnerships, and activities and is accessible to all Employees in the organization (E.g., PACT, boilerplate, highlights, value proposition: why partner with us, geographic presence, client break-up, TresVista services, TresVista ecosystem, support framework, client testimonials, Employee count, office information, organizational structure, leadership bios, service delivery model, etc.)
- Organizational materials include but are not limited to pitchbooks, brochures, CSR material, decks, recruitment decks/literature, firm intro decks, department intro decks, and firmwide training manuals
- Employees using any organizational information and material must refer to the templates saved on SharePoint and ensure that they are using the latest version of data available. These templates will be updated by the Marketing and Corporate Communication department on a quarterly basis

Email Signatures

- Employees are required to sign their emails in the defined format, to maintain certain etiquette and professionalism in the organization

- **SVPs and below:**
  - SVPs and below must follow the standard email signature format, as mentioned below. Default format signatures should not be treated as a replacement for writing an email sign-off (e.g., Best/Warm Regards/Cheers followed by the name of the Employee)
  - The email signature need not be present for consecutive emails that are/become a part of an ongoing conversation
  - Client-facing teams using a Virtual Desktop Infrastructure (VDI) must make an educated decision with regard to email signatures, keeping in mind the client relationship and firm guidelines
- Standard email signature format:



Out of Office

- When on leave, Employees should set up a formalized out-of-office response for all internal or external emails and MS teams messages received in their absence to help notify the sender of their unavailability and inform them of an alternate point of contact
- The standard out-of-office email template, as applicable, is as follows:

  Hello,

  Thank you for your email. I am currently on leave with limited access to my emails and will be back on <day>, <month date, year>. In my absence, please reach out to <Alternate Contact> <(Alternate contact's email-id)> for any immediate assistance.

  Email Signature
- **Internal Emails:** Employees must follow the below guidelines for internal email replies:
  - **SVPs and above:**
    - Decide whether they need an out-of-office email and customize their communication accordingly
    - Help determine the point of contact to be mentioned in the out-of-office email for all team members
  - **EVPs:** Redirect out-of-office emails to their VPs/Associates, as applicable

- **VPs:** Redirect out-of-office emails to their EVP/Associates, as applicable
- **Associates:** Redirect out-of-office emails to their VPs/EVPs
- **Analysts:** Discuss with their Managers and accordingly set an out-of-office email, if deemed necessary

- **External Emails:** Employees must follow the below guidelines for external email replies
  - **SVPs and above in the Client Development department**: Avoid setting out-of-office emails unless they are not able to access their emails for an extended period of time
  - **Client-facing teams:**
    - Large teams with a DL should not have an out-of-office email when individual Employees are on leave
    - For small teams consisting of a VP, an Associate, and an Analyst, it is the responsibility of the EVP or VP, as applicable, to determine whether they should have an out-of-office email
  - **Teams managing external stakeholders other than clients (e.g., vendors, campus communications, etc.):** Setting an out-of-office email is not required

Templates

- **Microsoft Teams Background:**
  - When not working from office, Employees to use their best judgment on whether to use an MS Teams background for internal meetings, whereas for external meetings, it is advisable to use the standard MS Teams background, as saved on SharePoint
  - When attending calls from the office, Employees may choose not to use a background
  - Employees may choose to use the celebratory or milestone-related backgrounds sent firmwide
  - Employees must not use the generic templates available on MS Teams
- **PowerPoint:**
  - Standard PowerPoint template, as saved on SharePoint, must be used for all internal and external presentations
  - Landscape template must be used for digital copies of the deck, while the letter size template must be used if the deck needs to be printed
- **Word:** Standard Word templates, as saved on SharePoint, must be used for all internal and external documents

1.13 Brand Communication Guidelines

The purpose of this policy is to educate Employees on the set standards that convey how TresVista should be presented in order to maintain a strong brand identity and consistency in communication across various platforms.

Eligibility

This policy is applicable to all the Employees

Particulars

Brand Tonality

- For any communication piece, Employees are required to first analyse the audience, situation, and platform of communication
- **Guidelines on Messaging and Tonality of the Communication:**
  - If the situation requires the tone of the message to be serious, Employees must be transparent, establish a two-way conversation, show that they are genuinely listening, and be approachable in their communication
  - It is expected that Employees are straightforward but not rude in their communication
  - If the communication piece is light-hearted, fun, or celebratory, Employees may structure their message accordingly and make the communication less verbose
  - Employees are encouraged to engage in non-confrontative humor but also have thoughtful conversations
  - Some best practices in this regard are as follows (including but not limited to):
    - Avoid any kind of suggestive innuendos
    - Be humble and respectful
    - Enable everyone to understand the communication and also be receptive to their viewpoints
    - Do not be authoritative or snobbish
    - Help others if possible, aim to not make others feel vulnerable
  - A few references in this regard are as follows:
    - Use pop culture references to make the communication more relatable, captivating, and entertaining (e.g., Marvel, cult movies, art, and songs)
    - Encourage teams to use memes, and opt for a young, easily consumable vocabulary (e.g., Mumbai Police Tweets)
    - Avoid words like ‘graciously’ and ‘courteously’
    - Avoid words like ‘booze’ and ‘drugs’, instead use ‘alcohol’, if required and necessary
    - Use ‘TVite’, instead of the term ‘Employee’, except for process/policy-related communications

Guidelines for Inclusive Communication

- For any communication piece, Employees must ensure that they are mindful of social sensibilities and social acceptance of words, terms, phrases, etc., as mentioned below:

- Ensure communication is neutral with regard to physical differences such as gender, disabilities, etc.
- Avoid using words like ‘handicapped’ and ‘disabled’; instead, use the term ‘persons with disabilities’, where appropriate
- Be careful about using icons that only refer to a man or woman and aim to be more inclusive
- Use authentic ways to include, portray, and integrate diverse populations, e.g., use gender-neutral pronouns ‘they/them’ instead of ‘he/she,’ ‘Ms.’ instead of ‘Miss/Mrs.’, ‘everyone and all’ instead of ‘ladies and gentlemen’, ‘chairperson’ instead of ‘chairman’ and ‘chairwoman’
- Employees must avoid stereotyping and should:
  - Be cognizant of reactions and assumptions and understand that it is important to acknowledge and identify stereotypes
  - Avoid jokes/assumptions that create stereotypical views
  - Avoid false assumptions, stereotypes, and biases that affect the fairness of decision making
  - Examples of stereotypes include but are not limited to:
    - Culture: people from x country are rude
    - Social: x types of people are weird/shallow
    - Racial: people of x race are athletic/good at maths
    - Gender: people of x gender are lazy/beautiful
    - Religious: people who practice x religion are intolerant/generous

2. Leaves and Holidays

This section provides information on firm-wide holidays, personal days and vacation days and the relevant application process. For further details related to other types of leave, kindly refer to the UK Addendum.

2.1 Firm-wide Holidays (Public and Bank Holidays)

This section provides information on firm-wide holidays decided per the list of government holidays in the given leave cycle.

Eligibility

All Employees are eligible for the designated firm-wide holidays.

Particulars

- Firm-wide holidays consist of public holidays, and/or other religious events and festivals

- A list of eight (8) firm-wide holidays decided as per the list of government holidays will be provided depending upon the Employee's office location
- There is no application procedure for these holidays, and they are auto applicable to all Employees

2.2 Personal Days

Personal Days are unplanned leaves that do not require prior approval of the Manager, as these leaves are provided to accommodate for any unplanned/unforeseen personal emergencies and sickness.

Eligibility

All Employees are entitled to Personal Days from their date of joining.

Particulars

- A total of five (5) paid Personal Days are available in Leave Cycle, calculated on a pro rata basis.
- **It should be noted that:**
  - Entire Leave Balance pro-rated for the annual Leave Cycle is made available to the Employee for utilization from their date of joining
  - Employees cannot carry forward Personal Days to the next annual Leave Cycle, and all unused days lapse at the end of the annual Leave Cycle
  - More than two consecutive Personal Days for any reason other than sickness can be deemed as Vacation Days
    - In case of sickness, the Employees can take more than two Personal Days at the discretion of the Manager
  - If an Employee's Personal Days are exhausted, the Vacation Days can be utilized with the prior approval of the Manager
  - The Company may ask Employees to take (or not to take) a leave on particular dates, including when the business is closed, particularly busy, or during notice period

Procedure for Application

- A Personal Day does not need prior approval from the Manager
- However, the Employee should inform the Manager as soon as they are aware that they require a Personal Day
- Employees must apply for leaves availed by them on DarwinBox under the 'Leaves and Flexwork' module, within the monthly leave and attendance timeline defined by the Corporate Finance department

2.3 Vacation Days

About this Policy

- This policy sets out the arrangements for Employees wishing to take vacation days (also known as annual leave)
- This policy covers all Employees at all levels and grades, including full-time, part-time, permanent, and fixed-term Employees, Managers, directors, trainees, and homeworkers
- This policy does not form part of any Employee's contract of employment and may be amended at any time. The Company may also vary the policy as appropriate in any case

Eligibility

All Employees are entitled to Vacation Days from their date of joining.

Particulars

- The Company's holiday year runs from 01 January – 31 December. If the Employee starts or finishes their employment at any time through the holiday year, the leave entitlement during that year shall be calculated on a pro-rata basis
- Entire Leave Balance pro-rated for the annual Leave Cycle is made available to the Employee for utilization from their date of joining
- Unless otherwise set out in the employment contract, Employees are entitled to [15] days' paid holiday in each holiday year, or the pro rata equivalent in case of part time. In addition, the Employees are entitled to take the usual public holidays in England and Wales or days in lieu where the Company requires Employees to work on a public holiday
- For the avoidance of doubt, the first four weeks of the leave taken in any holiday year shall be deemed to be the leave derived from regulation 13 of the Working Time Regulations 1998 (*SI 1998/1833*) and the remainder shall be deemed to be derived from regulation 13A of those regulations.
    - Currently, the law states that regulation 13 leave shall be paid at the rate of "normal remuneration" whereas regulation 13A leave may be paid at the rate of basic salary only
    - If the remuneration normally includes variable elements, such as commission or overtime, Employees will be notified separately whether such payments will be included in the regulation 13 holiday pay
    - A decision to reflect certain elements of the remuneration in holiday pay on one or more occasions shall not indicate that it will be included on future occasions
- Except as set out in this policy, holiday entitlement must be taken during the holiday year in which it accrues. Any holiday not taken by the end of the holiday year will be lost and will not be encashed
- Unused holiday can only be carried over to another holiday year:
    - In cases involving sickness absence as set out below;

- In cases of maternity, paternity, adoption, parental or shared parental leave, as set out below;
- In any other case where the Manager has given permission in writing limited to no more than five; and
- If otherwise required by law

Points to Note

- Employees are advised not to take annual leave for more than five (5) consecutive working days at a given time
- All holidays must be approved in advance by the Manager. Employees should normally give at least one month's notice of holiday requests to allow planning of rotations or work schedules where necessary and must not make travel bookings until approval has been given
- Annual leave requests may be denied by the Managers if there are client demands/critical deliverables or capacity constraints
- If the Manager requires an Employee to cancel or reschedule annual leave that has already been approved, any expenses that may be incurred in cancelling or rescheduling, that are not covered by the Employee's travel insurance, are reimbursed. This reimbursement is expensed to the respective department budget on producing relevant receipts. Annual leave will be cancelled only in the most urgent situations
- The Company may ask Employees to take (or not to take) a leave on particular dates, including when the business is closed, particularly busy, or during notice period
- Exceeding annual leave entitlement may result in a loss of pay and may also have an adverse impact on the Employee's performance evaluation
    - At the point of exit, TresVista can make a deduction from the Employee's final salary payment (or other payments due on termination of employment) for any annual leave days taken in excess of the Employee's accrued annual leave entitlement calculated on a pro rata basis till the last day of employment
    - Employees may be required to take vacation day during their notice period or whilst on garden leave

Sickness during Periods of Holiday

- If the Employees are sick or injured during a holiday period and would have been incapable of work, they may choose to treat the period of incapacity as sick leave and reclaim the affected days of holiday
- Employees already on sick leave before a pre-arranged period of holiday may choose to cancel any days of holiday that coincide with the period of incapacity and treat them as sick leave
- Company sick pay will only be paid for such days if the Employees comply with the Absence Management Policy, including notifying the Manager immediately of their incapacity and obtaining medical evidence if required (even if the Employees are abroad)

- Dishonest claims or other abuse of this policy will be treated as misconduct under the Disciplinary and Capability Procedure

Long Term Sickness Absence and Holiday Entitlement

- Holiday entitlement continues to accrue during periods of sick leave
- If Employees are on a period of sick leave which spans two holiday years, or if they return to work after sick leave so close to the end of the holiday year that they cannot reasonably take the remaining holiday, they may carry over unused holiday to the following leave year
- Carry over under this rule is limited to the four-week minimum holiday entitlement under EU law (which includes bank holidays), less any leave taken during the holiday year that has just ended
- If the Employee has taken four weeks' holiday by the end of the holiday year, they will not be allowed to carry anything over under this rule. If they have taken less than four weeks, the remainder may be carried over under this rule. For example, a full-time Employee who has taken two weeks' holiday plus two bank holidays before starting long-term sick leave can only carry over one week and three days
- Any holiday that is carried over under this rule but is not taken within 18 months of the end of the holiday year in which it accrued, will be lost
- Alternatively, Employees can choose to take the paid holiday during their sick leave, in which case they will be paid at the normal rate

Family Leave and Holiday Entitlement

- Holiday entitlement continues to accrue during periods of maternity, paternity, adoption, parental or shared parental leave (Referred to collectively in this policy as family leave)
- If Employees are planning a period of family leave that is likely to last beyond the end of the holiday year, they should discuss their holiday plans with the Manager in good time before starting the family leave. Any holiday entitlement for the year that cannot reasonably be taken before starting the family leave can be carried over to the next holiday year
- For the avoidance of doubt this covers the full holiday entitlement of the Employee
- Any holiday carried over should be taken immediately before returning to work or within three months of returning to work after the family leave

Arrangements on Termination

- On termination of employment, Employees may be required to use any remaining holiday entitlement during their notice period. Alternatively, they will be paid in lieu of any accrued but untaken holiday entitlement for the current holiday year to date, plus any holiday permitted to be carried over from previous years under this policy or as required

by law. Employees are entitled to be paid at a rate of 1/260th of their full-time equivalent basic salary for each day of untaken entitlement

- If the Employee's normal remuneration in the 52 weeks prior to the date on which their employment terminates also includes variable pay such as commission or overtime payments, some such elements will be factored into the calculation of their final holiday payment. For each day of untaken holiday entitlement, Employees are usually entitled to be paid at a rate of 1/260th of their full-time equivalent normal remuneration in the last 52 weeks of their employment

Procedure for Application

- Employees must apply for leaves availed by them on DarwinBox under the 'Leaves and Flexwork' module, within the monthly leave and attendance timeline defined by the Corporate Finance department
- When annual leave is requested, it should include all days like weekends and/or public and bank holidays if they fall part of the vacation
  - Although these days would not be counted against the Employee's annual leave entitlement, it will indicate that the Employee is unavailable to come to work on those days
- **It should be noted that:**
  - Employees are encouraged to discuss with their Managers and then plan their annual leave. This is to ensure that the deliverables/capacity is managed effectively and in a timely manner
  - An Employee can raise a grievance through the Grievance Procedure if they feel they were denied annual leave days unfairly

3. Exit

3.1 Notice Period

- Following acceptance of an offer of employment, if an Employee desires to resign, they are required to serve notice ("Notice Period"), as mentioned in their employment contract. In case the Company does not wish to avail the services of the Employee, it may in its sole discretion make a payment in lieu of all or part of the Notice Period, net of any lawful deductions
- The Company may terminate an Employee's employment by giving the requisite notice as per the notice period set out in the offer letter and Employment Agreement or statutory minimum notice, whichever is the greater ("Notice Period"). The Company may in its sole discretion make a full payment in lieu of all or part of the Notice Period, net of any lawful deductions

- Any lawful deductions as mentioned in this clause shall include income tax and National Insurance contributions, any adjustment to final pay if annual leave in excess of accrued annual leave entitlement up to the termination date has been taken by the Employee, and any amounts towards any Company assets which are not returned by the Employee on the last working day or are not returned in satisfactory condition
- The Employee's Manager approves the separation request on DarwinBox. In case the resignation is not acted upon within the defined TAT of 5 days, the resignation will be auto approved by the system which will be treated as the final approval for HR Operations team (ops@tresvista.com) to proceed with the separation formalities
- If an Employee is a part of any disciplinary proceedings, the Company reserves the right to reject their resignation request, at its sole discretion

3.2 Termination

Notwithstanding anything contained herein to the contrary, the Company can terminate the employment agreement with cause on the grounds including, but not limited to, misconduct, negligence, fraud, dishonesty, or breach of the employment agreement or of the Company's policies and procedures in force at the time.

3.3 Employee Separation Procedures

It is recommended that Employees who choose to terminate their employment should officially raise a separation request via DarwinBox, stating their last date of employment and the reason for leaving. Employees also accept that they must return all Company equipment and/or property before the last day of employment, including but not limited to, Company laptop, keys, access cards, Company phones, etc.

3.4 Garden Leave

The purpose of this policy is to safeguard data and confidential information that Employees may be privy to and protect the interests of the organization in the event of their exit.

Eligibility

This policy is applicable to all Employees designated as Vice President (VP) and above, effective their date of joining or Promotion, as applicable.

Particulars

- During any period of notice to terminate the employment (whether given by the Employee or the Company), or if the Employee purports to terminate his employment in breach of these terms, the Company may, in its absolute discretion, for all or any part of the Employee's notice period or such other extended period determined by the

Company (as the case may be) up to six months place the Employee on “Garden Leave”. During any such period of Garden Leave the Company may require the Employee to be:

- Suspended, in whole or in part, from their roles and responsibilities in the organization and restricted to hold any powers on TresVista’s behalf
- Bound by the policies of TresVista and the terms of their employment, including express and implied duties of confidentiality and good faith, as applicable and remain employed with TresVista
- Not permitted to contact or deal with any party associated with the Company, including but not limited to Employees, clients, vendors, or other business contacts of the Company or any of its affiliates
- Required to remain readily available and carry out any alternative duties and/or perform specific duties as may be expressly assigned to them by the Company
- Not permitted to enter the Company premises, and their access to emails and the network of the Company will be revoked

- **Exclusivity Coverage:** During the period of Garden Leave, Employees are not permitted to work elsewhere, in any capacity, whether for a third party or one’s own self (whether paid or unpaid)
- **Compensation:** For the duration of Garden Leave, Employees are paid their gross salary, as applicable. However, in accordance with the terms of relevant applicable policies and scheme rules, bonus and other monetary increments/incentives including the award of fresh ESOPs, equity, etc., are not paid/applicable
- **Points to Note:**
  - Duration of Garden Leave and notice period can be waived at the sole and absolute discretion of the Management
  - Garden Leave is included in an Employee’s tenure and the last day of Garden Leave is treated as their last day of employment in the organization

3.5 Non-Solicitation and Non-Compete

Employees may be subject to post-termination restrictions (such as non-solicitation of clients or Employees restrictions or a non-compete restriction). Any such post-termination restrictions will be set out in an Employee's contract of employment (or any subsequent amendment thereof).

(C) Monetary Policies

1. Business Travel – Domestic

The purpose of this policy is to define guidelines and criteria for domestic travel of Employees, covering aspects such as travel, accommodation, and various allowances.

Eligibility

This policy is applicable to all Employees traveling within the USA, UK, Singapore, Middle East, considering that such travel is undertaken for lead generation/prospective client outreach.

Particulars

- Employees can reimburse conveyance, accommodation, and food expenses for travel undertaken by them as a part of lead generation, prospective client outreach, sales trip or any non-local events they attend for networking purposes
  - Allowance limits can be referred to under 'Annexure – Monetary Policies' of this Handbook
  - Other expenses such as local travel or taking a prospective client for coffee/lunch, will be reimbursed only if such activities are related to lead generation
- **Allowable Expense:**
  - **Air Travel:**
    - All travel requisitions and any changes made to the request thereof, must be approved by the Employee's Manager, as applicable
    - Business trips must be planned at least four weeks in advance to ensure that they are purchased on reasonable lines
      - Employees must submit the relevant supporting documents if tickets are purchased at a higher cost and the Corporate Finance department will accordingly evaluate such requests
    - Flights should be selected based on cost and convenience and any additional cost incurred for upgrades will not be borne by the Company
    - Associate Directors and above should be allowed to travel in Premium Economy class as long as it is within the existing travel budget
    - Change in travel bookings due to business reasons will be accommodated within the policy, up to the limit defined in the travel budget

- Any additional cost because of change in travel/hotel bookings for personal reasons will be borne by the Employee and adjusted from their salary
- FMS department will inform Corporate Finance department of the salary adjustments to be made

- **Accommodation:**
  - All bookings should be made by Employees and accordingly reimbursed in accordance with the limits mentioned in the Annexure. Please note:
    - SVPs and above can book rooms on single occupancy basis
    - EVPs and below must share rooms if they are traveling with another Employee
    - The only exception is made in a situation where male and female Employees travel together
- **Hosts:** In case an Employee is staying with family, friends, or acquaintances, they will be entitled to a host entertainment amount per the limits mentioned in the Annexure, in order to entertain their host, as the Employee deems fit
- **Daily Allowance:**
  - Employees can claim daily allowance, per the limits defined in the Annexure, for their food expenses while traveling
  - All such expenses are reimbursable upon submission of the relevant receipts/bills
  - Employees may claim this amount in advance based on the number of days they are traveling, in order to do so, Employees must submit their travel tickets to the Corporate Finance department which will evaluate and accordingly process these requests
  - In case of extended stay for personal reasons, daily allowance will not be provided
- **Conveyance:**
  - The Company incurs or reimburses Employee conveyance expenses per day in accordance with the limit mentioned in the Annexure
  - When traveling, it is recommended that Employees use public transport to ensure that their commute is cost-effective
  - In case public transport is unavailable, Employees may use their discretion in determining the mode of transport
  - When traveling with other Employees/colleagues, it is recommended that Employees rideshare/carpool, to the extent possible
  - The Employee must submit receipts of these expenses with the Corporate Finance department in order to claim relevant reimbursements

- In case an Employee is traveling through the day and making multiple stops, it is advisable that they rent a car or cab for the entire day
- In case a car needs to be rented, it is recommended that Employees avail of the insurance policy to minimize exposure to themselves and the Company

- **Client Welfare:**
  - Employees are allowed to claim reimbursements up to a certain amount as defined in the annexure, for client-related expenditures such as business meals or beverages with a client
  - While claiming this amount, Employees must provide the following information to the Corporate Finance department:
    - Name of the individuals, Company, and their designation in the Company
    - Location details of the place where the meal or event was organized
    - Amount and date of the expense
- **Weekend:**
  - Employees are not allowed to reimburse expenses made on weekends unless they have Manager approvals. For example, in case the conference/meeting ended late on Friday night and employees require an extra day for travelling, or if there are back-to-back sales trips which require employees to stay over the weekend, etc.
  - The examples listed above are not exhaustive and it is expected that employees discuss such cases with their Manager before incurring any expenses over the weekend
- **Miscellaneous Expense:**
  - Office services (i.e., faxes, copies, courier, postage)
  - Reasonable laundry, dry cleaning, and ironing for trips exceeding seven (7) days

- **Non-Allowable Expense:**
  - Unsanctioned trips, entertainment, gifts, and/or donations
  - Mini bar items
  - Toiletries and other personal items
  - Membership fees to register for any reward program
  - Service, installation, and/or repairs cost of personal mobile phones
  - Expenses on tobacco
  - Repair, and maintenance of briefcases, luggage, or similar items
  - Loss of cash or other personal property
  - Personal medical supplies
  - Excess baggage charges

- Expenses for travel incurred by companions/ family members
- Other travel expenses considered as 'not necessary' during the trip

Procedure to Claim Reimbursements

- The allowance limits for business travel – domestic are mentioned in the Annexure
- Employees will be issued a Company credit card with a limit of £2,500 for their business expenses
  - The credit card bill will be paid for by the Company within the defined timeline however, Employees should submit the necessary documentation for the business expenses incurred by them on the card
  - Personal expenses incurred on the Company card will not be reimbursed and will be adjusted from the Employee's salary
  - Business expenses not incurred on the Company credit card can be reimbursed by submitting the necessary bills/invoices at accountsoverseas@tresvista.com on or before the 5th working day of the following month from the date on which such expenses were incurred
    - Requests raised by Employees beyond the defined timeline will not be considered and processed further by the Corporate Finance department unless Employees have approvals from their Managers to extend the deadline
- In case Employees are travelling to attend any event for lead generation or to meet a prospective client, the respective event/prospect name must be mentioned while reimbursing such expenses. Reimbursement requests will be rejected if such entries:
  - Are submitted by another employee on behalf of the one who incurred the expense
  - Have incorrect details/do not include any details such as name of the specific prospect/event, etc.
  - Are raised under the incorrect expense head on Microsoft Dynamics 365
- For detailed information concerning the reimbursement process, Employees must go through section 3 of this Handbook, under the header of monetary policies
- A few additional guidelines for claiming expenses for business travel are as follows
  - All reimbursement entries for business travel must be made on the reimbursement portal
  - E.g., When traveling for campus recruitment, reimbursement details must be as follows:
    - Client: HR Recruitment
    - Project: Analyst Financial Services 2020 (Relevant project name)
  - All the bills need to be submitted in electronic mode to the Corporate Finance department
  - If an Employee is unable to submit the original receipt, the expenses claimed will be subject to additional scrutiny, and will be approved/accepted at the discretion of the Corporate Finance department

Points to Note

- Employees are expected to exercise appropriate judgement when using the corporate card or submitting expenses for reimbursement
  - Employees can reach out to their Manager for further details before incurring any such expenses via corporate card
- Employees are expected to keep a track of their individual expenses on a real time basis. In case Employees foresee that their current expenses may exceed the pre-approved budget, they should immediately inform their Managers about the same and should seek approval to increase the budget
  - Such approvals will be subject to the nature of expenses which have been incurred and which are expected to be incurred in future
  - Any expenses incurred over the pre-approved budget without Manager's approval may not be considered for reimbursement
  - In case seeking Manager approval for exceeding the pre-approved budget is not feasible, employees should retain all documentation/proofs related to the incurred expense. Such documentation/proofs will be considered to decide whether these expenses can be reimbursed

2. Business Travel – International

The purpose of this policy is to define guidelines and criteria for international travel of Employees, covering aspects such as travel, accommodation, and various allowances.

Eligibility

This policy is applicable to all Employees traveling internationally from the US, considering that such travel is undertaken for lead generation/prospective client outreach.

Particulars

- Employees can reimburse conveyance, accommodation, and food expenses for travel undertaken by them as a part of lead generation, prospective client outreach, sales trip or any non-local events they attend for networking purposes
  - Allowance limits can be referred to under 'Annexure – Monetary Policies' of this Handbook
  - Other expenses such as local travel or taking a prospective client for coffee/lunch, will be reimbursed only if such activities are related to lead generation

- Expenses incurred by the employees as a part of their prospect outreach will be reimbursed as long as they are incurred as per the guidelines mentioned below:
  - **Air Travel:**
    - All travel requisitions and any changes made to the request thereof, must be approved by the Employee's Manager, as applicable
    - Business trips must be planned at least four weeks, where applicable, in advance to ensure that they are purchased on reasonable lines
    - Flights should be selected based on cost and convenience and any additional cost incurred for upgrades will not be borne by the Company
    - As the travel tickets are booked by the Employee, they are expected to report the number of miles accumulated on their cards as a result of business travel, if any. Employees are expected to redeem these miles for their future business travel
    - Bookings for tickets, rental cars, forex, visa, and insurance formalities are handled by the Employee and will be reimbursed
    - Employees must have a valid passport and credit card with a limit of not less than £1,200 The lack of an appropriate credit card may cause complications leading lead to additional travel costs, which will be borne by the Employee
    - Visa expenses, including travel from their residence to the visa office, will be reimbursed by the Company however, passport-related expenses will not be paid for by the organization
    - In case there is a layover of more than four hours at any airport, Employees may expense entry into a business class lounge
    - Change in travel bookings due to business reasons will be accommodated within the policy, up to the limit defined in the travel budget
      - Any additional cost because of change in travel/hotel bookings for personal reasons will be borne by the Employee and adjusted from their salary
      - FMS department will inform Corporate Finance department of the salary adjustments to be made
  - **Accommodation:** All bookings should be made by the Employee and accordingly reimbursed in accordance with the limits mentioned in the annexure. Please note:
    - SVPs and above can book rooms on single occupancy basis
    - EVPs and below must share rooms if they are traveling with another Employee
    - The only exception is made in a situation where male and female Employees travel together
  - **Daily Allowance:**

- Employees can claim daily allowance, per the limits defined in the Annexure, for their food expenses while traveling
- All such expenses are reimbursable upon submission of the relevant receipts/bills
- Employees may claim this amount in advance based on the number of days they are traveling, in order to do so, Employees must submit their travel tickets to the Corporate Finance department who will evaluate and accordingly process these requests. The boarding pass needs to be submitted with the remaining bills
- In case of extended stay for personal reasons, per-diem reimbursements are not provided

- **Travel Insurance:** Employees who travel on behalf of the Company are covered by comprehensive travel insurance for the duration of their proposed overseas stay. This insurance policy includes coverage of illnesses and accidents. Medical expenses incurred outside the coverage are not reimbursed. Employees can procure the insurance and reimburse this expense per the limit defined in the annexure, by submitting the necessary documentation and applying for it on Microsoft Dynamics 365
- **Client Welfare:**
  - Employees are allowed to claim reimbursements up to a certain amount, as mentioned in the Annexure, for client-related expenditures such as business meals or beverages with a client
  - While claiming this amount, Employees must provide the following information to the Corporate Finance department:
    - Name of the individuals, Company, and their designation in the Company
    - Location details of the place where the meal or event was organized
    - Amount and date of the expense
- **Weekend:**
  - Employees are not allowed to reimburse expenses made on weekends unless they have Manager approvals. For example, in case the conference/meeting ended late on Friday night and employees require an extra day for travelling, or if there are back-to-back sales trips which require employees to stay over the weekend, etc.
  - The examples listed above are not exhaustive and it is expected that employees discuss such cases with their Manager before incurring any expenses over the weekend

Procedure to Claim Reimbursements

- All travel expenses are subject to Manager approval, and basis the allowance limits defined in the Annexure
  - These limits do not apply to SVPs and above, and the detailed guidelines pertaining to them have been mentioned below
- Employees will be issued a Company credit card with a limit of £2,500 for their business expenses

- The credit card bill will be paid for by the Company within the defined timeline however, Employees should submit the necessary documentation for the business expenses incurred by them on the card
- Personal expenses incurred on the Company card will not be reimbursed and will be adjusted from the Employee's salary
- Business expenses not incurred on the Company credit card can be reimbursed by submitting the necessary bills/invoices at accountsoverseas@tresvista.com on or before the 5th working day of the following month from the date on which such expenses were incurred
    - Requests raised by Employees beyond the defined timeline will not be considered and processed further by the Corporate Finance department unless Employees have approvals from their Managers to extend the deadline

- In case Employees are travelling to attend any event for lead generation or to meet a prospective client, the respective event/prospect name must be mentioned while reimbursing such expenses. Reimbursement requests will be rejected if such entries:
    - Are submitted by another employee on behalf of the one who incurred the expense
    - Have incorrect details/do not include any details such as name of the specific prospect/event, etc.
    - Are raised under the incorrect expense head on Microsoft Dynamics 365
- For detailed information concerning the reimbursement process, Employees must go through section 3 of this Handbook, under the header of monetary policies. A few additional guidelines for claiming expenses for business travel are as follows:
    - All reimbursement entries for business travel must be made under the appropriate expense head on Reimbursement Portal, basis the nature of the expense incurred
    - The Employee must submit proof of the exchange rate at which foreign currency has been purchased and expenses have been incurred
    - If an Employee is unable to submit the original receipt, the expenses claimed will be subject to additional scrutiny, and will be approved/accepted at the discretion of the Corporate Finance department
    - All the bills need to be submitted in electronic mode to the Corporate Finance department
    - To claim reimbursements for payments through cash and personal credit/debit card, Employees must submit the following documentation to the Corporate Finance department:
        - Relevant bills/receipts etc. for any reimbursements not covered in the daily allowance
        - Relevant bills/receipts for the payments made through cash or personal credit/debit card
            - In the case of card payments, if the above is not available, then the card statement may be submitted, highlighting the specific transactions

- Supporting documents specifying the exchange rate and amount converted into foreign currency

- In case of SVPs and above make payments with someone else's card, reasonable justification for this must be provided

Additional Guidelines for SVPs and Above

- These guidelines only apply to SVPs and above and are in addition to the recommendations and guidelines mentioned above
- SVPs are given a fixed travel budget during each review cycle and are expected to maintain traveling costs within the set budget range and only claim expenses against the pre-defined reimbursement heads, as mentioned below:
  - **Local Travel Allowances**
  - **Air Travel**
  - **Hotel Stay**
  - **Insurance**
  - **Airport Travel**
  - **Visa Charges**
  - **Telephone**
  - **Laundry**
  - **Daily Allowance:** No documentation will need to be submitted to claim these expenses and this amount is reimbursed basis of the number of days an Employee is traveling
  - **Medical Expenses:**
    - During travel for business purposes, all the medical related expenses (including COVID-19 related expenses) should be covered in the travel insurance policy, and anything over and above the insured amount such as additional stay, food, and travel will be reimbursed by the firm
    - Employees must submit the relevant medical bills in order to claim this reimbursement
    - Purchase of OTT medicines for mild symptoms is not reimbursed under this policy
- In case their expenses are exceeding the allocated budget during any review cycle, SVPs must seek prior approval from the Strategy department. Subsequent to receiving the approval, these claims are processed by the Corporate Finance department
  - SVPs may get these additional expenses approved and reimbursed in the same or the following month of incurring them
- Any additional luggage cost will have to be borne by the Employee themselves
- Additional expenses will be approved by the Strategy department, only in the multiples of £500, basis Employees having a valid reason for incurring them

Points to Note

- Employees are expected to exercise appropriate judgement when using the corporate card or submitting expenses for reimbursement
  - Employees can reach out to their Manager for further details before incurring any such expenses via corporate card
- Employees are expected to keep a track of their individual expenses on a real time basis. In case Employees foresee that their current expenses may exceed the pre-approved budget, they should immediately inform their Managers about the same and should seek approval to increase the budget
  - Such approvals will be subject to the nature of expenses which have been incurred and which are expected to be incurred in future
  - Any expenses incurred over the pre-approved budget without Manager's approval may not be considered for reimbursement
  - In case seeking Manager approval for exceeding the pre-approved budget is not feasible, employees should retain all documentation/proofs related to the incurred expense. Such documentation/proofs will be considered to decide whether these expenses can be reimbursed

3. Intra-City Work Reimbursements

The purpose of this policy is to define guidelines for reimbursing travel, business development, and client-related expenses incurred by Employees in their city of residence (i.e. London).

Eligibility

This policy is applicable to all Employees, considering that such travel is undertaken for lead generation/prospective client outreach.

Types of Reimbursements:

- Employees can reimburse conveyance, accommodation, and food expenses for travel undertaken by them as a part of lead generation, prospective client outreach, sales trip or any non-local events they attend for networking purposes
  - Allowance limits can be referred to under 'Annexure – Monetary Policies' of this Handbook
  - Other expenses such as local travel or taking a prospective client for coffee/lunch, will be reimbursed only if such activities are related to lead generation

- Expenses incurred by the employees as a part of their prospect outreach will be reimbursed as long as they are incurred as per the guidelines mentioned below:
  - **Conveyance:** Employees can reimburse travel expenses (Through any mode of transport such as Uber, LYFT, etc.). The documentation required to avail these reimbursements is as:
    - **Public Transport:** Receipts, wherever available
    - **Toll:** If the Employee uses a road toll, then any expense in relation to the usage of the toll must be entered as a separate conveyance entry on Microsoft Dynamics 365
  - **Food:**
    - **Lunch/Dinner Allowance:** Expenses are reimbursed on an actual basis
    - **Business Promotion:** Employees may reimburse any reasonable expense incurred while entertaining a client
  - **Client Welfare:** This includes any reimbursements related to gifts and promotions for clients, vendors, third parties, etc. The maximum amount that can be reimbursed under this header is £50, per client/per interaction. The limit may be increased basis Manager's approval
  - **Weekend:**
    - Employees are not allowed to reimburse expenses made on weekends unless they have Manager approvals. For example, in case the conference/meeting ended late on Friday night and Employees require an extra day for travelling, or if there are back-to-back sales trips which require Employees to stay over the weekend, etc.
    - The examples listed above are not exhaustive and it is expected that employees discuss such cases with their Manager before incurring any expenses over the weekend

Procedure to Claim Reimbursements

- All reimbursement payouts are subject to Manager approval
- When claiming reimbursements, Employees must be mindful of the following:
  - Reimbursement entries for food, conveyance should be added on Microsoft Dynamics 365 on or before the 5th working day of the following month from the date on which such expenses were incurred
- In case Employees are travelling to attend any event for lead generation or to meet a prospective client, the respective event/prospect name must be mentioned while reimbursing such expenses. Reimbursement requests will be rejected if such entries:
  - Are submitted by another employee on behalf of the one who incurred the expense
  - Have incorrect details/do not include any details such as name of the specific prospect/event, etc.
  - Are raised under the incorrect expense head on Microsoft Dynamics 365

- Entries must be approved by Managers within the defined monthly timeline. Unapproved expenses are not reimbursed, unless necessary approvals from the line-manager are shared in advance to extend the defined timeline
  - All reimbursement bills should have proper supporting invoices/documentation
  - All receipts should be shared in electronic format with the Corporate Finance department. No reimbursements are paid out without corresponding receipts despite being approved by the Manager
- Employees will be issued a Company credit card with a limit of £2,500 for their business expenses
  - The credit card bill will be paid for by the Company within the defined timeline however, Employees should submit the necessary documentation for the business expenses incurred by them on the card
  - Personal expenses incurred on the Company card will not be reimbursed and will be adjusted from the Employee's salary
  - Business expenses not incurred on the Company credit card can be reimbursed by submitting the necessary bills/invoices at accountsoverseas@tresvista.com on or before the 5th working day of the following month from the date on which such expenses were incurred
    - Requests raised by Employees beyond the defined timeline will not be considered and processed further by the Corporate Finance department unless Employees have approvals from their Managers to extend the deadline
- Client and project must be entered correctly (especially in case of cross-department work)

Points to Note

- Employees are expected to exercise appropriate judgement when using the corporate card or submitting expenses for reimbursement
  - Employees can reach out to their Manager for further details before incurring any such expenses via corporate card
- Employees are expected to keep a track of their individual expenses on a real time basis. In case Employees foresee that their current expenses may exceed the pre-approved budget, they should immediately inform their Managers about the same and should seek approval to increase the budget
  - Such approvals will be subject to the nature of expenses which have been incurred and which are expected to be incurred in future
  - Any expenses incurred over the pre-approved budget without Manager's approval may not be considered for reimbursement
  - In case seeking Manager approval for exceeding the pre-approved budget is not feasible, employees should retain all documentation/proofs related to the incurred expense. Such documentation/proofs will be considered to decide whether these expenses can be reimbursed

- Below mentioned documentation is not considered for monthly reimbursements:
  - Email copy with order confirmation details
  - Any modifications to a printed bill (E.g., adding/overwriting)
  - Cash/credit memo
- The responsibility of putting the entries on the system, getting them approved, and sharing the necessary receipts is on the Employee. No entries, approvals, and/or receipts are accepted after the defined reimbursement timeline determined by the Corporate Finance department
- Any reimbursement entries with incorrect details (e.g., wrong date or amount) are not reimbursed at the discretion of the Corporate Finance department
- Any expense incurred by Employees on the Company account (including but not limited to car service) and not submitted for reimbursements per the process defined above are treated as a personal expense and deducted from the Employee's salary
- Reimbursements are paid out with the salary per the timeline defined by the Corporate Finance department

4. Medical Insurance

Presently, TresVista provides an option to Employees to purchase medical insurance and claim reimbursement. Insurance reimbursement includes coverage for Employees only and does not include family members.

5. Compensation and Benefits

Employees will be entitled to an annual compensation as mentioned in their respective offer letters, inclusive of all allowances and benefits (Example: Phone Expenses), which shall be subject to deduction of taxes, as applicable and excludes any bonus which shall be paid at the sole discretion of the Company.

(D) Risk-Oriented Policies

1. Conflict of Interest – Firmwide Applicability

TresVista is committed to conducting business in a manner that ensures Employee's business judgment and decision making are not influenced by undue personal interests. Given the possibility of a conflict of interest (actual, potential, or perceived) in the context of the nature of services provided by TresVista to its Clients, TresVista requires all Employees to comply with Company guidelines and make all relevant disclosures to prevent any such conflicts of interest (actual, potential, or perceived).

Applicability

This policy is applicable to all Employees.

Particulars

Per the policy, conflict of interest situations include, but are not limited to:

- Owning more than 1% stake in a competing Company (private or public), sole proprietorship firm or partnership firm (registered or unregistered)
- Partnership or Directorship in a private or public firm:
  - Director or a Partner in any other firm
  - Power of Attorney of any other firm
  - Sleeping partner in a business run by another individual
- Multiple employment leading to monetary benefit:
  - Side business
  - Part-time employment
  - Weekend jobs
  - Monetary benefit from any employment apart from TresVista
- Freelance activities:
  - Freelancing, irrespective of the area of expertise, location, and timing
  - Working on a contract (temporary or renewal basis)
  - Giving lectures or teaching online or offline, irrespective of the topic (e.g., Alma Mater, CFA tutor, Finance tuitions, etc.)
  - Collaborating with institutions to give lectures
  - Providing professional consultation services to other firms

- Blogging to generate online traffic and/or marketing products online
- Referring a vendor Company in which an Employee has vested interest

- Other types of conflict:
  - Failing to disclose that the candidate, the Company is considering hiring is an immediate relative or spouse
  - Failing to disclose information pertaining to immediate relative or spouse working with a competitor
  - Engaging in business or working for a competitor
  - Working for an organisation that provides a competing product or service
  - Direct or indirect interest in any activity or business, resulting in monetary gain, whose nature of business is similar to TresVista

For the purpose of this policy, the term 'competitor' shall include any outsourced financial services provider or any organization whose nature of business is similar to that of TresVista, including but not limited to Financial Services, Data Intelligence, CFO Office Services.

Conflict Disclosure and Resolution Mechanism

1. Conflict of Interest (COI) Committee

- Shall assess and evaluate any conflict situation reported by Employees to avoid or minimize the risk associated with any conflict of interest (actual, potential, or perceived)
- Comprises of senior members of the firm who will review all reported conflicts of interest
- Is responsible for:
  - Identifying whether a conflict exists
  - Evaluating the severity of the conflict
  - Communicating to the Employee, the steps necessary to resolve the conflict

2. Procedure

- Employees are required to declare any conflict of interest (actual, potential, or perceived) situation to the COI Committee and seek the Committee's approval before entering into any situation that may be deemed as a conflict of interest
- The Committee shall proceed to make an enquiry into cases brought to its notice:
  - The COI Committee will review the case and communicate their decision to the concerned Employee within one month of the case being presented
  - In the interim, the concerned Employee shall refrain from participating or continuing with the conflicting arrangement
  - The Employee will need to implement the Committee's recommendation within two weeks of being communicated of the Committee's decision

- The COI Committee may ask the Employee to submit supporting documentation/evidence related to the conflict of interest at different stages of the review process in addition to seeking proof of the implementation of the corrective action recommended by the Committee
- The decisions and recommendations of the Committee shall be binding upon the Employee. Failure to abide by this may result in Termination (Refer to section 3.2 of this handbook, under the header of people policies)

3. Exceptions

- An event or any act of an Employee that does not jeopardize the primary interest of the Employee towards TresVista shall not be categorized as a Conflict of Interest
- However, all such cases must be reported to the COI Committee, who will review it and may deem it as an exception (subject to approval from the COI Committee). There are certain activities which may not be a potential conflict, including but not limited to:
  - Volunteering for a non-profit organization over the weekend
  - Serving on the Board of Directors of any Company with no conflict of interest in context of the nature of services provided by TresVista to its Clients
  - Conducting guest lectures on weekends without using TresVista's confidential and proprietary information

2. Conflict of Interest – Delivery Teams Applicability

The purpose of this policy is to establish relevant principles and rules for preventing or managing conflicts of interest in the Organization and to explain how such principles and rules are implemented.

Scope

This policy applies to all Employees of TresVista.

Particulars

- **Conflict of Interest:**
  - Conflict of interest would arise in the situation wherein a department/team has one or more Employees assisting clients:
    - Working together on the same deal
    - Competing against each other
    - Across the table (on either sides of a transaction)
- **Managing Conflict of Interest:** TresVista has implemented an organizational structure and several procedures to ensure that conflicts of interest are prevented and there is no or minimal material risk of damage to the interests of the clients.

- **Disclosure of Conflict of Interest:**
  - In the event of a conflict, it is the responsibility of the VP/EVP of that department/team to disclose them to the Compliance department immediately via an email
  - The Compliance department reserves the right to inform the client in all conflict situations once they receive this intimation from Employees

Material Non-Public Information (MNPI)

- The MNPI Policy has been defined to support and comply with laws governing:
  - Trade in securities while in possession of material non-public information about any Company or its subsidiaries, and
  - Disclosure of MNPI to outsiders ('tipping')
- A separate MNPI Policy is maintained, detailing the definitions and treatment of MNPI, which can be referred to in section 17 of this Handbook under the header of risk policies

Outside Business Activity

- Given the possibility of a conflict of interest in the context of the nature of services provided by TresVista to its clients, all the Employees are required to comply with laws in this regard and make all relevant disclosures to TresVista to avoid any conflict of interest
- Employees must disclose such conflicts of interests to the Conflict of Interest Committee, per the process defined in section 1.3 of this Handbook under the header of risk oriented policies

Employee Awareness

The Compliance department reiterates the policies annually to all Employees, as part of the induction process.

Compliance

- The Compliance department will carry out internal checks, and verifications as a part of the internal audit process. It will verify adherence to this policy through various methods, including but not limited to, random checks or any other means as deemed necessary
- Once the Compliance department receives intimation from the department/team about the receipt of information leading to material risk of damage to the client's interests, necessary steps as defined in this policy are taken

Non-Compliance

Any non-compliance with the policy attracts disciplinary action. Serious offenses such as theft of MNPI, illegal disclosure of sensitive data, etc., will be grounds for termination and may also involve legal consequences, at the discretion of the Company.

3. Code of Conduct

The purpose of this policy is to define standards and set guidelines concerning acceptable behaviour from Employees. The code of conduct is a commitment to conduct business ethically and helps the Company lay the foundation for core Company values and maintain high standards of behaviour and performance. By committing to the code of conduct, Employees are expected to support the Mission, Vision, and PACT of TresVista.

Overview

All Employees must conduct their personal affairs and manage their business transactions in a manner that does not result in adverse comments or criticism from the public, or in any way damage the Company's reputation as a responsible financial services organization. This policy addresses both business and social relationships, which may present legal and ethical concerns, and sets forth a code of conduct to guide Employees and provides an understanding of consequences and disciplinary actions if the conduct is violated/not adhered to. Sections of this policy have reference matters for which specific policies also exist, this is because the code of conduct encompasses standards of behavior outlined in other TresVista policies.

Applicability

This policy applies to all Employees of TresVista. Each Employee is expected to become familiar with TresVista policies that directly or indirectly impact their day-to-day operations/responsibilities and are required to affirm to have read and understood the code of conduct at the time of joining.

Particulars

- TresVista expects its Employees to fully comply with the spirit and intent of all applicable laws, rules, and regulations in accomplishing their assigned duties while using good judgment and ethical standards
- Compliance to the code of conduct is mandatory and all Employees are expected to comply with the policy when performing their duties
- Employees are expected to understand their obligations as per the guidelines defined in this policy
- Employees must promptly report any known or suspected violations of the Company's code of business conduct and ethics
- Adherence to the code is monitored through audit, examination, and human resource procedures

Fair Outcome and Conduct towards the Clients

- Serving clients is the focal point of TresVista's business and they deserve the highest quality service and standards in all transactions

- Employees must build and foster long-term relationships. This helps serve the clients better and improves and upholds the Company's reputation
- Employees should provide clients with valued services and deal with them fairly
- Employees must act with integrity and do everything possible to provide excellent service to them either directly or by supporting the work of other individuals
- Employees must not make any promises that cannot be fulfilled by them or the organization
- Employees must ensure that TresVista's services are:
  - Well-designed
  - Efficient
  - Transparent and based on useful advice
  - Performed as expected

Payment to Clients and Vendors

- Payments of any nature, which would violate any law, are not allowed by the organization
- All payments of fees must be per sound business practices
  - Payments, gifts, or favours must not be made to any person with the intent to induce them to violate their duties or to obtain favourable treatment for the Employee or TresVista

Disclosure to the Media

- Social Media and Social Media (Corporate Accounts) policies are supplementary and should be read in conjunction with this policy. The purpose of the social media policies is to ensure that Employees understand and comply with TresVista's disclosure requirements in terms of media interaction and public presentations. The detailed social media policies can be referred to under sections 5 and 6 of this Handbook, under the header of risk policies
- If Employees are delegated to speak on behalf of TresVista, they are briefed before being interviewed, to review what is public and private information
- Also, if asked for opinions from the media regarding any of their outside interests, Employees should know that their comments are strictly personal. They should be cautious not to compromise on the Mission and Vision of TresVista

Conduct when Representing TresVista

- Employees must conduct themselves professionally and with personal integrity, both in and out of the workplace, reflective of TresVista values
- Employee must communicate and negotiate honestly with all clients, partners, stakeholders, suppliers, associates, and other members of the public

- Obligation to act with integrity and within the spirit of this code of conduct continues while traveling, whether domestically or internationally
- It is recommended to avoid having alcoholic drinks while representing TresVista at social gatherings and parties
- Employees are expected to carry business cards, etc. as may be required to represent TresVista

Involvement in Out-of-Office Activities

- This clause helps Employees understand and comply with TresVista's code of conduct
- They must refrain from directly or indirectly expressing or using the Company's name while involving themselves or participating in or providing their views and opinions on sensitive matters, including but not limited to political, social, or any other comments on any platforms

Conduct in the Company

- Employees are expected to maintain high standards of professionalism as set by TresVista. TresVista aims at enhancing its reputation as a quality service provider and an enjoyable, stimulating, and challenging place to work
- It expects its Employees to achieve and maintain high standards of ethics, professional conduct, and work performance to ensure that TresVista maintains its reputation with all internal and external stakeholders
- High ethical standards must be recognized and valued. Any unethical or illegal behavior must be reported to the Ethics Committee
- An environment of honesty, trust and integrity must be maintained
- TresVista's property must be maintained and not be damaged intentionally
- In all dealings with third parties, the policies and directions of the Company must be complied with
- Any behavior or collective action which harms or could harm the integrity and/or interests of TresVista must be avoided
- Use of any Company Resources in connection with any illegal activity is strictly prohibited, and TresVista cooperates with any legitimate law enforcement investigation of potential criminal activity

Absenteeism and Tardiness

Employees must adhere to the work hours defined for them. They are expected to be punctual when reporting to work.

Equal Opportunity

- TresVista ensures to provide equal employment and advancement opportunities to individuals without distinction or discrimination because of age, colour, caste, national origin, race, religion or belief, gender reassignment, pregnancy and maternity, marriage and civil partnership status, sex, sexual orientation, or disability

- This clause applies to all Employees and candidates for employment and all aspects of the employment relationship, including recruitment, hiring, compensation, benefits, training, transfer, and any other terms and conditions of employment
- Refer to Diversity, Equity and Inclusion Policy and Anti-harassment and Bullying Policy under the header of people policies of the UK Addendum for further information and guidance

Professionalism

Employees must show integrity and professionalism in the workplace.

Personal Appearance

Employees must follow the dress code and personal appearance guidelines as mentioned in Section 1.5 of this Handbook, under the header of people policies.

Respect in the Workplace

- Employees should respect their colleagues and should maintain a safe and inclusive work environment free from discrimination, bullying, harassment, or exploitation of any form
- Employees must be open to communicate with their colleagues, seniors, or team members
- Employees should treat colleagues fairly and work together to deliver the brand promise
- Employees should be friendly and collaborative and should not disrupt the workplace or pose any obstacles to their colleagues' work
- Employees are expected to communicate in a professional manner while communicating within the office premises and during official duties outside the office premises

Communication with Former and Potential Employees

Employees may not disclose confidential information about the Company with former and/or potential Employees.

Legal and Social Responsibility

Employees must ensure that their actions comply with and are within the meaning and intent of all applicable laws and regulations. Employees' actions should be free from suspicion and criticism and have no adverse impact on society.

Sustainability and Environmental Protection

- TresVista continuously educates its Employees on environmental issues and stimulates individual and local initiatives
- TresVista strives to continually reduce environmental impact and endeavours to reduce energy consumption and waste etc.

- TresVista encourages Employees to use eco-friendly means of transport, and set environmental requirements when purchasing goods and services

Protection of Company Property

- Employees should treat TresVista's property, tangible or intangible, with respect and care
- Employees should not misuse TresVista's equipment or use it frivolously
- Employees should respect all kinds of intangible property, such as trademarks, copyrights, etc. and should use them only to complete their work responsibilities
- When exiting or retiring from TresVista, Employees must ensure that they return all Company property in their possession, including but not limited to records and equipment

Protection of Confidential Information

- Employees of TresVista should protect confidential information about the Company, clients, etc. received during the term of their employment
- For ensuring that confidential information is well protected, Employees should disclose information only on a "need-to-know" basis

Prohibition of Insider Trading

- TresVista restricts its Employees from trading in personal accounts using price-sensitive information of clients received during the term of their employment for personal gain/benefit
    - Details can be referred to under section 15 of this Handbook, under the header of risk policies

Frauds and Thefts

TresVista ensures that incidents of fraud and theft relating to the Company are promptly investigated, reported, and, where appropriate, prosecuted.

Anti-Bribery

- This clause helps Employees understand and adhere to the Company's ethical standards and comply with legal obligations
- It restricts Employees from directly or indirectly, offering, giving, requesting, or accepting any bribe from any clients, business associate, vendors, competitors, government officials or any other parties, thus observing and upholding TresVista's position on bribery and corruption
- Employees must ensure that they demonstrate high levels of integrity, act ethically, honestly, transparently and in a trustworthy manner in all their deals to protect the Company's and their own interests

Internet Usage: Cybersecurity, Social Media, and Corporate Email

- Employees must refrain from sharing information that is private or proprietary to TresVista
- Employees must avoid posting derogatory comments about clients, competitors, employer, or their practices on social media
    - For more information, kindly refer to the sections 5 and 6 of this Handbook, under the header of risk policies
- Employees must align themselves with the Company's Social Media and Social Media (Corporate Accounts) policies and plan before posting anything on social media platforms

Sexual Harassment

- TresVista does not tolerate sexual harassment, which may involve the solicitation of sexual favours or the initiation of any unwelcome sexual advance by one Employee towards another. It may also include other sexually related physical or verbal conduct. The creation of a work environment that is hostile, intimidating, or offensive to an individual or a group because of gender may also constitute sexual harassment
- Employees throughout TresVista should treat one another with courtesy, dignity, and respect, regardless of gender
- Employees must be alert to the possible presence of sexual harassment in the workplace. Appropriate steps must be taken to prevent sexual harassment. Complaints about sexual harassment can be made to Manager, Human Resources department, or the Internal Committee. Any charges should be promptly, reasonably, and thoroughly investigated. There is no retaliation for truthfully reporting sexual harassment or participating in the Company's investigation of a complaint
- If sexual harassment occurs, it leads to immediate disciplinary consequences ranging from a warning to termination with cause
    - For more information, refer to Section 1.8 of this Handbook, under the header of people policies. Additionally, refer to Diversity, Equity and Inclusion Policy and Anti-harassment and Bullying Policy under the header of people policies of the UK Addendum

Drugs, Alcohol and Smoking

- Employee must not distribute, possess or use illegal or unauthorized drugs or alcohol on the Company's property, time, in connection with the business or in a manner that might affect the performance of their responsibilities and duties to the Company
- No Employee is permitted to smoke at the workplace
- Employee whose behavior, judgment, or performance is impaired by drugs or alcohol should not report to work. Such Employees are prohibited from entering the Company's premises or engaging in Company business
- Violation of this clause is serious and results in the appropriate disciplinary actions, including dismissal

Workplace Violence

- Employees should have a safe place to work. Workplace violence, including threats, threatening behavior, harassment, intimidation, assaults, and similar conduct, is not tolerated
- Any threats or concerns about Employee's safety or the safety of others must be immediately reported to the respective Managers

Violation

In case of any violations (whether it is the code of conduct, TresVista policies or outside laws, rules, and regulations), TresVista does not hesitate to report to the relevant authorities. Additionally, the Employee, the Employee's Manager or any other person who was conscious of the breach is subject to the disciplinary action including but not limited to dismissal.

4. Code of Ethics

The purpose of this policy is to define a set of principles for Employees to ensure that their actions are in accordance with the ethical standards and primary values of the Company.

Overview

The Code of Ethics provides further clarity on TresVista's mission, values, and principles, linking them with professional conduct standards. It also articulates values that TresVista wishes to foster in Employees and, in doing so, defines desired behavior. Employees should adhere to the core ethical principles for guidance in decision-making and business conduct. Thus, the code of ethics becomes a benchmark against which individual and organizational performance can be measured. It establishes a direction and pathway to meet the organization's ethical responsibilities towards its stakeholders.

Competence

Employees must develop and maintain relevant knowledge, skills, and behavior to ensure that any activity is conducted professionally and proficiently. This includes but is not limited to acting with diligence, as well as obtaining, and regularly updating the appropriate qualifications, training, expertise, and practical experience. All Employees must understand and comply with any applicable laws, rules, regulations, and internal policies.

Integrity

During and after the term of their employment with TresVista, Employees must:

- Behave in an accountable and trustworthy manner
- Avoid any acts that might damage the reputation of the Company or bring discredit to the organization at any time
- Personally escalate noncompliance issues appropriately

- Exercise reasonable diligence when approving transactions and expenditures or signing documents
- Understand the importance of internal controls and consistently comply with them
- Not solicit or accept anything of value from anyone (directly or through others such as family members) if it is intended or could reasonably appear as intended to improperly influence the decisions to be taken on behalf of TresVista
- Neither indulge in the trade of the Company's stock for which they have access to confidential material and/or non-public information about a supplier, customer, or competitor nor should they advise others including connections to do so (definition of connections can be referred to in the Personal Account Dealing Policy)
- Act based on ethical behavior with an aim to build relationships on honesty and transparency
- Not engage in practices that distort prices or artificially inflate trading volume with the intent to mislead market participants

Reputational Damage to TresVista

If an Employee commits any act, which:

- Might tend to bring the Employee to public disrepute, contempt, scandal or ridicule
- May embarrass, offend, insult or denigrate individuals or groups
- May shock, insult or offend the community or the Company's workforce or public morals or decency or prejudice the Company
- Results in actual or threatened claims against the Company

TresVista has the right to look into such matters and take necessary actions in its sole discretion as it deems appropriate. These actions might include but are not limited to the immediate right to unilaterally terminate the employment agreement for cause; in such cases no prior notice of termination is provided, upon written notice to the Employee.

Fair Dealing, Diversity and Equal Opportunity

- TresVista condemns discrimination in any form and aims to provide a healthy and dignified work environment for all Employees
- Employees must treat all fellow Employees and third parties with respect and merit irrespective of their sex, age, sexual orientation, marital or civil partnership status, religion or belief, color, race, caste, nationality, gender reassignment status, whether they are pregnant or on maternity leave or any disability they may have. Harassment and bullying are considered as gross misconduct and are prohibited
- Employees must create a culture of fairness and transparency, which includes treating those with whom we have professional relationships with respect and ensuring that Employees consider the impact of their decisions and actions towards all stakeholders

- TresVista does not hire or terminate, reward or punish, or award or deny contracts based on personal considerations, including but not limited to favoritism, nepotism, or bribery

Confidentiality

During and after the term of their employment, Employees must:

- Hold in the strictest confidence and not use, divulge, or disclose, disseminate, publish, lecture upon, sell or transfer any confidential information to any person except as required by their employment and for the benefit of the Company
- Not permit any person to examine and/or make copies of, any documents, writings, drawings, materials or records, that contain or are derived from any confidential information received during the term of employment without the Company's prior written permission
    - Such confidential information is solely and absolutely vested in and owned by the Company, and the Employee does not have or claim any right, title, or interest therein
- Not divulge or disclose to any other Employee, the Employee's salary, or bonus arrangements with the Company
- Comply with, and do all things necessary to permit the Company to comply with all laws, and with the provisions of contracts executed by the Company relating to intellectual property or to the safeguarding of information, including the signing of any confidentiality agreements required in connection with the performance of their duties and functions
- Hold and use the confidential information which may be in the nature of 'inside information' or 'unpublished price sensitive information' as defined in the FCA Handbook and the UK Market Abuse Regulation (UK MAR) and the US SEBI's (Insider Trading) Regulations, 1992 and Securities Exchange Act, 1934 (as may be modified/amended/re-enacted from time to time), in the manner and in terms compliant with those regulations
    - Not pass along sensitive information or tip anyone to buy or sell securities whilst in possession of such information of such securities
- Upon termination of employment for whatever reason, deliver to the Company all working papers and/or other material and copies provided to the Employee pursuant to their employment or prepared by the Employee during the term of their employment, without retaining any copies
- Follow the highest standards of information security to keep any client information confidential in order to protect the confidentiality and sensitivity of the information provided by them
- Ascertain that any data shared by the clients is used for intended purposes only and any sensitive information is not divulged to anyone, including third parties, without the explicit consent of those involved – unless disclosure is required by law or regulation

- Believe that all information about the Company and its business (including the past, present and prospective clients, business partners, vendors, directors, and Employees) is confidential unless otherwise stated
- Not share user IDs, passwords, access details, software, or authentication devices that are intended for individual use to gain access to a system
- Respect the Company's security controls and access information only within their authorized access level
- Not discuss the clients in public to prevent unauthorized people (outside the team) from gaining access to this information
- Not share any data or information within or outside TresVista unless express consent is received from the respective Manager or other authorized Employee
- Confirm that all the files are precisely stored, deleted or destroyed as directed by the Manager or other authorized Employee and as mandated by the contract
- Not cause any unauthorized disclosure of any material, through any failure to exercise due care and diligence
- Not reproduce, store in a retrieval system or transmit in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, any copyrighted material which is the property of the Company, for their own benefit or for the benefit of any third party, that contain or are derived from any Confidential Information received during the term of their employment
- Not at any time during the continuance of their employment or on expiry or termination or cessation of employment with the Company, issue any unauthorized statements to the press or any third party regarding the Company, the Company's business, this Agreement and their employment with the Company
- Not have or claim any right, title or interest therein since Confidential Information shall be deemed as the Company's trade secrets and solely and absolutely vested in and owned by the Company

Obligations under this section continue after the termination of employment, without any restrictions regarding time (i.e., indefinitely) and are binding upon the Employee's heirs, assigns, executors, administrators and other legal representatives. Employee's obligations under any such additional confidentiality agreements shall supplement and not override the other provisions of this policy unless otherwise expressly stated otherwise. The obligations under this section do not apply:

- To information which is or comes in the public domain other than through the Employee's unauthorized disclosure
- To the extent that such information is required to be disclosed by any law or any applicable regulatory requirements or by any regulatory body to whose jurisdiction the Company is subject or with whose instructions it is customary to comply under notice to the Company
- In such cases, the Employee must immediately notify the Company and cooperate as reasonably requested by the Company in its attempt to prevent or limit such disclosure

- To prevent the Employees from using their own personal skill in any business in which they may lawfully be engaged after the termination of their employment, provided such employment is in compliance with Employee Separation Procedure provided in the Handbook (Refer to section 3.3 of this handbook, under the header of people policies)

Communication

During and after the term of their employment, Employees must:

- Use electronic technology maintained by the TresVista responsibly and professionally
- Foster open lines of communication amongst team members
- Ensure client communication is complete, accurate, professional, and consistent with the Employee's stated duties to clients
    - It is essential to proofread all emails prior to sending and use a business email address with proper signature (Refer to section 1.12 of this handbook, under the header of people policies)
- Avoid phrasal verbs, contractions, colloquial, and textspeak in any written communication, whether internal or external
- Disclose to clients and prospective clients the basic format and general principles of the processes used at TresVista and promptly communicate any changes that might materially affect those processes. It is essential that Employees use reasonable judgment in identifying factors that are essential to servicing clients and include these factors in communication to both current and prospective clients
- Refrain from exaggerating or using inaccurate statements that could be easily misunderstood or used against TresVista in legal proceedings

Commitment to Quality

- TresVista aims and ensures to deliver unmatched quality to its clients by helping every Employee embrace the ethos of utmost diligence and establish multiple levels of quality checks and instant investigation and correction of any deviations
- TresVista only recommends services/solutions that it believes is a proper fit for each client's needs
- Employees must make reasonable inquiries into a current or a prospective client's requirements, industry practices, business requirements, and constraints, if any, and strive to reassess and update this information regularly
- Employees must ensure that any completed product is suitable and consistent to the client's written objectives, and mandates, specified orally, via emails or in line with the terms of the signed agreement
- It is imperative for Employees, to be honest and upfront in advertising and marketing claims to avoid misrepresentation, exaggeration, ambiguity and reduce complexity and excel at execution

Ownership

During and after the term of their employment, Employees must:

- Act with reasonable care and exercise prudent judgment
- Accept responsibility for any decisions or actions that may impact the Company's interests or stakeholders
- Act for the benefit of clients and place the client's interests before the Company's or the Employee's personal interests
- Ascertain accuracy and completeness in the delivery of the Company's services
- Display consistency between speech and actions
- Commit to have zero tolerance for both internal and external fraud
- Report potential or suspected violations of the law or TresVista policies including, situations when they know or suspect that other Employees are currently or potentially engaging in illegal, or unethical activities

Partnership

During and after the term of their employment, Employees must:

- Work with others to develop solutions and break down internal barriers
- Assume positive intent in working with others, value and encourage diversity
- Share ideas and resources across the organization for scale and impact
- Manage resources rather than owning them
- Build effective relationships with colleagues and industry partners to enable others to be successful
- Discuss the importance of ethics and compliance regularly with all team members
- Deliver and seek timely and actionable feedback
- Foster fair competition between any potential suppliers and encourage suppliers to comply with the sound business practices TresVista embraces, follow the law, and conduct activities in a manner that respects human rights
- Build a positive working environment, along with the responsibility to speak out and ask for a change if any conduct that runs contrary to this principle is observed

Health and Safety at the Workplace

Employees must be cautious and do nothing that might endanger or harm TresVista's business associates in any way – whether they are fellow Employees, vendors, visitors, etc. Employees are expected to keep the workplaces safe by following the health and safety norms, ensuring a safe, dignified, and productive work environment.

Objectivity and Independence

Employee should work at TresVista in a professional manner with objectivity, independence of mind and appearance. Employees must impose an obligation on their fellow Employees to not compromise their professional or business judgment because of bias, conflict of interest, or any undue influence of others.

Fairness, Care, and Respect Towards Employees

Employees must treat fellow Employees & third parties in TresVista, with fairness, care, and respect and make all decisions in complete fairness and free from competing self-interest and prejudice.

Human Relationships

Employees must ensure that relationships with fellow Employees & Third parties are based on trust, integrity, and respect. They must avoid aggression (physical or verbal) or any related act against personal dignity.

Good Environment Practices

- TresVista pledges to minimize wastage of energy, water, and other resources, prevent discharge that would harm the environment, and recycle wherever possible
- TresVista strives to ensure and demonstrate continuous improvement in preserving the environment
- Employees must ensure to switch-off lights, computers, printers, and other electronic devices when not in use and/or at the end of the workday and avoid unnecessary printing of documents
- Employees must make a judicious use of air-conditioning and heating devices and switch-off devices when not in use

Additional Compensation Arrangements

- Employees should not accept gifts, benefits, compensation, or consideration in any form from the clients, vendors, consultant, service provider, and any outside agency or other parties who have a business relationship with TresVista without following the approval matrix prescribed in the Gifts Policy
- Employees should not accept any remuneration, salary, fee, perquisites, or other compensation in any form from any person, or entity for working as part-time, assignment, contractual basis or otherwise

Loyalty, Prudence, and Care

- Employees must not use resources, including time, material, equipment, and information provided by TresVista for personal use or to create, access, store, print, solicit or send any materials that are harassing, threatening, abusive, sexually explicit, or otherwise offensive or inappropriate

- Employees must not use any equipment of TresVista such as computers, copiers, and fax machines in the conduct of an outside business or support of any religious, political, or other daily activity, except for Company-requested support to non-profit organizations
- Employees who represent TresVista must behave responsibly and use good judgment to conserve resources

Upholding the Code

- The Board of Directors (Board) and Management of the Company are committed to the maintenance of high standards of ethics, honesty, and integrity, and promoting a corporate culture that adheres to these values
- TresVista does not accept any justification or excuse for breaking the code, whatever the reason – whether for profit, convenience, competitive advantage, or request/demand from any third-party or individual

Fraud, Whistleblower and Raising Concerns

- TresVista through its work ethics is committed to the highest standards of moral and ethical behaviour and has a zero tolerance for both internal and external fraud or any other activity detrimental to the TresVista's mission and values.
- Each Employee at TresVista is its ambassador and expected to uphold the principles of honesty and integrity, on which TresVista is built. With a view to ensure ethical behaviour; TresVista considers it appropriate to provide a channel to its Employees and stakeholders to speak up when they see behavior inconsistent with its values and bring to the notice of the Compliance department any event of concern that may warrant necessary disciplinary action (E.g., an Employee raising a concern regarding the dishonesty of a superior/an Employee from the top Management)
- Through this clause, TresVista is committed to support and enforce the Fraud and Whistleblower Policy, which aids in the detection and prevention of such activity. This clause also ensures honest, open and well-intentioned working environment where people are confident to raise their concerns without fear of reprisal, retaliation, discrimination or any kind of harassment
- Any concerns involving unethical behavior should be reported via email to the Ethics Committee at coe@tresvista.com

Ethics Committee

- The Ethics Committee has been designated to deal with grievances, and unethical issues arising in the organization and Employee's acts within and outside their employment at TresVista, which might damage the Company's reputation or adversely impact client and vendor relations
- The Committee offers assistance in addressing and giving solutions to the issues mentioned above with the intention of establishing fairness in the organization

1. **Definition**

   Cases under the purview of the Ethics Committee include, but are not limited to:

   - Violation of the code of ethics or code of conduct

- Unauthorized consumption of alcohol in the office premises
- Misuse of the Company's resources
- Theft/embezzlement in and/or around the office premises
- Misappropriation or misrepresentation of Company funds
- Misconduct by another Employee
  - Engaging in physical or verbal abuse with other Employees
  - Bullying or playing pranks on another Employee
- Discrimination based on age, disability, gender reassignment, marriage and civil partnership status, pregnancy and maternity, race, caste, religion and belief, sex and sexual orientation
- Damage caused to TresVista's property
- Undue influence/nepotism
- Cheating/malpractices while completing training assignments
- Issues with Manager/superior
  - Inappropriate or unethical conduct
- Violation of Company policies and procedures
- Working conditions
  - Concerns regarding infrastructure
  - Workplace hygiene
  - Workplace decorum
- Any act which might bring the Employee to public ignominy, offends other Employees or public ethics or pose a risk to the Company's reputation

2. Scope

- This clause applies to all Employees of TresVista
- For this clause:
  - "Complainee" refers to an Employee who is complained about, a subject of the complaint
  - "Complainant" refers to a person who files a complaint

3. Points to Note

- All Employees of TresVista must report any grievances, unethical issue/s, violation of code of ethics or code of conduct experienced by them, or brought to their knowledge or witnessed any act that might damage the Company's reputation to the Ethics Committee

- Confidentiality of information of a complaint against unethical issues/grievances or any inappropriate act of Employee (including name of the complainee, details of the complaint and all related matters) must be maintained at all times

4. **Committee Formation**
   - Inquiry into complaints against unethical issues and grievances is undertaken by an Ethics Committee ("EC") at TresVista
   - The Committee comprises of senior members of the firm who review all reported cases
   - EC should be reconstituted per the tenure defined by the organization
5. **Stages of Redressal Mechanism**
   - Employees should follow standard guidelines before lodging a complaint. At times complaints can be a way of negative feedback, which may not require a resolution or formal follow-up
   - The complainant may choose to express their concern to the respective Manager/head of Employee's department or write to the EC directly
6. **Complaint Making**
   - A written complaint to the EC with a detailed record of the incident(s) (such as date, time, locations, details of the incident, etc.) is mandatory for initiating an inquiry into the matter
   - The complaint can be raised by sending an email to coe@tresvista.com
   - The EC does not investigate against anyone based on verbal complaints
7. **Malicious or False Complaints and False Evidence**
   - A person making a false complaint or providing false evidence in an inquiry is subject to disciplinary action
   - A mere inability to substantiate a complaint, or provide adequate proof, does not lead to the complaint being considered as false or malicious
8. **Inquiry Process**
   - The EC follows the inquiry process as laid out in the guiding principles of the Ethics Committee
   - The EC hears both, alleged complainee and complainant to record their statements
   - Both parties may submit evidence and a list of witnesses supporting their statements, to the EC

   Upon receiving any concerns regarding unethical issues/grievances, the EC convenes a meeting to deal with the complaint and makes a preliminary inquiry to verify the facts for the complaint within a time frame of two (2) to five (5) working days from the time of the receipt of the written complaint.
9. **Post Inquiry**
   - If the allegations against the complainee have not been proved, the EC does not take any action in the matter

- If the allegations have been proved, the EC takes appropriate action against the complainee based on the disciplinary actions under this clause, and the decision of the Committee is binding and final

10. Reports and Documents

- Investigation results are not disclosed or discussed with anyone other than those who have a legitimate need to know. This is important in order to avoid damaging the reputation of the complainee subsequently found innocent of wrongful conduct and to protect the Company from potential civil liability
- All disclosures made by the Ethics Committee, reports and documents obtained during the course of any investigation, along with the results of the investigation relating to it, are retained by TresVista for a minimum period of four (4) years
- EC submits a summary of the reported concerns, if any, on a quarterly basis to the HR Compensation and Benefits 2 team (compensation2@tresvista.com) and the Management, highlighting the following:
  - Nature of reported cases and the proposed action
  - Status of cases reported in the current/prior period and the action taken
  - Results/status of any investigations/enquiries with reference to the cases reported

Disciplinary Procedures

- In case of any violations (whether it is the Code of Ethics, Code of Conduct, TresVista policies, or outside laws, rules, and regulations), TresVista does not hesitate to report it to the relevant authorities
- The Employee, their Manager and any other person who was conscious of the breach and did not report it is subject to the following disciplinary actions, including but not limited to:
  - Reconciliation/resolution of the issue through conversation
  - Rendering a written apology
  - Warning letter
  - Withholding promotion
  - Reduction of performance rating
  - Termination with cause in keeping with section 3.3 of this Handbook, under the header of people policies
- Please see our Disciplinary and Capability Procedure and Rules in the UK Employee Addendum for further information and guidance

Affirmation Process

Employees must declare that they have read and affirm their awareness of the Code as part of the annual affirmation process.

Legal Notice

- This Code serves as a reference to Employees. TresVista reserves the right to modify, suspend or revoke this Code and any policies, procedures, and programs in whole or in part, at any time, with or without notice. TresVista also reserves the right to interpret this Code and these policies in its sole discretion as it deems appropriate
- Neither this Code nor any statements made by any Employee of TresVista, whether oral or written, confer any rights, privileges or benefits on any Employee, create an entitlement to continued employment at TresVista, establish conditions of employment, or create an express or implied employment contract of any kind between Employees and TresVista. Employees should also understand that this Code does not modify their employment relationship and does not form part of their contract of employment

5. Social Media

The purpose of this policy is to define guidelines and best practices for Employees concerning the usage of social media.

Overview

While technology enables easy exchange of information, there is also a threat of information leaks, clients forming unwarranted opinions about certain Employees or any other consequences which may have an undesirable impact on the Company's reputation.

Scope

Social media includes but is not limited to:

- Social networking websites (e.g., Facebook, LinkedIn)
- Video and photo sharing websites (e.g., Flickr, YouTube)
- Blogs (not including TresVista blogs)
- Micro-blogging (e.g., Twitter)
- Wikis and online collaborations (e.g., Wikipedia)
- Forums, discussion boards, chat rooms and groups (e.g., Google groups)
- Video on Demand (VOD) and podcasting
- Status updates on messenger services (e.g., WhatsApp, Telegram, Facebook Messenger, or any other instant messaging application)
- Geospatial tagging (e.g., Foursquare)
- Interviews, columns or talk shows (e.g., Television, print media or radio)

Applicability

This policy is applicable to all Employees.

Particulars

- Employees are not permitted to:
  - Use TresVista's name and refer or state that they are working at TresVista across any social media platforms
    - If the Employees wish to update their social media account with details of their current role, they may mention the name of the employer as 'Financial Services Firm'
  - Post any information about TresVista, its internal processes, or any other information which is not publicly available
    - Disclose or publish any information that is confidential or proprietary to TresVista, including but not limited to specific details on projects and clients
    - Generic references are acceptable (e.g., working with a Middle Eastern PE firm), however, Employees should be vigilant that no further details are mentioned (e.g., working with the biggest Middle Eastern Non-Sovereign PE firm)
    - Queries regarding what is considered proprietary and confidential can be discussed with Marketing and Corporate Communications and/or Compliance departments
  - Expressly state or imply that they are authorized to speak as a representative of TresVista or give the impression that the views expressed by them are those of the organization
  - Use their official email address or TresVista logo on social media platform, in case it gives the impression that the organization supports or endorses their personal comments
  - Post commentary, content, or images on social media that are defamatory, pornographic, proprietary, harassing, libelous, bullying, discriminatory towards another Employee or that can create a hostile work environment
  - Post anything that may lead to potential infringement of intellectual property rights, including but not limited to, brand names, trade names, logos, copyrights, or trade secrets of TresVista or any of its clients
  - Post or publish any information that could be in contravention of a law, statute, or regulation applicable in their jurisdiction as well as in the jurisdiction of the third party referred to in any such publication
    - Engaging in prohibited or unlawful conduct will not be tolerated and the Employee may be subject to disciplinary action
  - Tag the Company's official account in any of the posts or comments

- Employees must refrain from engaging in inappropriate posts, including but not limited to threats of violence, discriminatory content such as racial, ethnic, sexual, religious, physical disability slurs, etc.
- Employees should be aware that the Company may observe content and information made available by them on social media platforms
- Employees must refrain from publishing or engaging in rumors that can have a significantly adverse impact on the Company's reputation
- Employees should use their best judgment in posting content that is neither inappropriate nor harmful to the organization, other Employees, or clients
- TresVista reserves the right to request the withdrawal of any posts, comments, or content from any social media platform (including internal platforms). Employees must be aware that some forms of internet conduct may be open to criminal prosecution and lead to disciplinary action

Points to Note:

- Any queries from social media networks, blogs and other types of online content that may generate press, media attention, and/or legal questions must be redirected to Marketing and Corporate Communications department
- Marketing and Corporate Communications department will conduct monthly audits to ensure adherence to this policy
- Non-compliance with the policy, in any form, shall lead to disciplinary actions including, but not limited to policy reminders, warning letter, or dismissal, at the discretion of the Company

6. Social Media (Corporate Accounts)

The purpose of this policy is to define guidelines for usage of corporate social media accounts on networking sites including but not limited to professional websites such as LinkedIn, for business purposes as required by TresVista.

Scope

This policy applies to Employees who are designated and eligible to use specific social media platforms for business purposes, per Company requirements, and the roles and responsibilities defined in their Employment Agreement.

Particulars

- **Corporate Accounts:**
  - Employees should be mindful that corporate accounts are only used for business purposes, and in accordance with the directions and guidelines defined by the organization

- Corporate accounts include, without any limitation, all log-in information (including passwords) and content related to the account and TresVista has exclusive proprietary rights to the data, including contacts, conversations, and any other related material contained or collected in/from these accounts
  - All corporate accounts are owned by TresVista, and the organization has the right to control them, irrespective of whether the account is being used, managed, or accessed by any Employee
  - The Company can access these corporate accounts at its discretion, unless otherwise limited by the applicable laws
- Upon termination of employment, Employees having access to these corporate accounts are required to cease using them on immediate basis
- In case of any change in the credentials of the corporate account during their tenure, Employees are required to keep the organization informed of these changes
- **For Senior Vice Presidents and Above in Client Development:**
  - SVPs and above in the Client Development department will be given the option to transfer their LinkedIn account (each, an "account") into a premium corporate account via the Inside Sales department
  - Those who opt for this transfer will be required to share their credentials with the IT department so the necessary premium licenses can be purchased
    - Once opted in, Employees will not have an option of opting out of this setup
  - Further to this transfer, Employees will need to sign an amendment to their Employment Agreement, to this effect
  - At the time of exit, (s), the account(s) shall be retained by TresVista or returned to the Employee at sole discretion of the Company
    - In case the account is retained by TresVista, the Inside Sales Department will coordinate with the IT department to modify the credentials of the account and make it inaccessible to the Employee, as part of the Employee's exit checklist
    - Corporate Finance department Discontinues the premium license as per the billing cycle and license terms
  - Employees are not permitted to engage with any prospects, referrals, clients, ex-clients, potential prospects, or third parties connected to or shortlisted by TresVista for business opportunities, after their termination of employment

- **Personal Accounts**
  - Employees using personal accounts are not permitted to engage in any conversation with TresVista's potential prospects, current clients, or third parties through any social media platform

- Employees are only allowed to communicate with them through MS Outlook and MS Teams for conversations concerning business operations

- Employees are not permitted to send a request to any potential prospects, current clients, or third parties on social media platforms unless they receive instructions from the organization or the potential prospects, current clients, or third parties, to do so
- Employees who have connected with potential prospects, current clients, or third parties on social media platforms cannot post any status update that may prove detrimental to TresVista's interest. For instance, Employees are not allowed to post status updates like "Open to work", "Looking for better opportunities", etc. on any social media or professional networking platform including but not limited to LinkedIn
  - In case of violation of this restriction, it would be termed as a material breach of the employment terms and shall be a ground for disciplinary action up to and including dismissal
- Due to any overlapping situation, where an ex-Employee is introduced to potential prospects, current clients or third parties by any other party or such potentials reach out to an ex-Employee directly, the ex-Employee is required to take pre-clearance from TresVista
- Employees are not permitted to use TresVista's name and refer or state that they are working at TresVista across any social media platforms
  - If the Employees wish to update their social media account with details of their current role, they may mention the name of the employer as 'Financial Services Firm'
- Employees are not allowed to expressly state or imply that they are authorized to speak as a representative of TresVista or give the impression that the views expressed by them are those of the organization
- Employees are not permitted use their official email address or TresVista logo on social media platform, in case it gives the impression that the organization supports or endorses their personal comments
- In any given scenario, Employees are required to adhere to the guidelines laid down in the social media policy and maintain high standard of ethical and professional conduct, and performance while interacting with any clients or third party on behalf of TresVista
- Any behavior or collective action which harms or could harm the integrity and/or interests of TresVista must be avoided. Any unethical or illegal behavior will be reported to the Ethics Committee and will be considered as a breach of the employment terms and the Employee will be liable for disciplinary actions, at the discretion of the Company
- During the term of employment and thereafter, the Employee shall not circumvent TresVista, take no actions to the detriment of TresVista and refrain from communicating or conducting business, in whatsoever manner, with

TresVista's prospects, clients, or contacts, either directly or through other representatives, without prior written consent from the organization

- The Employee declares to have read and understood the content mentioned hereinabove and agrees to abide by the terms. In the event of any breach of any of the covenants set forth hereinabove, TresVista shall reserve its rights to initiate appropriate actions against the Employee

7. Approval Matrix

The purpose of this policy is to establish guidelines concerning approvals in the Company.

Procedure

- Approvals must always be received in the form of a written statement from the required/designated approving authority(ies)
- This policy defines the approval workflows that need to be initiated at the initial or operation stage of specific requests, as applicable
- The approval mechanism or hierarchy to be followed, as applicable, is defined below:

Employee Designated	Approving Authority
Analyst/Sr. Analyst/Associate	Sr. Associate
Sr. Associate	VP/EVP
VP/EVP	SVP
SVP	Management Committee

8. Internet Policy

This policy governs the use of internet by all users in TresVista that are in scope of Information Security Management System (ISMS).

Particulars

- TresVista recognizes the business need for providing internet access to its Employees and it is not to be treated as a basic facility, privilege or right of an Employee
- Employees are eligible to use internet services based on their role and prior approval from their respective Heads of Department/Manager
- Formal guidelines are established in order to control and regulate the use of internet in the organization

- TresVista specifically prohibits Employees from accessing the following type of sites and messenger tools on Company devices:
  - Gambling sites
  - Auction sites
  - Hate sites
  - Pornographic sites
  - Any site engaging in or encouraging illegal activity
  - Hacking sites
  - Social Networking sites (e.g., Orkut, Matrimonial Sites)
  - Messenger tools (e.g., Yahoo Messenger, MSN Messenger, Google Talk)
  - Online shopping sites
  - OTT and entertainment sites
- Access to the internet should not be used for:
  - Viewing, storing, and transmitting indecent, obscene, offensive, sexually explicit materials
  - Upload/download commercial software in violation of its copyright
  - Unauthorized access to remote systems
  - Attempt to hack internal and external networks
  - Crack passwords of other logins
- All communication to and from the internet is enabled through a firewall to protect the network from being affected by malicious code attack
- Employees must only connect via secured internet sources and avoid connecting to public internet sources (i.e., airport Wi-Fi, lounge Wi-Fi, etc.)
- Remote access to LAN must only be done through secure authentication
- Inbound traffic is checked for malicious code attacks at gateway level
- Users must comply with the Email Policy of the organization
- All illegal sites and downloads are to be identified and blocked on proxy servers on regular basis
- IT department monitors the internet activity and reports actual and potential security incidents or non-compliance of the policy to the Incident Management Response Team
- Logs of proxy are maintained to reflect user/IP, time of request, request link and files downloaded
- Logs are analysed on a fortnightly basis for forbidden sites and the IT department sends a report to the Head of the Department

- Any breach in this policy results in disciplinary action being taken against the Employee. The disciplinary action may range from warning letter to termination with cause, at the discretion of the organization

9. Gift Policy

The purpose of this policy is to define guidelines in order to restrict Employees from directly or indirectly, offering, giving, requesting, accepting any bribe (i.e., gifts with mala-fide intentions, loan, payment, reward or advantage, either in cash or any other form of inducement) from clients, business associates, vendors or competitors thus observing and upholding TresVista's position on bribery and corruption.

Applicability

This policy applies to all Employees of TresVista. Further it also applies to any stakeholder, client, consultant, vendor, service provider, external agency or any other parties who have a business relationship with TresVista.

Policy

- Employee must not directly or indirectly solicit or accept cash/cash equivalents or any other gift from any stakeholder, client, consultant, vendor, service provider, external agency or any other parties who have a business relationship with TresVista or give any sort of gift to a client without following the defined approval matrix Employee
- Employees are not allowed to accept any gifts or give any gift from/to competitors
- It is prohibited, directly or indirectly, for any Employee to offer, give, request or accept any bribe (i.e. gifts with mala-fide intentions, loan, payment, reward or advantage, either in cash or any other form of inducement), to or from any person or Company in order to gain commercial, contractual or regulatory advantage for TresVista, or in order to gain any personal advantage for an individual or anyone connected with the individual in a way that is unethical
- Employees on behalf of TresVista should:
  - Not offer, promise, or make any bribe or unauthorized payment or inducement of any kind to anyone
  - Not solicit business by offering, promising, or making any bribe or unofficial payment to suppliers
  - Not request or accept any kind of bribe or unusual payment or inducement that would not be authorized by TresVista in the ordinary course of business
  - Refuse any bribe or unusual payment and to do so in a manner that is not open to misunderstanding or giving rise to false expectation; and to report any such offers
  - Not make facilitation payments. These are payments used by businesses or individuals to secure or expedite the performance of a routine or necessary action to which the payer of the facilitation payment has a legal or other entitlement
  - Report any breaches of this policy to the Compliance department

Approval Matrix

- Employees need to take necessary approvals for accepting/giving any gifts from/to clients, business associates, and vendor, as per the below defined approval matrix

Amount	Approval (Via Helpdesk)	Authority
Up to £150	Intimation	Line Manager (VP/EVP) Compliance department
Up to £250	Prior approval	Line Manager (Head of Department) Compliance department
£250 and above	Prior approval	Management Compliance department

- For FMS support staff, line Managers must inform/seek approval on behalf of Employees
- Compliance department reserves the right to ask Employees to return the received gifts
- Post receiving approvals, all Employees should intimate the Inside Sales department (insidesales@tresvista.com) when they receive from or give a gift to a client
- Gifts may include (but are not limited to) compensatory favours (team dinner, donations, comp-offs), vouchers, souvenir, event passes, etc.
- This process should be followed for the purpose of tracking favours between TresVista and its clients

Employee Awareness

At TresVista, training is provided to all new Employees as a part of the induction processCompany.

Compliance

- The Compliance department verifies adherence to this policy through various methods, including but not limited to, walk-throughs, and internal audits conducted monthly
- The department will verify cost of the gifts and adherence to the above approval matrix

Non-Compliance

Any non-compliance with the aforementioned policy shall attract disciplinary actions as per the ‘Annexure A’ of this handbook.

10. IT Security Policy

The purpose of this policy is to prevent unauthorized access, ensure the safety and security of TresVista networks, and to protect and to avoid misuse of client data and other confidential information.

Applicability

This policy applies to all Employees of TresVista except EmployeeFMS support staff.

Particulars

TresVista has adopted access control policies as defined below:

- **Data Access Control:**
  - Access to each data store is restricted, and the data owner determines access provision and retention requirements
  - IT administrators manage and monitor the data stored on the centralized servers/storage
  - Regular backups are done to ensure the safety and availability of data
  - Antivirus protection software is installed on the endpoints to ensure that the data is protected from virus and malware threats
  - Access to all portable media/storage devices is disabled
  - Data leak prevention (DLP) controls are implemented across all systems to prevent data leakage
  - Employees' access to Company data is limited based on Employee profiles as defined by IT department and the access is automatically enforced
- **Network Access Control:**
  - Unique Employee IDs and passwords should be used for every Employee to maintain individual accountability of internet, intranet, and e-mail resource usage (Details can be referred to user ID and password below)
  - Access to the network is provided to Employees for the purpose of business operations and made available only from the Employee's Company device with a unique Employee ID
  - The provided access does not allow copying of the text or files on any external devices (such as pen drives, USBs, CDs, etc.)
  - TresVista has installed a variety of firewalls, proxies, internet address screening programs, and other security systems to prevent unauthorized access and spam and to ensure the safety and security of TresVista networks
  - Access to the restricted website, domains and email IDs is provided to Employees for research purposes subject to them following the whitelisting process, and basis approval from the Head of Department and the Compliance department (Details can be referred to in the whitelisting process clause mentioned below)

- Systems and configurations are strictly monitored and accessed by the Compliance team and IT administrators only

- **Systems/Information Access Control:**
  - The appropriate level of access to systems and information is determined upon the business need, job functions and role. The respective VPs/EVPs (of delivery teams) and SVPs (of non-delivery teams), define the access rights for specific roles, basis which access of information is provided
  - For systems containing restricted or personal information, an access control matrix has been developed to record accesses across different roles and departments. The access matrix is updated and maintained regularly to reflect accurate records of access
  - Access to specific systems and information is granted to Employees according to the whitelisting process. If approval is granted to use these systems and information, the Employee is required to login using the unique Employee ID and password
  - Generic logins are not permitted across TresVista, unless for exceptional circumstances with appropriate monitoring controls
- **User Registration/De-registration Control:**
  - When an Employee joins TresVista, the IT administrator on receipt of information from the HR Operations team (ops@tresvista.com), shares with the respective VPs/EVPs (of delivery teams) and SVPs (of non-delivery teams) or equivalent an access rights checklist based on which the IT administrator creates login IDs and provides assigned access to the Employee's system
  - If the VPs/EVPs/SVPs or equivalent deems it unfit or inappropriate for an Employee to have access to systems and/or information then, the same is communicated immediately to the IT administrator who accordingly alters/ removes such access rights. The access matrix is updated to accurately reflect access records
  - If an Employee is on leave for more than one (1) month, the respective VPs/EVPs/SVPs or equivalent informs the IT administrator to alter/remove the Employee's access rights. Such changes are reflected in the access matrix to accurately reflect access records
  - On resignation/termination of an Employee, the IT administrator backs up the necessary user data which is to be archived and disables the login ID of such Employees
- **Privileged Account Access Control:**
  - Privileged accounts (as compared to regular user account) are system or application accounts that have advanced permissions. Examples of user accounts with privileges include IT administrators, IT Managers, SVPs, and Management

- Privileged rights are given to any other user on request after obtaining the necessary approvals and such privileged access rights are reviewed by the IT administrator on a monthly basis
- Request for termination of such access rights is communicated to the IT administrator through the Helpdesk a day in advance. Moreover, IT administrator also pro-actively checks with the Employees for continuation/ termination of privileged rights during the quarterly review

- **E-mail and Messaging Control:**
  - All email communications to and from TresVista servers are encrypted using the TLS standard
  - All email communications (internal/external) are logged into a database and audited at regular intervals, eliminating risk of data leakage
  - Spam filtering tools are employed to block spam and other unauthorized messages entering and leaving the Company servers
  - Only authorized users are allowed to configure TresVista emails on their smartphones and such emails are provided via Microsoft Intune (MDM) which prevent emails from being copied or forwarded. The settings for the user can be configured only by the TresVista IT administrator

Folder Access, Domain, Website, and Email Control

All domains, websites, and email IDs that are blocked must be whitelisted and run through the Company firewall using the following processes:

- **For Whitelisting of Websites:**
  - The request is raised through a ticket, seeking approval from the respective VPs/EVPs/SVPs and the Compliance department, along with the below details:
    - VPs/EVPs (of RIS teams) and SVPs (of non-RIS teams)
    - Client name
    - Project name
    - Duration
    - Purpose or valid business justification (E.g., research work on social networking)
  - VPs/EVPs/SVPs and the Compliance department should not approve whitelisting requests unless all the above details have been shared by the requestor
  - The websites can be whitelisted for a maximum period of three months
- **For Whitelisting of Email IDs/Domains:**
  - The request is raised through a ticket, seeking approval from the respective VPs/EVPs/SVPs and the Compliance department, along with the below details:
    - VPs/EVPs (of RIS teams) and SVPs (of non-RIS teams)

- Client name
- Project name
- Duration
- Purpose or valid business justification

- VPs/EVPs/SVPs and the Compliance department should not approve whitelisting requests unless all the above details have been shared by the requestor
- The emails ids/domains can be whitelisted for a maximum period of three months. The duration can be extended basis quarterly reviews sent by IT

- **For Whitelisting of Google Drive/Dropbox/ FTP:**
  - The initial request from an Employee for access to a particular client's google drive/drop box/box is raised through a ticket, seeking approval from the respective VPs/EVPs/SVPs and the Compliance department, along with the below details:
    - VPs/EVPs (of delivery teams) and SVPs (of non-delivery teams)
    - Client name
    - Project name
    - Duration
    - Purpose or valid business justification
  - For all subsequent requests for data transfer through the above domains, pertaining to the same client and user, ticket should be raised to the IT department with similar details. These requests do not require additional approval from VPs/ EVPs/SVPs or Compliance department. However, Employee must ensure that these subsequent requests capture the initial ticket ID and relevant approvals
  - Access to google drive, drop box and box is provided to Employees through offline sync folder. Only IT administrator can manage accesses on the file sharing platform through web portal
  - Employee must take ab acceptance of responsibility from the client for revoking accesses (Details can be referred in Annexure C)
    - The template is available at https://tresvista.sharepoint.com/sites/Common/SitePages/Home.aspx
  - VPs/EVPs/SVPs and the Compliance department should not approve the whitelisting requests unless all the above details have been provided by the requestor
- **For Folder Access:**
  - The request must be raised through a ticket, seeking approval from the respective VPs, specifying the path of the folder
  - Authorities reserve the right to ask Employee for any additional information in this regard

- On receiving approval from VPs/EVPs (of RIS teams) and SVPs (of non-RIS teams), the access is granted to the Employee. However, in exceptional cases approval is given subject to prior approval of the Director
- All approvals are routed through the N+1 matrix in case the VPs/EVPs/SVPs are serving their notice period

Remote Access Control

- Remote access is provided to Employees to work from other location/home
- To take remote access of the system, Employees are required to connect through SSL/IPsec VPN application provided by the Company
- Remote access is provisioned via two (2) factor authentications
- Necessary host integrity checks shall be configured prior to authorizing remote access to TresVista network
- Remote access from internet cafe is restricted, and Employees should use remote access from their personal devices, or the Company provided laptops, when on business trips
- Activities such as remote file transfer and screenshots are restricted

Wireless Access Control

- Access to wi-fi is provided to all Employee's handset for accessing work emails along with limited access to the internet (Details can be referred to in mobile devices policy mentioned below)
- Security measures like firewalls, DLPs, and web protection software are implemented to prevent access to data files through the wi-fi network
- Wireless connections on mobile devices are terminated on segregated guest network
- Wireless access point is controlled through a centralized management portal
- Access to restricted websites by illegal means such as proxy applications is prohibited

Operational Software Control

- All applications installed on the operational systems are monitored and controlled as per the IT checklist
- Installation of non-compliant application is strictly prohibited
- If an Employee wants to use an application, not on the checklist, they need to raise a Helpdesk ticket with the IT department for approval prior to using the program on a system connected to the Company's network

Mobile Devices

- Only the Company's list of supported devices is allowed to connect to the network or access emails
- Devices are presented to the IT department for proper job provisioning and configuration of standard MDM apps, such as emails, browsers, office productivity software and security tools
- In case of remote onboarding, the IT department configures the MDM application remotely

- Emails are configured on mobile devices through the MDM application (Microsoft Intune) for all Employees except the Management
- Taking screenshots of email and attachment is restricted and controlled through the MDM application
- Attachments are encrypted and can be viewed only in MDM within the device and cannot be exported to an SD card or the device
- Software audit can be conducted at any time to ensure the network security is in operation
- The Employee's device is remotely wiped if:
  - The device is lost
  - The Employee terminates his/her employment
  - IT detects a data or policy breach, a virus or similar threat to the security of the Company's data and technology infrastructure
    - Details can be referred to in the Personal Device Policy

Backup

- TresVista follows strict backup procedures for data safety and ensures that industry standards are met
- Off-site backups are done on LTO tapes and on cloud, accessible only to the authorized individuals
- Data backup on cloud and LTO tapes are encrypted using paraphrase key (256-bit encryption)
- Access to backup databases and other data are reviewed annually
- Restoration of data is performed on regular basis to ensue integrity and availability of data backed up on cloud and tapes

User ID and Password

- Employee user IDs and passwords help maintain individual accountability for the internet, intranet and email resource usage. Employees are responsible for all activities on their username/account ID
- Sharing or using another Employee's user IDs or passwords to obtain access to the internet, intranet or email is prohibited
- Employees should select an obscure password and change it frequently, to prevent security breaches
- Five (5) invalid password attempts lock the user's account. The amount of time required to automatically unlock a locked account is ten (10) minutes
- Following password requirements should be complied with:
  - Minimum length – eight (8) characters
  - Maximum length – fourteen (14) characters
  - Minimum complexity - passwords should use four (4) of the following types of characters:

- Lowercase
- Uppercase
- Numbers
- Special characters such as! @#$%^&*(){}[]

- Passwords are case sensitive; the username or the login ID is not case sensitive
- Password history - requires a minimum of three (3) unique passwords before an old password may be reused
- Maximum password age – thirty (30) days
- Minimum password age – two (2) days
- Password-protected screen savers are enabled and protect the computer within ten (10) minutes of user inactivity

Employee Awareness

At TresVista, IT security training is provided to all new Employees as a part of the induction process and further refresher training is conducted for the entire firm annually.

Compliance

- The Compliance department validates the control self-assessment checklist done by IT department on a monthly basis and collects evidence if required
- The Compliance department conducts random end user checks and other necessary periodic audits as and when necessary

Non-Compliance

Any non-compliance with the aforementioned policy may result in disciplinary action.

11. Personal Device Policy

The purpose of this policy is to prevent unauthorized access, ensure the safety and security of TresVista networks, and to protect and avoid misuse of the client data and other confidential information.

Overview

The Personal Device Policy has been designed to support policies such as IT security and confidentiality policies, so that information is protected from unauthorized disclosure, use, modification, and deletion as TresVista grants its Employees the privilege of accessing emails on their devices for their convenience.

Applicability

This policy applies to all Employees of TresVista except FMS support staff.

Particulars

Employees at TresVista must agree to the terms and conditions set forth in this policy to use and connect their personal devices to the Company network.

Devices

In this policy, devices mean and include only the Employee's personal smartphones/tablets with android operating system and iOS which are used to install standard MDM apps (Microsoft Intune). The Company does not reimburse/cover the cost of the device.

Support

- When a new Employee joins the Company, they must contact the IT department for proper job provisioning and configuration of standard MDM apps, such as emails, browsers, and office productivity software & security tools
    - In case of remote onboarding, the IT department configures the MDM application on the Employee's personal device remotely
- IT department does not provide support in case the device has issues with the hardware and operating system
- Employees have their official email ID configured through the MDM application (Microsoft Intune) only on one device

Security

- Employees must protect their devices by using a password, PIN or any other feature of the device which prevents unauthorized access. To access the Company's network using the device Employees must use their username and a strong password
- The device must lock itself with a password or PIN if it's idle for more than five (5) minutes
- Rooted (android) or jailbroken (iOS) devices are strictly forbidden from accessing the Company's network (Wi-Fi access)
- Devices that are not on the Company's list of supported devices (other than android and iOS) are not allowed to connect to the network
- Employees' access to Company data on their devices is limited based on user profiles defined by IT department and such access is automatically enforced
- The Company reserves the right to disconnect devices or disable services without notification

Responsibility of Device Owner

- The device owner is expected to always use their device in an ethical manner and adhere to the security and support aspects of this policy as outlined above

- If the device needs a remote wipe, the IT department takes necessary precautions to prevent any personal data loss and the onus to take additional precautions, such as backing up personal data such as contacts, etc. is on the device owner
- In case of theft/loss/damage/change of device, the device owner must follow these guidelines:
    - **Theft/Loss:**
        - Report to the IT department within six (6) hours from the time of theft/loss by raising an incident on the Helpdesk
        - Employees can use their personal email ID during non-working hours to report such incidents to IT department at IT@tresvista.com
        - Employees must also notify the mobile carrier immediately upon loss/theft of a device
    - **Device Change/Damage:**
        - A request needs to be raised through a Helpdesk ticket, requesting re-installation of Microsoft Intune
        - Device owner needs to submit old device along with the new device to the IT department for configuration of standard MDM apps, such as emails, browsers, and office productivity software and security tools
        - It is mandatory to submit the old device before getting email configured on the new device
        - In exceptional cases where the Employee is on leave and the old device cannot be submitted, the device owner must seek approval from their respective VPs/EVPs (for delivery teams) and SVPs (for non-delivery teams) and the Compliance department for re-installation of Microsoft Intune
            - Once approval is granted the IT department shares the necessary details required to configure email with the device owner
            - However, the device owner must present the new device to the IT department in order to change the email ID password as and when they resume work

Liabilities of the Device Owner

Although this policy provides overall guidance to achieve consistent information protection, the device owners are fully liable for risks including, but not limited to, 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.

Compliance

- The Compliance department reviews the following on a monthly basis:
    - Adherence to the procedures laid down in the policy above
    - IT reports for re-installation of Microsoft Intune and user emails to IT informing them of theft/loss of device

- Employee should inform the Compliance team immediately if they come across any violation of this policy

Non-Compliance

Any non-compliance with the aforementioned policy may result in disciplinary action

12. Password Management Policy

The purpose of this policy is to ensure that security practices with respect to password-protected information infrastructure are informed to and adhered by all Employees in the organization.

Overview

- Users must practice due diligence in controlling access to their systems by protecting their user accounts with passwords that are not easily guessed or deduced
- Passwords are an important aspect of computer security and act as the front-line protection for user accounts
- A poorly chosen password may result in the entire corporate network of TresVista being compromised
- As such, all Employees (including contractors and vendors with access to TresVista's systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords

Particulars

- Password Policy ensures that all user accounts are protected by strong passwords and the strength of the password meets the security requirements of the system
- The concept of aging is used for passwords and on their expiry, the passwords cease to function
- Users are educated about password protection and the policy is implemented to ensure that users follow best practices defined in this policy
- For critical information systems, the account lockout strategy is defined basis the risk analysis of the system as well as the costs to be incurred in case such a strategy is implemented
- **Password Standards:** All user and system passwords (Including temporary passwords set for new user accounts) must meet the following characteristics:
    - Be at least eight characters in length
    - Consist of a minimum of one character from [A-Z]
    - Consist of a minimum of one character from [a-z]
    - Consist of a minimum of one number from [0-9]
    - Consist of a minimum of one special character [$@!%*#?&]
    - Do not use first name and/or last name
    - Do not use previous three passwords

- Should not be simple keyboard patterns

- In addition, users are required to select a new password immediately after their initial login. Passwords must be changed at least every thirty (30) days and previously used passwords should not be re-used

Enforcement

Unauthorized personnel are not allowed to see or obtain sensitive data. Any Employee found to have violated this policy is subjected to disciplinary action, as determined by the organization.

13. Physical Security Policy

The purpose of this policy is to define procedures to mitigate the risk of security breaches, to establish the standard privacy control, to enforce applicable laws and regulations, and create information barriers in the workplace.

Applicability

This policy applies to all the Employees of TresVista including full-time, part-time, and interns, whether permanent or temporary

Scope

This policy will be applicable to all the Employees full-time, part-time, and interns, whether permanent or temporary, subject to the availability of TresVista owned controls such as:

- Biometric Access
- Secured Zones
- Tailgating
- Closed Circuit Television System (CCTV)
- Work Area Security
- Desk Security
- Vendor Access

Particulars

- **Biometric Access:**
  - A biometric system is installed to restrict the access of Employees in the TresVista office premises apart from the basic function of capturing attendance
  - Biometric access logs are stored in an application
  - Access to specific work area is granted based on the role and responsibilities of the personnel
- **Secured Zones:**
  - Secured zones have been defined to restrict access to a specific work area

- Secured zone access is reviewed quarterly by the respective Head of Department (HOD)
- A separate secured zones access matrix is maintained, clearly segregating the access type which is to be referred to along with this handbook
  - The secured zones access matrix is available at sites/Common/SitePages /Home.aspx

- **Tailgating:** Employees (except EmployeeFMS support staff) are not allowed to tailgate and should use the biometric system while entering areas wherever access control is applicable
  - Employees are responsible for reporting the presence of any suspicious person in the TresVista office premises
- **Close Circuit Television System (CCTV):**
  - CCTV cameras are installed at all the entrance/exit points and across restricted areas within the workplace
  - The CCTV systems are reviewed regularly
  - The images/recordings are stored for thirty (30) days on the DVR (Digital Video Recorder) and NVR (Network Video Recorder)
  - The Management may delegate administration of the CCTV system to another Employee, if required
  - Access to view CCTV recordings is limited to the authorized individuals on a need-to-know basis
    - The Compliance department will audit such CCTV recordings on a monthly basis and as and when necessary
- **Work Area Security:**
  - All Employees, excluding FMS support staff:
    - Are required to display the ID card at all the times while in the office premises
    - Should ensure that no data either on desktops, laptops, TV screens or hard documents/ files, etc. is captured while clicking pictures or making videos within office premises. While working out of office premises, Employees should ensure they do not click pictures or videos of their desktop/laptops/tablets or any other device displaying TresVista data
    - Are not allowed to carry their personal laptops to the office
  - All official print outs should only be taken using the secured print feature
    - To take printouts while working from out of the office premises, Employees need to seek prior approval from their line Manager and the Compliance department via a Helpdesk ticket
  - Employees are not allowed to carry any Company documents (including notepads) outside the office premises. In exceptional cases, if required, Employee shall be allowed to take documents subject to approval per the below matrix:

Documents	Approval (Via Helpdesk)	Authority

Carrying documents outside office premises	Prior approval	Line Manager Compliance department (Authorities reserve the right to ask Employee for details of project, etc.)

- **Desk Security:** Except for FMS support staff, all Employees must ensure that:
  - All documents are kept in locked drawers (including, but not limited to client related documents, backup documents, analysis, information received from clients and any other material marked as confidential)
  - The drawer keys should not be kept unattended
  - Any paper should not be left unattended on the desks
  - Printouts should not be left unattended near the printer. Such unattended printouts are shredded within ten (10) minutes from the time of printout, without any intimation
  - Any other unattended documents at the desks are shredded daily at 7:00 AM IST
- **Vendor Access**
  - Vendors are permitted to visit the office premises at the discretion of the concerned department
  - Vendors should always be accompanied by a SPOC from the concerned department they are working with
    - If the SPOC is on probation/serving notice period, the responsibility of the visit lies with their line Manager

Compliance

Employee should inform the Compliance team immediately if they come across any violation of this policy.

Non-Compliance

Any non-compliance with the aforementioned policy may result in disciplinary action

14. Confidentiality Policy

The purpose of this policy is to educate Employees on the protection of confidential information of Company, clients, etc. received by them during the course of their employment.

Applicability

This policy applies to all Employees of TresVista including full-time, part-time, and interns, whether permanent or temporary.

Particulars

- To ensure that confidential information is well protected, Employees should only disclose information on "need-to-know" basis.
- Employees are not allowed to:
  - Disseminate or provide access of information to unauthorized recipients inside or outside the Company
  - Use information for personal benefit
  - Share or use another Employee's user ID or password to obtain access to the internet, intranet or email
  - Take confidential information out of the office
  - Leave confidential information/documents unattended or unlocked at the desk or near a printer
  - Replicate information in an unauthorized manner
  - Share client name, project details, etc. while sharing any document for illustration purposes
  - Discuss client-related information in public areas (E.g., client name, ongoing projects, etc.)
- Additionally, all the Employees must execute a Non-Disclosure Agreement (NDA) and submit it virtually to the HR Operations team (ops@tresvista.com) via email

Compliance

- The Compliance department conducts internal checks, and verifications as a part of the monthly internal audit
- Email surveillance, desk checking, and physical checking (frisking of Employees) also forms a part of the internal audit to ensure confidentiality

Non-Compliance

Any non-compliance with the aforementioned policy may result in disciplinary action.

15. Personal Account Dealing Policy

The purpose of this policy is to detail out procedures for restricting Employees from trading in personal accounts using price sensitive information for personal gain/benefit.

Employees are required to comply with the restrictions on insider trading and market manipulation under the UK Market Abuse Regulation (UK MAR), the Criminal Justice Act 1993 and Financial Conduct Authority (FCA) guidance relating to UK MAR and in the FCA Handbook

Applicability

This policy applies to all Employees of TresVista except those in the following team/departments: Admin, Strategy, FMS, Corporate Finance, Financial Strategy, Human Resources, Compliance, Information Technology, Legal, Procurement,

Marketing & Corporate Communications, Training, Software Development, Sales, Career Enhancement Cell and FMS support staff.

Particulars

- **Personal Account (PA) Dealing:** In this policy, each of the following is considered as PA Dealing:
  - Trading in securities from a personal trading account (In this policy 'dealing in securities' means an act of subscribing, buying, selling, or agreeing to subscribe, transferring, and transmitting any securities)
  - Dealing in securities by any individual or entity for an Employee's account, or for the account of any of his/her connections or where the Employee or his/her connections benefit

Securities

- Securities have the meaning assigned to it under the US Securities Contracts (Regulation) Act, 1956 (42 of 1956) or Securities Exchange Act, 1934, and includes "financial instruments" as specified in the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (SI 2001/544) for the purposes of UK MAR or any modification thereof and include securities listed in foreign countries except units of mutual fund, cryptocurrencies, donation and rewards which may include following:
  - Shares, scrips, stocks, bonds, debentures, debenture stock or other marketable securities of a similar nature in or of any incorporated Company or another body corporate
  - Derivatives
  - Units or any other instrument issued by any collective investment scheme to the investors in such schemes
  - Security receipt as defined in Securities Exchange Act, 1934, Securitization and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002 or such other US Laws as may be applicable along with any modification thereof
  - Government securities
  - Such other instruments as may be declared by the Central Government to be securities
  - Rights or interest in securities
- However, dealing with a Discretionary Portfolio Management Service ("PMS") or Pension Plan where there is no prior relevant communication (direct or indirect) between the portfolio Manager and the Employee, or any other person for whose account the relevant dealing takes place, is not PA dealing
- If an Employee or their connections use the same service provider to provide both such discretionary Portfolio Management services and also to place or execute PA dealing orders, then the Employee should ensure that the service provider keeps separate records for transactions entered under the discretionary Portfolio Management Service and for PA dealing

Connections

- An Employee's connections are:
  - Dependent Parents including stepmother and stepfather
  - Dependent spouse or another partner equivalent to a spouse
  - Dependent children, stepchildren, and adopted children
  - Dependent siblings (including stepbrother and sister)
  - Any other person who is financially dependent on the Employee
- For the purpose of this policy, the definition of 'dependent' has the meaning assigned to it under section 80DD of the US Income Tax Act, 1961 (43 of 1961) or the applicable Law
- An Employee should check with the Compliance department if they are unsure of how to interpret above connections in their case

Disclosure

- Employees must provide the following documents to the Compliance department on Darwinbox:
  - **Initial Holdings Declaration:** Employees need to provide the securities holdings information of the active/dormant/inactive trading account held by them and their connections (Refer Annexure B)
  - **Discretionary PMS Declaration:** Employees need to provide the confirmation letter signed by the broker, if applicable for the accounts held by them and their connections (Refer Annexure B)
  - **Foreign Holdings Declaration:** Employees need to provide the foreign securities holdings information, if applicable for the accounts held by them and their connections (Refer Annexure B)
  - **Trading Account Opening/Closing Declaration:** Employees need to notify the Compliance department about the opening/closing of the trading account held by them and their connections by filling Form C under the category of Personal Account Dealing Declarations on Darwinbox within two (2) working days of opening/closing the account, including any trading account opened/closed to deal in foreign securities (Refer Annexure B)
- Guidelines and timelines to fill up the above-mentioned documents are available at https://tresvista.sharepoint.com/sites/Common/SitePages/Home.aspx
- It is the responsibility of the Employee to read the guidelines and submit the declarations as per the instructions mentioned therein
- An existing account is a trading account which has already been disclosed in Form A at the time of joining or any subsequent account opened during the Employee's tenure at TresVista which has been disclosed in Form C

- In case an Employee needs an extension to submit the trading account statements/or fill the initial holding declaration/annual declaration, they may raise a ticket with the Compliance department on the Helpdesk in the template provided therein, within the submission deadline
- In case of physical onboarding, new hires must fill in the disclosures on DarwinBox within two (2) working days of completing their compliance training and subsequently submit their stamped and signed trading account statements within ten (10) working days of completing their compliance training

Holding Period

- Employees should hold securities for a minimum period of thirty (30) days from the last date of purchase
- There shall not be any exceptions are made to the above-mentioned holding period even in cases of a stop loss order, margin loss, trailing stop orders, or any other methods for limiting losses
- The Compliance department may at any point of time ask for statement of the investments, and Employees are bound to provide the same within the requested timeline
    - In case these statements are not submitted within the timeline specified during the audit, they may face disciplinary action

Role of the Compliance Department

- The Compliance department constantly checks that all the steps mentioned above are followed before and after a trade
- It will verify adherence to this policy through various methods, including but not limited to, monthly internal audits, random checks, or any other means as deemed necessary
- The Compliance department scrutinizes the following documents:
    - Account statements received from Employees
    - Transaction holding period
    - Disclosures provided by Employees from time to time

Non-Compliance

- Any non-compliance with the aforementioned policy may result in disciplinary action
    - Serious offenses such as not holding securities for a minimum period of thirty (30) days from the date of purchase, etc., may amount to gross misconduct resulting in summary dismissal

16. Data Privacy Policy

The purpose of this policy is to outline the procedure for Management of incidents, breaches or events that may result in interruption in the daily operations and to ensure that data is stored and maintained regularly and systematically.

Overview

- The policy outlines Management of:
  - Incidents or breaches that may occur inside/outside TresVista premises, including those that involve service users, Employees, visitors, or vendors
  - Incidents or breaches that have occurred and those that were a 'near miss'
- Employees must treat information of Clients, stakeholders and other interested parties with the utmost care and confidentiality

Applicability

This policy applies to all as well as any contractors or service providers acting on behalf of TresVista.

Policy

- **Data Privacy Issues:** Data privacy issues can come in many forms, some of which are mentioned below:
  - Loss or theft of papers with information which fall under any data classification category except public information
  - Data posted, emailed or faxed to an incorrect recipient
  - Loss or theft of equipment on which the data is stored
  - Inappropriate dissemination of information
  - Data corruption
  - Unescorted visitors accessing data
  - Non-secure disposal of data
  - Shared Client related information/proprietary data without legitimate reason
  - Compromise on integrity of information
- **Responsibilities:**
  - Employees are required to report all data privacy issues (including potential or suspected incidents or breaches) as soon as they become aware of it
  - In the event of a data privacy issue which involves an Employee or another Person within their team and/or area of responsibility, line Managers are required to ensure that such issues are reported centrally as outlined under this policy
  - The Compliance department has the responsibility to ensure that all data privacy issues are dealt with appropriately
  - The Head of Department - Compliance has overall responsibility for ensuring that TresVista complies with this policy

- **Data Privacy Management:**
  - **Reporting**
    - All data privacy related issues should be reported and notified to the Compliance department via email, as soon as possible
    - The reporting email should provide the following information:
      - Description of the data shared
      - Classification of the data shared (to be finalized by the data owner as per data classification policy)
      - Difference in the timeline between reporting and the privacy issues
      - Action taken to retrieve data if any
      - Client name if such data pertains to a specific Client
    - All emails that report data privacy issues will be considered as critical
    - The Compliance department ensures that such emails are responded within thirty (30) minutes and resolutions are provided within two (2) hours from when the email was shared on business working days
  - **Business working days:** Monday-Friday between 9:00 AM to 6:00 PM IST

Investigation and Resolution

- On intimation from Employees, the Compliance department evaluates the situation in consultation with the Head of Department - Compliance and responds to any reported issues after assessing the below mentioned aspects:
  - Assessment of data classification shared
  - Assessment of whether the data was shared inappropriately internally or externally

Data Type	Situation	Privacy Incident	Privacy Breach
Public	NA	NA	NA
Internal	Unauthorized disclosure or access to data transmitted, stored, or processed by TresVista with individuals internally	NO	YES
	Unauthorized disclosure or access to data transmitted, stored, or processed by TresVista with individuals externally	YES	NO

Restricted	Unauthorized disclosure or access to data transmitted, stored, or processed by TresVista with individuals internally and externally	YES	NO
Confidential	Unauthorized disclosure or access to data transmitted, stored, or processed by TresVista with individuals internally and externally	YES	NO

- The issue is notified to the Management in case the privacy breach or incident relates to Client data. SVP of the Client team after consultation with the Head of Department – Compliance and Management shall further notify to the Client as they deem fit
- Log-sheet is maintained to review successful resolution of the data privacy issues reported and to ensure that all the policy breaches and incidents as captured in the logs are recorded and dealt with accordingly
- Learnings and corrective actions of privacy incidents are reported and recorded in the quarterly incident Management meetings
- Suitable actions are taken as per the Consequence Management Process

Escalation Matrix

The email is escalated to the following authorities in case of delay of resolution:

Department	Level one	Level two	Level three
Compliance	Compliance department requests.compliance@tresvista.com	EVP, Compliance department vandana.pandey@tresvista.com	SVP, Compliance department nilay.vyas@tresvista.com

Record Maintenance

The record of all the incidents and breaches reported under this policy are maintained by the Compliance department.

Compliance

The Compliance department conducts periodic checks to ensure adherence to the policy.

Non-Compliance

Any non-compliance to the aforementioned policy may attract Disciplinary Actions as defined in the annexures of this handbook.

17. Policy for Material Non-Public Information (Insider Information)

The purpose of this policy is to ensure that any confidential information about the Company, clients, etc. received by Employees during the course of their employment is protected, and to define guidelines in order to ensure compliance with laws governing:

- Trading in securities while in the possession of "material non-public information"(MNPI) (inside information) about any Company or any of its subsidiaries, and
- Disclosing MNPI to outsiders ("tipping")

Objective

- Set out procedures to restrict Employees from trading in personal accounts using MNPI for personal gain/benefit
- Educate Employees about MNPI, tipping and promote TresVista's ongoing commitment to compliance with all applicable insider trading laws
- Assist Employees in meeting their responsibilities in terms of complying with these laws and internal policies

Scope

This policy applies to:

- All Employees of TresVista
- All transactions in securities of a client Company, MNPI of which the Employee has obtained during the course of their employment with TresVista
- Employees are required to comply with the restrictions on insider trading and market manipulation under the UK Market Abuse Regulation (UK MAR), the Criminal Justice Act 1993 and Financial Conduct Authority (FCA) guidance relating to UK MAR and in the FCA Handbook, as well as relevant US laws and regulations

Definitions

- **Material Information:**
  - Any information about the client Company that a reasonable investor would consider important in the decision to buy, hold, or sell securities of the client Company is considered as material information

- In simple terms, material information is any type of information that could reasonably be expected to affect the price of client Company securities, regardless of whether the information is positive or negative
    - E.g.: Information regarding future earnings or losses; changes in dividend policies; declaration of a dividend; any pending or proposed merger; acquisition or tender offer; a significant sale of assets or sale of a subsidiary; significant management changes; labor negotiations; the offering of additional securities; information about the Company's capital structure, including liquidity or other financial metrics; unusual gains or losses in major operations; major marketing changes; the gain or loss of a substantial customer or supplier; significant new products or discoveries

- **Non-public information:**
    - Any information about the client Company that has not been publicly disclosed is considered as non-public information
    - Information ceases to be non-public when it has been broadly disclosed and investors in the client Company's securities have had sufficient time to assimilate and react to it
    - The circulation of rumors, even if accurate, widespread, and reported in the media, does not constitute public disclosure. Similarly, only disclosing part of the information also does not constitute public dissemination
    - To this policy, TresVista considers information as generally be considered public i.e., information about the client Company has ceased to be non-public after the second business day following the date on which the client Company has disclosed such information to the public
    - Generally, the client Company discloses this non-public information by filing annual, quarterly, current, or other reports and communications with the Securities and Exchange Commission and respective enforcement agency
- **Tipping:** For this policy, tipping is defined as passing or providing access of MNPI about a client Company by the Employee to any individual who does not have a confidential relationship with the client Company or have a valid reason to be in possession of such information

Standards of Business Conduct

- TresVista seeks to comply with federal securities laws and regulations applicable to its business and Employees who have access to confidential information are not permitted to use or share that information for the purpose of trading securities or any other purpose except to conduct regular business operations
- Employees should share information on a need-to-know basis
- If an Employee possesses any material, non-public information about the client, they are not permitted to trade, (i.e., buy or sell) in any securities of the client Company or engage in any action that takes advantage of such MNPI until such information ceases to be non-public

- No Employee should tip off or disclose MNPI about any client Company, or give trading advice of any kind to anyone while in the possession of MNPI
- All the Employees must execute a Non-disclosure Agreement (NDA) at the time of joining TresVista to protect the material, non-public information about the Company, clients, etc. received by Employees during the term of their employment
- If Employees are sent or receive access to any material, non-public information concerning the client, they should ensure that this information is kept confidential and immediately inform the Compliance department about it
- Questions regarding whether the information is "confidential", "material" or what restrictions exist on the use or distribution of such information should be directed to the Compliance department
- In addition to this policy, Employees are also required to adhere to the applicable policies /clauses detailed out in this manual

Treatment of MNPI

- Guidelines and procedures which form a part of this handbook limit the flow of MNPI from one team/department or area to another
- TresVista creates an information barrier (i.e., a Chinese wall) to further limit the flow of MNPI from one area to another (e.g., client specific captives for teams managing MNPI)
    - The information barrier safeguards and restricts the flow of MNPI and prohibits anyone in an "inside" area from communicating MNPI to anyone in an "outside" area, unless approved by the Compliance department
    - The Compliance department monitors the flow of information within inside areas at regular intervals
- If a team/department is functioning in a business area that is not within the information barriers, and any MNPI is received, the responsibility is of the VP/EVP of that team/department to reach out to the Compliance department immediately
    - The Compliance department then relocates the team/department to an information barrier till the time the project is concluded
- If a team/department is in possession of MNPI which may lead to a potential conflict of interest for another client, it is the responsibility of the SVP of that team/department to reach out to the Compliance department immediately

Inadvertent Disclosure

- The Compliance department is responsible for the administration of this MNPI Policy
- If any Employee becomes aware that MNPI is inadvertently disclosed by another Employee, officer, etc., to a person outside the Company who is not obligated to keep this information confidential, they must be immediately report this to the Compliance department so that appropriate remedial action can be taken

Compliance

- The Compliance department conducts internal checks, and verifications as a part of internal audit. It verifies adherence to this policy through various methods, including but not limited to, random checks or any other means as deemed necessary
- Once the Compliance department receives information from the relevant team/department about the receipt of MNPI, it takes necessary steps to prevent unauthorized flow of MNPI
- Compliance department also scrutinizes the:
  - Account statements received from Employees
  - Transaction holding period to ensure that no trades have been carried out by Employees who are in possession of MNPI
  - Disclosures provided by Employees from time to time

Non-Compliance

- Any non-compliance of the policy leads to disciplinary actions
- Serious offenses such as theft of MNPI, illegal disclosure of sensitive data, etc., may amount to gross misconduct resulting in summary dismissal and may also involve legal consequences, at the discretion of the Company
- Non-compliance of this policy could also result in both civil and criminal penalties, including fines and jail sentences even for the person who trades based upon a tip
- Employee also incurs penalties for such violations by tipping information to others, even if the Employee has not personally gained any profit from the other person's actions

18. Fraud and Whistle-Blower Policy

The purpose of this policy is to establish and define:

- A framework for reporting instances of unethical/improper conduct under the definition of fraud
- Procedures to review disclosures and direct corrective/preventive action concerning disclosures reported to the relevant authorities within the organization
- Roles and responsibilities for prevention, detection, and investigation of fraud within the organization

Overview

All the Employees at TresVista act as ambassadors of the organization and are expected to uphold the principles of honesty and integrity, on which the organization is built. With the intention of ensuring ethical behavior, TresVista considers it appropriate to provide a channel for Employees and stakeholders to report any behavior which is inconsistent with firm

values and bring to the notice of Compliance department any event or concern that may warrant necessary disciplinary action (E.g.: Employee recommending dismissal of a senior person for dishonesty).

Through this policy, TresVista is committed to supporting and facilitating the detection and prevention of fraud and ensure an honest, open, and well-intentioned work environment wherein people are assured that they can raise concerns without fear of reprisal, retaliation, discrimination, or harassment.

Scope

This policy applies to any fraud that is detected or suspected by a 'whistle-blower', and committed by anyone who has a business relationship with TresVista, including but not limited to an Employee, stakeholder, client, consultant, vendor, service provider, etc.

Whistle Officer

For the purpose of this policy, the Head of Department - Compliance has been appointed as the Whistle Officer by the Management.

Executive Committee

- The Executive Committee responsible for investigating fraud comprises of:
  - Chairperson: Managing Director
  - Member: Director
  - Member: Head of Department – HR

Roles and Responsibilities

- TresVista values the integrity of its Employees and recognizes that they have a key role to play in the prevention, detection and reporting of fraud
- Employees are encouraged to always be vigilant and to report any concerns they may have immediately and must ensure that they:
  - Are aware and informed of the 'Work ethics' and 'Fraud and Whistle-blower' policies
  - Seek advice from their colleagues or Managers, when required
  - Offer suggestions on improving the work environment
  - Report potential or suspected violations of the law or TresVista policy, including situations when they are aware that an Employee or third party engaged with the firm is currently or will potentially engage in illegal, inappropriate, or unethical activity
- The Head of Departments must ensure that:

- Employees are communicated the applicability of the 'Work ethics' and 'Fraud and Whistle-blower' policies within their areas of responsibility
- An adequate system of internal fraud control exists within their areas of responsibility and these controls operate effectively

- The Whistle officer must ensure that:
  - All frauds are investigated promptly and diligently
  - Guidance is provided in case there is any question as to whether an action constitutes fraud
- The Executive Committee must ensure that:
  - The investigation process is fair and transparent
  - Appropriate legal and/or disciplinary action is taken in cases where it is justified/required
  - Systems and procedure changes as a result of unique cases are incorporated immediately to prevent similar instances from occurring again

Reporting a Suspected Fraud

- Fraud must immediately be reported by the whistle-blower to the whistle officer or the Compliance department through any of the modes of communication defined below:
  - **Email:** An email can be sent to requests.compliance@tresvista.com which is accessed by the Senior Vice President and/ or the Compliance department
  - **Written Complaint:** A written complaint can be made and delivered in person or dropped in the drop box at the following address:
    - Head of Department - Compliance,
      TresVista Analytics LLP,
      5th floor, North wing block-2, Milestone Buildcon IT SEZ,
      Bhartiya Centre of Information Technology,
      Thanisandra Main Road,
      Bengaluru Urban, Karnataka, India – 560064
  - **Protect:** protect is an independent UK whistleblowing charity. It can be contacted as follows:
    Helpline: 0203 117 2520
    Email: info@protect-advice.org.uk
    Website: https://protect-advice.org.uk/contact-protect-advice-line/
  - **Financial Conduct Authority (FCA):**
    Contact details for whistleblowing team:
    Telephone: +44 (0)20 7066 9200

Email: whistle@fca.org.uk

Postal address: Intelligence Department (ref PIDA), Financial Conduct Authority, 12 Endeavour Square, London, E20 1JN

Website: www.fca.org.uk/firms/whistleblowing

- In order to establish reliability of the event, all complaints of fraud should be supported by the following details:
  - Day, date, time and venue
  - Name of the whistle-blower
  - Names of the person accused of committing fraud
  - Details of the unethical or improper activity or suspected fraud
  - Other witnesses and evidence (if any)
- Irregularities concerning an Employee's moral, ethical or behavioural conduct should be resolved by the department VP/EVP/SVP in consultation with the HR department and there is no involvement from the Compliance department and the Whistle Officer

Anonymous Allegation

- Though we endeavour to keep the identity of the whistle-blowers anonymous, it is strongly advised that the whistle-blower discloses his/her identity when making the complaint, as follow-up questions and investigations may not be possible unless the source of the information is identified
- This also ensures timely resolution of the issue and that adequate protection granted to them under relevant provisions of this policy
- Disclosure of the identity is also important to ensure that complaints are authentic and validated prior to pursuing any action

Action on False Disclosures

- This fraud and whistle-blower policy intends to cover serious concerns that could have a grave impact on the operations, performance and reputation of TresVista
- The policy neither releases Employees from their duty of confidentiality in the course of their work nor does it provide a platform to take up grievances concerning a personal situation
- Fraud reported must not be frivolous in nature and based on conjecture or hearsay. If we conclude that false disclosures/complaints are made, then the complainant will be subject to disciplinary action

Protection

- Protection is provided to the whistleblower who has reported a fraud which they reasonably believe to be true and in the public interest to report

- To ensure that this policy is adhered to, and to assure that disclosures are acted upon seriously, TresVista aims to ensure that:
- The identity of the whistle-blower is kept confidential, and protection is provided to the whistle-blower for an indefinite period of time
- The whistleblower and/or the whistle officer processing the fraud are not victimized for doing so
- No adverse personnel action is to be taken or recommended in retaliation to their disclosure of unethical and improper practices or alleged wrongful conduct. This policy protects such Employees from unfair termination and unfair prejudicial employment practices
- No unfair treatment is vetted out towards the whistle-blower by virtue of having reported a fraud and they receive protection against:
  - Unfair employment practices like retaliation, threats, intimidation of termination/suspension of services, etc.
  - Disciplinary action including transfer, demotion, refusal of promotion, etc.
  - Any kind of prosecution, impeachment, or indictment
  - Direct or indirect abuse of authority to obstruct the whistle-blower's right to continue performing their duties/functions during routine business operations, including making further disclosures under this policy
- Appropriate disciplinary action is taken against any person who is found committing any of the above actions against the whistle-blower

Investigation of Suspected Fraud:

- The whistle officer is primarily responsible for investigating all suspected frauds based on the communication received from whistle-blowers
- On receipt of a suspected fraud disclosure, the whistle officer must send an acknowledgment to the whistle-blower informing them not to:
  - Attempt to personally conduct investigations, interviews or interrogations in this regard
  - Contact the suspected individual to determine facts or demand restitution
  - Discuss the case, facts, suspicions, or allegations with anyone
- All subjects must be duly informed about the complaints of unethical practice(s) made against them at the commencement of the formal investigation process and be provided opportunities to explain themselves during the investigation process
- The investigation conducted against any subject shall not be construed by itself as an act of accusation. The investigation would be conducted in a fair manner, as a neutral fact-finding process, without the presumption of guilt and providing an adequate opportunity for the affected party to present their side of events

- During the investigation all inquiries concerning the activity under investigation from the subject, their legal representative, or any other person must be directed to the whistle officer. Information concerning the status of an investigation should be kept confidential
- Confidentiality of the information and the subject should be ensured by the whistle officer. If initial inquiries indicate that a complaint has no basis, or it is not a matter to be pursued under this policy, it may be dismissed at this stage and the decision is documented
- During the investigation the Whistle Officer has the:
  - Right to call for and examine any information/document of TresVista
  - Unrestricted access to all TresVista records and premises, whether owned or rented; and without prior knowledge or consent of any individual who might use or have custody of any such items or facilities, as may be deemed necessary for the purpose of conducting investigation under this policy
- If the preliminary investigation substantiates that fraud has occurred, the whistle officer must submit a 'whistle-blower report' to the Executive Committee for their consideration
- Until the investigation is concluded, and decision of the Executive Committee is released, TresVista is not liable or bound to any litigation

Executive Committee Review

- On submission of the whistle-blower report by the whistle officer, the Executive Committee must review the findings from the investigation
- The review process is conducted in a fair manner, as a neutral fact-finding process, without the presumption of guilt
- Post the review process, the Executive Committee directs appropriate corrective/preventive disciplinary action in cases where there is reason to believe that fraud has been committed
- The decision of the Executive Committee comprising of all, or any two (2) members are considered binding and final. In the event of a dispute between the members, the decision of the Chairperson prevails
- Decisions to prosecute or refer the examination results to the appropriate law enforcement and/or regulatory agencies for independent investigation is to be made by the Chairperson of the Executive Committee in conjunction with the Legal department

Reports and Documents

- Investigation results are not to be disclosed or discussed with anyone other than those who have a legitimate need to know
- This is important in order to avoid damaging the reputations of subject(s) subsequently found innocent of wrongful conduct and to protect the Company from potential civil liability

- All disclosures made by the whistle-blower, the whistle-blower report, and the documents obtained during the investigation, along with the results of the investigation relating thereto, must be retained by TresVista for a minimum period of four (4) years

Compliance

- Head of Department - Compliance submits on a quarterly basis to the Board and Senior Management, summarizing the fraud cases along with the following details, as applicable:
  - The nature of cases reported under this policy and the proposed action thereon
  - The status of fraud cases reported in the previous and current period and action taken thereon
  - Results/status of any investigations/enquiries in reference to the fraud cases reported
- Head of Department - Compliance is responsible for the administration, revision, interpretation, and application of this policy. The policy is to be reviewed annually and revised as needed

TresVista Powers

This policy is hosted on the TresVista website and is available to all Employees in the organization. A hard copy of this policy is made available to any person on demand. TresVista reserves its right to amend or modify this policy in whole or in part, at any time without assigning any reason whatsoever, after due consultation with the Executive Committee.

19. Data Classification Policy

The purpose of this policy is to provide a framework for classifying data based on the level of sensitivity, value, and its criticality to Company and clients. Classification of data helps in determining baseline security controls required for the protection of data.

Applicability

This policy applies to all Employees, except FMS support staff, who process, have access to, or store sensitive client and Company data.

Scope

- This data classification policy applies to all information that is in the Company's possession (e.g., confidential information from clients, business partners, internal information, and others), and protected under this policy
- For the purpose of this policy, the words - data, information, knowledge, and wisdom are used interchangeably

Particulars

- This policy has been designed to support policies such as IT security, access controls and confidentiality policies, so that information is protected from unauthorized access, disclosure, use, modification, and deletion
- Consistent use of the data classification system facilitates business activities, improves client confidence, and helps to keep the costs of information security to a minimum

Consistent Protection

- Information must be consistently protected throughout its life cycle, from origination to destruction
- Information must be protected in a manner commensurate with its sensitivity, regardless of where it resides, what form it takes, what technology is used to handle it, and/or what purpose(s) it serves
- Although this policy provides overall guidelines for consistent information protection, Employees are expected to apply and extend these concepts to their day-to-day operations

Data Classification Matrix

- The IT administrator is the owner of the data classification matrix
- The data classification matrix provides classification on data as well as an overview of the access rights given to Employees

Data Owners

- Data owners are at the VPs/EVPs/SVPs and equivalent designations
- Data owners are responsible for abiding by the appropriate sensitivity classifications as defined by the client/stakeholder
- Data owners do not legally own the information entrusted to their projects
- Data owners are instead designated members of the Company’s management who supervise ways in which certain types of information is used and protected

Personal Data

Personal data means any information relating to an identified or identifiable natural person such as name, online identifiers (such as an IP address), mental, economic, cultural, or social identity and location data of that person

Sensitive Personal Data

Sensitive personal data (special category personal data) means any information consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life and sexual orientation

Classification and Labels

- **Public Information:**
  - Public information is the information that is declared/published for public knowledge by someone with the authority to do so, either for publicity purpose or as a mandatory requirement per the regulation
  - This classification applies to information that is available to the general public and intended for distribution outside the Company
  - This information may be freely disseminated without potential harm and is labelled as public (e.g., details shared on the Company website, advertisements, job openings, event announcements, press releases, etc.)
  - In case data is not labelled then such data shall also be considered as public data
- **Internal Information**
  - This type of information is meant for circulation within TresVista only
  - It is declared/published by someone in the organization with the authority to do so
  - This classification applies to all information that is intended to be used by Employees within the Company. All such data is labelled as internal
  - The unauthorized disclosure, modification or destruction of this information could expose the Company, Employees, or its business partners to a moderate level of risk. (E.g.,: Company telephone directory, new Employee training materials, and internal policy manuals)
- **Restricted Information**
  - This type of information should be protected very closely, as it is integral to the success of the organization
  - This classification applies to sensitive business information that is intended strictly for the use of specified departments and Employees in the Company. All such data is labelled as restricted
  - Such information is made available on a need-to-know basis within TresVista (e.g., price sensitive information, merger and acquisition documents, corporate level strategic plans, internal projects, litigation strategy memos, etc.)
- **Confidential Information**
  - This type of information could belong to another Company/personnel which has been entrusted to TresVista by that Company/personnel under non-disclosure agreements and other relevant contracts
  - This classification applies to the most sensitive business information that is intended strictly for use by specified departments in the Company and its unauthorized disclosure could adversely impact the Company, Employees, and Clients

- All personal and sensitive personal data is treated as confidential information and accordingly labelled as confidential. This information is made available only on need-to-know basis within TresVista (e.g., Employee information, department specific files, etc.)

Classification and Labelling of Data

- IT administrators in consultation with the data owners appropriately classify data and accordingly mention this information in the data classification matrix
- IT administrator only classifies data based on drive access rights and basis the classification and data details, it is the responsibility of the data owner to further classify and label the data
- The onus is on IT administrators to ensure that data is provided to the specified departments or specified personnel within or outside the Company as the case may be, on the basis of the data classification matrix and the necessary approvals are sought from the data owner

Reclassification of Data

- The classification of data is evaluated by the IT administrator in consultation with the data owner, to ensure that the assigned classification is still appropriate based on changes to legal and contractual obligations as well as changes in the use of the data or its value to the Company
  - Changes are accordingly made to the data classification matrix
- Conducting an assessment on a quarterly basis is encouraged however, the data owners should determine and inform the IT administrator of the appropriate frequency based on the available resources
- If a data owner determines that the classification of a particular data set has changed, then in consultation with the IT administrator, an analysis of security controls should be performed to determine whether existing controls are consistent with the new classification
- If gaps are found in existing security controls, they are promptly corrected in relation to the level of risk presented by the gaps
- At all times, it is the responsibility of the data owner to label data accordingly

Responsibility of the Recipient

- All Employees who receive confidential, restricted, internal, or public data as defined above are expected to familiarize themselves with this data classification policy and to use these guidelines in their daily business operations
- This document provides a conceptual model of information security for classifying information based on its sensitivity, and an overview of the required approaches to protect information based on these same sensitivity classifications

Compliance

- Data stored on the centralized servers/storage are managed and monitored only by IT administrators
- The Compliance department verifies adherence to this process through various methods, including but not limited to internal audits on a periodic basis

Non-Compliance

Any non-compliance with the aforementioned policy may result in disciplinary action

20. Incident Management Policy

The purpose of this policy is to define the process of reporting interruptions in the daily operations of the Company due to unplanned events or incidents (e.g., security/data breach, system failure, cybercrimes, presence of suspicious person in the premises, unattended documents, etc.). For personal data breaches affecting UK based data subjects, Employees should also refer to the Data Breach Policy in the UK Employee Addendum.

Applicability

This policy applies to all the Employees of TresVista including full-time, part-time, and interns, whether permanent or temporary.

Particulars

- **Procedure:** This policy outlines the procedure for managing:
  - Incidents that may occur within/outside TresVista premises, including those that involve service users, Employees, visitors, vendors, etc.
  - Incidents that have occurred and those that are considered a 'near miss'
- **Incident:** Incident is an event, adversely affecting the business operations or becomes a threat to the Company. Some examples of incidents are mentioned below (including but not limited to):
  - System/application failure
  - Unauthorized access to system/networks
  - Cybercrime
  - Loss/theft of mobile handsets
  - Virus attacks
  - Theft and damage to Company's proprietary equipment
  - Documents carried outside office premises without prior approval
  - Misplaced or missing portable media containing client/Company proprietary data

- Inadvertently relaying passwords
- Breach of any policy mentioned in this handbook

Responsibility

- **Employee:** Employees are required to report all incidents (including potential or suspected incidents) as soon as they become aware of it
- **Line Manager:** In the event of an incident involving an Employee or another person within their team and/or area of responsibility, line Managers are required to ensure that the incident is reported centrally, conduct an investigation where appropriate/necessary, and take an action as outlined under this policy
- **Compliance Department:** The Compliance department has the ultimate responsibility of safety and risk management within the Company and will ensure that all incidents are dealt with appropriately

Incident Reporting Process

- **Reporting**
  - All the incidents are reported via a Helpdesk ticket under appropriate category to the respective incident response teams (IT, FMS, HR, and Compliance)
  - Contractual and third-party Employees should report incidents to their line Managers who in turn should raise an incident on the Helpdesk
  - Physical security related incidents, unintentional security breaches and any other policy breaches should be reported to the Compliance Department
  - All information security incidents (e.g., system breakdown, intranet portal not working, etc.) should be reported and notified to the IT department
  - All information security breaches (sharing of password, unauthorized access etc.) should be reported and notified to the IT and Compliance departments
  - Employees should observe and report suspected incidents at the earliest possible
- **Incident Evaluation/Severity:**
  - On intimation from Employees, the incident is evaluated by the incident response team who determines the severity based on the five (5) grades
    - P1 – Critical: Incident that will have significant impact on all Employees and functioning of business operations
    - P2 – High: Incident that will have impact on a group of users/particular teams/SVPs who are not able to do their job which is time sensitive

- P3 – Medium: Incident that will have impact on individual users who are not able to do their job which is time sensitive
- P4 – Low: Incident that will have impact on individual users/particular teams who are not able to do their job which is time sensitive
- P5 – Very Low: Incident that will have no impact on individual user/teams/business

- The severity of an incident is used in determining the priority for resolution

- **Incident Response/Resolution Time:** All the Incidents must be reported and resolved by the concerned teams based on priority mentioned below:

Priority Code	Description	Target Response Time	Target Resolution Time
P1	Critical	15 mins	1 hour
P2	High	1 hour	2 hours
P3	Medium	1 hour	4 hours
P4	Low	2 hours	8 hours
P5	Very Low	3 hours	1 day

- **Priority Determination:** Priority given to an incident determines how quickly it is scheduled for resolution and priority is assigned basis severity of the incident and its impact on the business

Change Priority			Urgency		
			3 - Low	2 - Medium	1 – High
			Issue prevents the Employees from performing a portion of their duties	Issue prevents the Employees from performing critical time sensitive functions	Service or major portion of a service is unavailable
Impact	3 – Low	No impact on business	P5 –Very Low	P4 – Low	P3 – Medium
	2 –Medium	Multiple personnel in one physical location	P4 – Low	P3 – Medium	P2 – High
		Degraded service Levels or able to perform only minimum level of service			
		Moderate impact on business			

	1 – High	All users of a specific service	P3 – Medium	P2 – High	P1 – Critical
		Personnel from multiple teams are affected			
		Client facing service is unavailable			
		Significant impact on business			

- **Incident Investigation and Resolution**
  - Respective incident response team must carry out a detailed investigation to identify the cause of the incident and seek suitable resolution based on the investigation
  - Once the Critical incidents (P1) have been dealt with and closed, the team should notify the Compliance department about the incident resolution
  - A root cause analysis of the incident is done and recorded in the incident log on Helpdesk for future references and learning
  - Log-sheet shall be extracted from the Helpdesk on a quarterly basis to review successful resolution of the incidents within the timelines mentioned in this document and to ensure that all policy breaches captured in the logs are recorded, dealt with accordingly and suitable actions are taken as per the Consequence Management process

Escalation Matrix

The incident is escalated to the following authorities of the respective incident response team in case of any delay in resolving it, basis impact of the said incident

Department	Level one	Level Two	Level Three
Compliance	Compliance Department requests.compliance@tresvsia.com	Compliance Department vandana.pandey@tresvista.com	Compliance Department nilay.vyas@tresvista.com
Compliance Department	IT Department IT@tresvista.com	IT Department bhanukiran.salunkya@tresvista.com	IT Department

			abdulbari.ansari@tresvista.com
Human Resources	HR Department businesspartner@tresvista.com ops@tresvista.com	HR Department charmi.shah@tresvista.com shruti.tendulkar@tresvista.com	HR Department faraaz.lodhi@tresvista.com isha.vashistha@tresvista.com
Facilities Management Services (FMS)	FMS Department FMS@tresvista.com	FMS Department pooja.chawla@tresvista.com	FMS Department abdulbari.ansari@tresvista.com

Record Maintenance

- Record of all incidents are maintained by the Compliance department
- Reports showing statistics of incidents resolved/unresolved are presented by the Compliance department to the Management on a quarterly basis, highlighting the critical priority (P1) incidents, key learnings and corrective actions taken

Non-Compliance

Any non-compliance with the aforementioned policy may result in disciplinary action.

21. Acceptable Usage Policy

The purpose of this policy is for the firm to provide Employees access to email facility and intranet, in order to boost Employee efficiency and streamline interaction with colleagues, customers, and business partners. This policy defines and educates Employees about the boundaries of responsible behavior, the scope of acceptable use detailing the protection of user's rights, and the consequences of violating those boundaries. This policy is designed to protect TresVista against issues like unauthorized use of facilities which can lead to serious consequences in the form of wasted resources, reduced Employee morale, risks arising from diminished corporate reputation, and compliance issues, etc.

Applicability

This policy applies to all users including Employees including having access to Information and IT resources in TresVista.

Particulars

- Employees must agree to the terms and conditions set forth in this policy
- The activities mentioned in this policy are prohibited

- Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services)
- Under no circumstances, an Employee of TresVista is authorized to engage in any activity that is illegal under local, state, national and/or any applicable law of the land and/or international law while utilizing TresVista owned resources
- The activities mentioned below are by no means exhaustive, but attempt is to provide a framework for activities which fall into the category of unacceptable use

Information Disclosure and Handling of Data

Employees are required to:

- Be accountable and responsible for judicious and ethical use of the TresVista information and IT resources
- Ensure that their actions do not compromise the security of TresVista information assets and resources and comply with the IT Security and other related policies of the organization
- Access only authorized resources, and utilize IT resources only for business purposes
- Treat all TresVista data as a valuable asset and protect it accordingly
- Comply with non-disclosure and confidentiality agreements that TresVista has entered into
- Inform the Compliance department and their Managers immediately, in case they accidentally come across unsecured sensitive information that could affect client interest
- Follow the data classification policy and manage data accordingly
- Not discuss and/or transfer any TresVista related information with anyone who is not authorized to have access to it
- Not access any information which does not pertain to their business operations
- Not copy, collect, or propagate any TresVista data or documents outside the network

Work Area Security

- All Employees are required to comply and cooperate with spot checks and audits
- Employees are responsible for visitors, contractors and clients that they bring to the office premises
- It is an Employee's responsibility to immediately inform their Managers and raise an incident with the Compliance department in case they come across any unauthorized person
- Employees must not access areas that are designated as restricted, unless they are authorized to do so

System Security

The following points are applicable to all except third party Employees:

- Desktop ownership lies with the IT department and data ownership rests with the respective Employee

- Employees must not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of or access to any TresVista IT assets
- Employees must secure data on their systems by using passwords (power-on, screensaver password etc.) and ensure compliance with the password policy
- Employees must not reveal account passwords to others or allow others (including family and other household members) to use their account
- Employees must not leave any confidential information on their system unattended
- Employees must not keep liquids or magnets on or near computer equipment
- Employees are not permitted to remove or transport computers from the office premises without the necessary permissions
- Employees must not transport removable media's back and forth between home and office

Software Security

The following points are applicable to all except third party Employees. Employees must not:

- Download shareware or freeware from the internet, unless or otherwise authorized to do so
- Use TresVista software for personal use
- Install personal software on Company devices
- Copy, collect, propagate TresVista software onto an external network
- Distribute software or fonts to clients, customers, vendors, and other persons who are not Employees of TresVista

General Security Guidelines

The following activities are strictly prohibited, with no exceptions:

- Employees must not circulate, store and create obscene, vulgar, or inappropriate materials, jokes, pictures, chain letters etc. in any media/form
    - In case any Employee receives such material, they must immediately remove the material, and inform incident management response team
- Employees must not use or aid by any means attempts to thwart access rights like stealing IP, hacking etc.
- Employees must not indulge in any activity that violates local, state, national and international applicable laws and information security policy of TresVista, during their association with TresVista
- Employees must not introduce any malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.)

- Using TresVista computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction
- Making fraudulent offers of products, items, or services originating from any TresVista account
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties
- Port scanning or security scanning is expressly prohibited unless with prior notification
- Executing any form of network monitoring which intercepts data not intended for the Employee's host, unless this activity is a part of the Employee's normal job/duty
- Circumventing user authentication or security of any host, network or account
- Interfering with or denying service to any user other than the Employee's host (for example, denial of service attack)
- Using any program/script/ command or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the internet/ intranet/extranet
- Providing information about, or lists of, TresVista Employees to parties outside TresVista
- Coveting information gathering on or of the Company assets and business activities
- Exporting software, technical information, encryption software, or technology, in violation of international, regional, or local laws
- Leaving equipment unattended without appropriate protection or security
- Leaving desktop or any information processing facility without locking the user account
- Effecting security breaches or disruptions of network communication including, but not limited to:
    - Accessing data of which the user is not an intended recipient or logging into a server
    - Account that the user is not expressly authorized to access unless these duties are within the scope of regular duties
    - Interfering with or denying service to any user other than the Employee's host (for example, denial of service attack)
    - Executing network sniffing, ping floods, packet spoofing, denial of service and forged routing information for malicious purposes
    - Attempt to test a suspected weakness in the environment without authority
    - User must always raise a service request for any change

Non-Compliance

Any non-compliance with the aforementioned policy may result in disciplinary action.

22. IPR Policy

The purpose of this policy is:

- To provide a comprehensive single window reference system for all intellectual property rights issues relating to intellectual property generated at TresVista
- To safeguard the interest of creator of intellectual property and provide fair distribution of returns accruing from the commercialization of IPR
- To provide legal support, wherever necessary, to defend and protect the intellectual property rights obtained by the Organization against any infringement/ unauthorized use

Applicability

This policy applies to all Employees of TresVista including full-time, part-time, and interns, whether permanent or temporary.

Scope

This policy covers all rights arising from intellectual property devised, created, or made by the staff in the course of their employment by TresVista irrespective of the eligibility of these rights for registration. The IP arising from business research includes patents, designs, trademarks, service marks, copyright, know-how and undisclosed information.

Particulars

Intellectual Property and Ownership

- **Copyrights:**
  - If the work is produced during the course of sponsored and/or collaborative activity, specific provisions related to intellectual property, made in contracts governing such activity, shall determine the ownership of intellectual property
  - The organization shall be the owner of the copyright of work, including software, created by the personnel during the course of their employment and/or with significant use of organization resources. The organization may demand assignment of the copyright in whole or in part depending on the degree of organization-supported resources used in producing the copyrightable work
  - The organization shall be the owner of the copyright of work produced by non-organization personnel associated with any activity of the organization with the intellectual contribution of the organization personnel. However, the authors shall have the right to use the material in her/his professional capacity

- **Invention(s), Design(s) and other creative work(s):**
  - For invention(s) including software, design, and other creative work produced during the course of sponsored and/or collaborative activity, specific provisions related to intellectual property made in contracts governing the collaborative activities shall determine the ownership of intellectual property
  - Invention(s) including software, design, and other creative work produced by the organization personnel without significant use of the organization resources and not connected with the profession for which he/she is employed at the organization shall be owned by the creator(s)
  - The organization shall be the owner of all invention(s) including software, design, and other creative work, created by a team of the organization and non-organization personnel associated with any activity of the organization
  - Non-organization personnel, who create invention(s) including software, design, and other creative work at the organization without any intellectual contribution of the organization personnel and significant use of the organization resources, shall be the owner of the invention(s)
  - Except as stipulated above, the organization shall be the owner of all invention(s) including software, design, and other creative work, produced by the organization

- **Patents:** This section refers to intellectual property that is patentable or protectable by confidentiality agreements
  - The organization will not require being assigned to it the intellectual property created by the creator(s) where there is the use of usual organization resources only
  - The organization will require being assigned to it such intellectual property as is created by the creators using organization-supported resources. In this case, the organization will take steps to commercialize the property through patenting or agreements. Where a patent is applied for, the creator shall agree to maintain all relevant details of intellectual property secret and confidential until the patent application is filed. In the case of protection through confidentiality, the same information will be kept secret and confidential as long as the intellectual property has commercial value. The creator shall furnish such additional information and execute such documents from time to time as may be reasonably requested for effective protection and maintenance of proprietary rights of the organization in the intellectual property
  - The creators of organization-owned intellectual property shall retain their right to be identified as such unless they specifically waive off this right in writing

- **Trade Mark(s)/Service Mark(s)**
  - The ownership of trademark(s)/ service mark(s) created for the organization shall be with the organization. In cases of all IP produced at the organization, the organization shall retain a non-exclusive, free, irrevocable license

to copy/ use IP defined activities, consistent with the confidentiality agreement(s), if any, entered into by the organization

- The authorities responsible on behalf of the organization and creators have the responsibility to ensure the following:
  - Any association with the organization implied by third parties is accurate
  - The activities with which the organization is associated with third parties maintain standards consistent with the organization's business purpose

IPR Administration

This policy shall be applicable to all the organization personnel, as well as non-organization personnel associated with any activity of the organization such as but not limited to outcomes of research, consultancy and covers different classes of Intellectual Property - Patents, Designs, Trademarks/Service marks, Copyright, Trade Secret and Undisclosed Information.

Disclosure

When the creators believe that they have generated patentable or commercialize intellectual property using organization-supported resources, they shall report it promptly in writing along with relevant documents, data, and information, to the organization through the appropriate authority. Disclosure is a critical part of the IP protection process for claiming the inventorship. The information shall constitute a full and complete disclosure of the nature, particulars and other details of the intellectual property, identification of all persons who constitute the creator(s) of the property, and a statement of whether the creator believes he or she owns the right to the intellectual property disclosed, or not, with reasons. Where there are different creators of components that make up a system, the individual creators, and their contributions must be identified and treated separately. In the case of the sponsored and/or collaborative work the provisions of the contract pertaining to disclosure of the creative work is applied. By disclosure, the inventor(s) shall assign the rights of the disclosed invention to the organization.

Responsibilities of Departments

Each department head will administer organization policy as defined herein. In particular, each creator must maintain in his or her department records detailing his or her activities in generating intellectual property. Such records must be made available on demand to the organization.

Authority or Contracts

All Commitments, Agreements, Memoranda of Understanding, etc. relating to commercialization or exploitation of organization-owned intellectual property will be granted in the name of the organization.

Obtaining IPR

If the organization opts to protect the creative work, it shall provide an IPR Advisor/Patent Attorney for drafting the IP application as appropriate. The organization shall pay for access to the relevant IP information databases and other associated costs. The inventor(s) shall conduct IP searches, study the present state of the art and provide the necessary inputs to assist in the drafting of the IP application. The Organization shall bear all costs of drafting and file anIP application. If the Organization/creator chooses to file IP applications in other countries, then it shall bear the cost of application and other associated costs. The Organization shall be free to enter into agreements with the overseas organization for protection and licensing of the IP.

23. Escalation Matrix Policy

The purpose of this policy is to detail out the escalation processes followed for various issues such as resource shortage, technical issues, delivery problems and timelines, etc. Having a defined escalation matrix reduces uncertainty about the point of contact during times of distress and helps provide timely resolutions to problems.

Applicability

This policy applies to all Employees of TresVista including full-time, part-time, and interns, whether permanent or temporary.

Particulars

In the case of escalation policies, it is the responsibility of the line Manager to ensure that the necessary analysis have been performed. Listed below are some best practices for better escalation(s):

- The escalation matrix as well as all levels and areas of escalation should be clearly defined and documented at the beginning of the project
- Escalation mechanism to be followed is defined below:

Designation	Level
Analyst and Equivalent	1
Associate and Equivalent	2
VP/EVP	3
SVP	4
Management Committee	5

- Project stakeholders should be aware of the escalation process
- Any escalations should be made to the succeeding level as per the matrix defined in the policy
- Escalation can be initiated when there is a breach of SLA as defined in the Incident Management policy in this handbook. The response time for any escalation is between 0-8 hours and during this escalation, no further action will be taken by the user
- All data points must be thoroughly analysed before the escalation

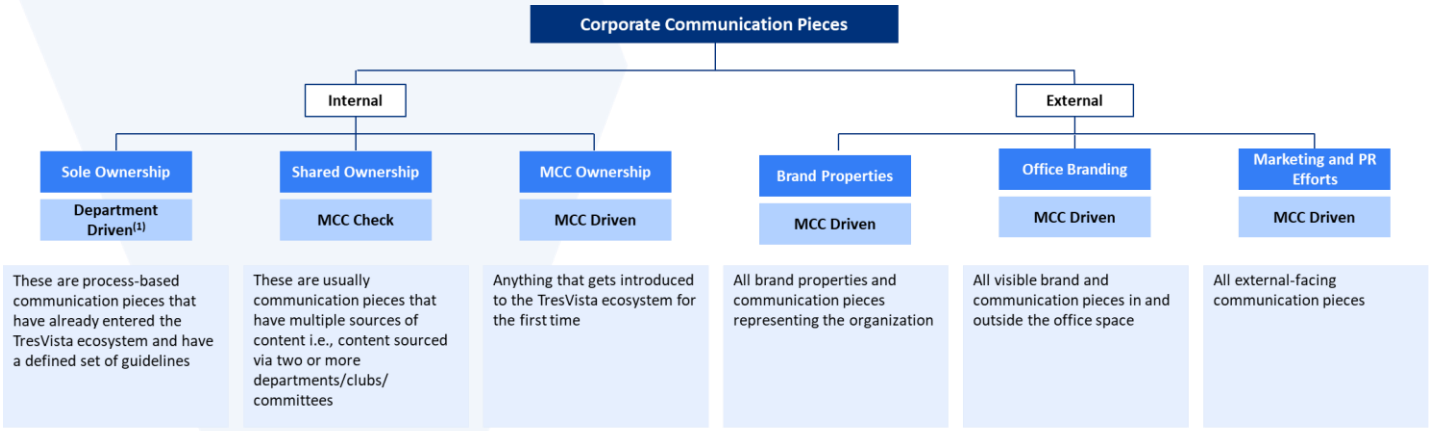
24. Corporate Communication Policy

The purpose of this policy is to define guidelines for internal and external corporate communication pieces and have a central authority to help:

- Standardize messaging & tonality across all communication materials
- Maximize efficiency in planning and execution of corporate communications
- Define a systematic and well-structured chain of action to be followed at any point of time

Particulars

- **Corporate Communication Structure:** The corporate communication structure at TresVista consists of two verticals, namely, internal, and external. For any communication, Employees are required to follow the below defined flowchart



Please note that an internal piece can also have an external branding leg to it
For example, hobby clubs have Sole Ownership when it comes to Yammer posts and Firmwide emails. However, as soon as the department wants to put up an office standee or print customized t-shirts for their club or club event, it becomes an external comms. piece

Examples of corporate communication pieces include but are not limited to:

- **Internal Communication**
  - **Sole Ownership:**
    - Communication pieces falling under this category include process-based communications that are already in practice within the Organization and follow a defined set of guidelines
    - The source for producing this content usually lies with only one team/department and this form of communication does not require another team/department to make a decision
    - These communication pieces do not typically involve determining a new strategy or creative route for executing them
    - This content is communicated to the Firm at defined intervals, depending on the regularity of occurrence
    - Process to be followed:
      - Decide whether a communication material falls under the category of sole ownership
      - Get a signoff from the Head of Department before sending any firmwide communication
      - Follow the brand tonality and guidelines as mentioned in section 1.13 of this Handbook, under the header of people policies
      - Use their discretion to determine whether a communication piece requires a Yammer post, firmwide email, campaign, or a series of posts; depending on the use case

- Be mindful of the target group when sharing information (E.g., If an email is pertaining to Bengaluru, then it should only be sent to the Bengaluru Employees instead of being sent firmwide)
- Follow TresVista Branding for any internal communication pieces/Collaterals that are in collaboration with any organizational Partner
- Reach out to the Marketing and Corporate Communications (MCC) department for any communication regarding policy/process changes or in case there is any doubt/uncertainty at any point of time, the team will accordingly inform Employees whether MCC approval is required in a particular scenario
- New initiatives, templates, or campaigns will not fall under this category, and guidelines listed below under the category of shared ownership and MCC ownership will have to be followed (E.g., Pre-decided templates for Spotlight that go on Yammer on a regular basis will only need approval from the Head of Department, however, if there is a need to revamp the template, it will fall under the purview of the MCC department)

- **Shared Ownership:**
  - Communication pieces falling under this category include those that receive content from multiple sources i.e., content sourced via two or more teams/departments/clubs/committees
  - Even if only one team/department is the source of content, the nature of this bucket requires a holistic view due to its larger impact on the Firm or brand implications
    - The communication material in this regard may be recurring, however, it will need a fresh perspective every time
  - This category includes communication to departments, functions, Firm or exchange of critical information to specific forums or the Firm
  - This form of communication consists of crucial information that requires cross-checking and its brand impact requires the MCC department to help in planning the communication strategy and crafting the final message
  - Any communication material that involves campaign planning, communication strategy, and/or creative messaging to the Firm or forums will fall under this category
  - Process to be followed:
    - For cross-checking communication materials, reach out to the MCC department at least 1 week in advance and account for a buffer time to incorporate feedback

- Any change suggested by the MCC department will be in reference to corporate communication, tonality, branding, user experience standardizing organizational information, and sensitivity of the information
- MCC department may raise information present in these materials to Management for strategic guidance, on need basis

- For campaigns, special occasions, events, one of the 2 options mentioned below must be followed:
  - **Option 1:** Reach out to the MCC department for final checks/approvals
    - Share the required details on campaign idea/plan, creatives, requirement brief to corroborate MCC department's inputs, if any, at least 2 weeks in advance
    - The team will revert on the status and timeline for proceeding with the project/communication piece
    - If the project/communication piece receives initial approval, inputs/feedback provided by the MCC department will need to be incorporated and the final deliverable has to be shared with them for approval
  - **Option 2:** Reach out to the MCC department with a requirement brief at least 1 month prior to the initiation of the project/communication piece
    - The team will revert on the status and timeline for proceeding with the project/communication piece
    - If the project/communication piece receives initial approval, the MCC department will share following details via an email within 3 working days: further questions, if any, exact deliverable from their end, timelines for the deliverables, cost, if applicable (in case an external Partner is involved, e.g., leveraging services of the marketing agency)
    - Any project coordination and JRS should be raised by the respective team/department to the Design team keeping the MCC department marked on the communication and the team will share their inputs/guidance, where required
    - In case of any queries, Employees can reach out to the MCC department and the team will inform Employees whether their approval is required in a particular scenario

- **MCC Ownership:**
  - Communication pieces falling under this category include material/projects being introduced to the Company for the first time (e.g., New initiatives, campaigns, and internal brand properties)
  - Process to be followed:

- Reach out to the MCC department at least 3 months in advance for any brand properties, campaigns, and new initiatives
- The team will revert on the status and timeline for proceeding with the project/communication piece
- If the project/communication piece receives initial approval, the MCC department shares the following via email within 1 working week: further questions, if any, exact deliverable from their end, timelines for the deliverables, cost, if applicable (in case an external Partner is involved, e.g., leveraging services of the marketing agency)
- JRS should be raised by the respective team/department to the Design team keeping the MCC department marked on the communication and the team will share their inputs/guidance, where required
- In case, respective teams/department has any feedback; a call is setup to discuss it further however, the final decision lies with the MCC department, keeping in mind the use case and impact
- The MCC department will subsequently share the final deliverable with the respective team/department

- For any communication regarding policy and process changes or in case of any queries, Employees can reach out to the MCC department, and the team will accordingly inform Employees whether MCC approval is required in a particular scenario

- **External Communication**
  - Any external facing property that represents TresVista in any form falls under this category
    - Examples include but are not limited to external awards, recognition, and milestones (for Organization and Employees), corporate gifting, brand campaigns and properties – external campaign/communication on online and offline platforms, logos, mascots, videos, identities, merchandise, brand assets – Website, thought leadership pieces, social media, digital platforms, any formal or informal media or Promotional interaction, including interviews, providing a quote/testimonial to any Organization or Partner, delivering a lecture, or conducting a workshop/session/panel discussion and public speaking opportunities

- There might be several use cases that will be internal in nature as well however, at any point if they have an external branding associated with them, teams/departments will have to follow the guidelines provided below (E.g., A hobby club firmwide email is internal but an office standee will fall under external branding and hence will follow the below guidelines)
- Process to be followed:

- Employees must reach out to the MCC department in case the requirement falls under the below defined categories:
    - Any team/department/ that wants to use TresVista Branding, including Logo, pennant, values, or any organizational information for external purposes must send an email with the exact use case (where TresVista is to be used in any way) at least 1 (one) month in advance
    - For external campaigns, creation of a brand property, and logo, the department must reach out with a requirement brief at least 2 months before the initiation date, although it is recommended that they reach out 3 months in advance

- MCC department will revert on the status and timeline for proceeding with the project/communication piece
- If the project/communication piece receives initial approval, the MCC department shares the following via email within 1 working week: further questions, if any, exact deliverable from their end, timelines for the deliverables, cost, if applicable (in case an external Partner is involved, e.g., leveraging services of the marketing agency)
- JRS should be raised by the respective team/department to the Design team keeping the MCC department marked on the communication and the team will share their inputs/guidance, where required
- The MCC department will subsequently share the final deliverable with the respective team/department
- Marketing budget expensed, if any, will be attributed to the respective department budget
- Teams/departments are required to assign a certain amount towards the marketing budget for the upcoming financial year which will be transferred to the MCC department at the end of the respective year, depending on the deliverables
- In case of any queries, Employees can reach out to the MCC department and the team will inform Employees whether their approval is required in a particular scenario

- **Marketing and Communication Guidelines for Partners**
    - At the time of onboarding a Partner, departments are required to share TresVista logo files along with the linked document with the Partners the path of the same is: TresVista Common (SharePoint) > Standard Organizational Materials > Partnership Guidelines
    - Department/teams must reach out to the MCC department if a Partner requires any of the following details:
        - A quote or any other information from TresVista
        - Mention TresVista as a Partner on any platform or state that they are affiliated with TresVista in any way
        - Use the Company's logo, name or any information related to TresVista in any of their communication pieces
        - Tag TresVista or its Employees on any online platform

- Partner's poster/Collateral/marketing material is going to be circulated in TresVista (In such cases, the material needs to adhere to TresVista brand guidelines)

- Once a request is received from a department, the MCC department will first check the feasibility of proceeding with the aforementioned communication/request and share their inputs within 5 working days
- Depending on the nature of the request, the MCC department will revert with the expected turnaround time for the deliverable and the required approvals/feedback, if applicable

Non-Compliance

Non-compliance with the policy, in any form, shall lead to Disciplinary Actions including, but not limited to policy reminders, warning letter, or Termination with Cause, at the discretion of the Company.

Glossary

1. **Account Lockout Strategy:** A method to restrict user's account after a defined number of failed password attempts and to prevent the user from logging onto the network for a certain period of time
2. **Accrual:** The accumulation or increase of something over time, especially payments or benefits
3. **Annual Review Period:**
    - July 01 to June 30
    - January 01 to December 31
4. **Arrears:** Employees are not entitled to receive any amount till the required documents are submitted
5. **Bonds:** Investment securities where an investor lends money to the Company for a set period of time, in exchange for regular interest payments

6. **Child:** Biological, adopted, foster, stepchild, legal ward, a child of domestic partner, or a child to whom the Employee stand in loco parentis
7. **Client:** Persons or entities to which the Company has sold any products or for which the Company has performed any services
8. **Collateral:** Any canvas or space (digital or offline) that acts as the background for the TresVista brand, trademark, name, tagline and/or logo to be incorporated along with any associated branding element of TresVista, such as committee or club logos/names, department and function names, and organizational information
9. **Commercialize:** Manage or exploit in a way designed to make a profit
10. **Company/Organization/Firm/Employer:** TresVista and its subsidiaries and affiliates as below under "TresVista"
11. **Confidential Information:**
    - All Company and third party information which is proprietary and not available to the general public and shall include but not be limited to plans, client lists, budgets, funds and investments, products in development, portfolio management strategies, tools and procedures, finance issues, marketing strategies, personnel records, information technology, board and executive structures and methods of conducting meetings
    - Knowledge, technical data, trade secrets, confidential commercial information relating to the business finances or affairs of the Company or third party
    - Inventions accessed, created, received, exploited, developed or obtained by the Employee during the course of employment with the Company
    - Any information, data and materials of whatever nature, whether or not stored in any medium and/or disclosed orally or in writing by the Company, its affiliates, agents, partners, suppliers, clients, contractors and consultants including, but not limited to, information about equipment, software, designs, samples or technology, trade secrets, commercially sensitive information, business plans, personal data (including sensitive personal data), technical documentation, business information, product or service specifications or strategies, marketing plans, pricing information, financial information, information relating to existing, previous and potential customers, contracts and products, inventions, unreleased software applications, methodologies and other know-how, drawings, photographs, models, mock-ups, and design and performance specifications, production volumes, and production schedules, together with any notes, summaries, reports, analyses, or other material derived or developed by the Company or the Employees, in whole or in part
    - Any documents or information, which reflect or are generated from any such Confidential Information, will also be deemed as Confidential Information

- All Confidential Information shall be deemed as the Company's trade secrets

12. **Copyright:** The exclusive and assignable legal right, given to the originator for a fixed number of years, to print, publish, perform, film, or record a given material
13. **Confirmation:** Upon successful completion of probation, an Employee may get confirmed as per the clause mentioned in the offer letter
14. **Corporate Accounts:** Any social media account procured and paid for by TresVista for the purpose of business activities and requirements
15. **Contractual Employees:** The Employees retained by a Company for a predetermined time and renumeration
16. **Debenture:** A marketable security that the Company can issue to obtain long-term financing without needing to put up collateral or dilute the equity
17. **Dependent Parents:** Any legal guardians, or legally verifiable mother and father, whether biological or otherwise, of an Employee who are emotionally, physically or financially dependent on the Employee for the purpose of their subsistence. For the purpose of this policy, dependent parents shall not include in-law relatives of an Employee
18. **Developments:** Any idea, Invention, design, technical or business innovation, computer program and related documentation, or any other work product developed, conceived, or used by the Employee, in whole or in part that arises during employment with the Company, or that are otherwise made through the use of the Company's time or materials
19. **Disciplinary Action:** This indicates any action that can be taken on the completion of investigation and disciplinary proceedings including but not limited to a warning, final written warning, imposition of fine, suspension from official duties or any such action as is deemed to be fit considering the gravity of the matter
20. **Employee:** All individuals who are directly employed by Tresvista, including but not limited to those who are on probation, notice period, etc. in accordance with the terms of their respective employment agreements
21. **Employment Agreement, Employment Contract or Offer Letter:** The agreement that specifically sets out the terms and conditions, and the scope of employment of the Employee at TresVista
22. **Employee Handbook:** A defined document and all its annexes, schedules and instruments supplemental to or amending, modifying or confirming the handbook (if any) in accordance with the provisions of the employment agreement and offer letter

23. **Family members:** Family members include the Employee's child, parent, grandparent, grandchild, spouse, or domestic partner. The definition of parents includes the Employee's biological, foster or adoptive parent, a parent-in-law, a stepparent, a legal guardian, or another person who stood in loco parentis to the Employee when the Employee was a child

24. **Fraud:** Any concern raised by written communication that discloses or demonstrates information that may act as evidence for unethical or improper activity. This term applies to both internal and external fraud and is used to describe offenses including, but not limited to, deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts, collusion perpetrated for personal profit or to gain some unfair advantage. It further includes the following:

- Intentional, false representation or concealment of a material fact to induce another to act upon it to his or her injury
- False accounting: Dishonestly destroying, defacing, concealing, or falsifying any account, record, or document required for any accounting purpose
- Knowingly providing false, deceptive, misleading, or incomplete information within business/functions, to its partners, or other business relations, or deliberately failing to provide information where there is an obligation to do so
- Disclosing confidential, sensitive, or proprietary information to internal or external parties
- Forgery of any document, cheque, bank draft, or any other financial document or account that belongs to TresVista
- Alteration, destruction, or removal of any document, cheque, bank draft, or any other financial document or account that belongs to TresVista, unless instructed to do so by the organization
- Misappropriation of funds, securities, or misuse or destruction or removal of supplies, or other assets of TresVista including computers, vehicles, machines, mobiles, furniture and fixtures, equipment, or any other property, or services outside of professional duties or without specific authorization
- Impropriety in the handling or reporting of money or financial transactions
- Making unfair profits due to insider knowledge of Company activities
- Accepting or seeking any offering that may influence the action of any person such as taking inducements, gifts, anything of material value or favours from contractors, vendors, or persons providing services/ materials to TresVista. For the approval matrix refer to the Gift Policy defined in section 9 of this Handbook, under the header of risk policies
- Any similar or related inappropriate conduct

25. **FMS Support Staff:** Employees on TresVista's payroll, hired for facility management and operations
26. **Geospatial Tagging:** The process of adding geographical identification metadata to various media such as a geotagged photograph or video, websites, SMS messages, QR Codes or RSS feeds and is a form of geospatial metadata
27. **Financial Services:** All Employees who provide financial services
28. **Firm-wide Holiday:** Firm-wide holidays, or day offs as declared by the firm
29. **HR Department:** All Employees in the human resource teams at TresVista
30. **Information Security Management System:** A set of policies and procedures to manage information security risks in a structured and systematic way to protect confidential, personal, and sensitive data from being compromised
31. **Intellectual Property:** Intellectual property means and includes creations and/or information, whether registered or unregistered and/or pending registration of trademarks, patents, designs, copyrights including design copyrights, Inventions, service marks, internet domain names, processes, geographical indications, computer software, Confidential Information, know-how and any research effort relating to any of the above mentioned business, names whether capable of registration or not, moral rights and any similar rights in any country in the world
32. **Internal Audit:** An independent service to evaluate the Company's internal controls, its corporate practices, processes, and methods
33. **Inventions:**
    - Developments, know-how and intellectual property, which an Employee may solely or jointly conceive or develop or reduce to practice, or cause to be conceived or developed or reduced to practice
    - Inventions means and includes whether registered or unregistered and/or pending registration of neighbouring rights, trade secrets, integrated circuits, exploitation of any present or future technologies, applications for any of the foregoing and the right to apply for them in any part of the world; discoveries, creations, inventions, modifications or improvements upon or in addition to an existing inventionEmployee
34. **Know-how:** Any or all information (including that comprised in or derived from information technology of all sectors, electronic intellectual property, manuals, instructions, catalogues, booklets, data disks, tapes, source codes, formula cards and flowcharts) relating to the business of the Company and the products or services and markets therefore, clients of the Company (including, but not limited to, clients with whom the Employees have become acquainted with during the term of their employment), software, developments, inventions, processes, formulas, technology, designs, drawings, engineering, hardware configuration information, marketing, finances or other business information, services provided or products manufactured and developed by the Company

35. **KPI:** Key Performance Indicator

36. **Law:** All laws, byelaws, rules, regulations, orders, ordinances, protocols, codes, guidelines, policies, notices, directions, judgments, decrees or other requirements or official directive of any governmental authority or person acting under the authority of any governmental authority and/ or of any statutory authority that are applicable to TresVista and/ or its Employees

37. **Leave Balance:** Total number of leaves allotted to the Employees in the given leave cycle

38. **Leave Cycle:** January 01 to December 31

39. **Management:** The managing directors, and any other authorized Employee of TresVista

40. **Manager:** Supervisor of an Employee, or any individual designated as such by the organization from time to time. For the purpose of this document, Managers refers to VPs and above, as applicable, unless mentioned otherwise

41. **Material Information:** Any information about the client Company that a reasonable investor would consider important in the decision to buy, hold, or sell securities of the client Company is considered as material information

42. **Non-Disclosure Agreement (NDA):** A legally binding contract between the Company and the Employees that prevents sensitive information from being shared with unauthorized personnel

43. **Non-public information:** Any information about the client Company that has not been publicly disclosed is considered as non-public information

44. **Notice Period:** The party who is terminating employment will give to the other advance notice in writing, with such notice not to be less than the period indicated in the Employee's offer letter or as specified in subsequent promotion letters (subject to applicable statutory minimum notice requirements)

45. **Opportunity:**

    - Any prospective client; or
    - Any private equity or private debt or asset backed security, or structured finance or real estate opportunity which is offered to or under consideration by any Employee of the Company for the Company or any person for which the Company provides advisory, consultancy or management services

46. **Partner:** Partners include but are not limited to vendors, clients, campuses, CSR partners, institutions and any third parties who are not affiliates of TresVista or the TresVista group of companies

47. **Patent:** A government authority or license conferring a right or title for a set period, especially the sole right to exclude others from making, using, or selling an invention

48. **Permanent Employees:** The Employees who work for and are directly on the payrolls of TresVista without a predetermined end date for the employment at hand
49. **Perpetrator:** One against whom allegations of sexual harassment have been proved, based on the Inquiry conducted by the IC
50. **Person:** An individual, firm, limited partnership, limited liability partnership, Company, association, corporation or other organization
51. **Personal Account:** Any social media account created by Employees for their personal use
52. **Personal Data:** Personal data means any information relating to an identified or identifiable natural person such as name, online identifiers (such as an IP address), mental, economic, cultural or social identity and location data of that person
53. **Personal Day:** A day that an Employee is not present in the office as stated in the section 2.2 of this handbook, under the header of people policies
54. **Policy Handbook:** A defined document and all its annexes, schedules and instruments supplemental to or amending, modifying or confirming the handbook (if any) in accordance with the provisions of the employment agreement and offer letter
55. **Podcasting:** The practice of using the internet to make digital recordings of broadcasts available for downloading to a computer or mobile device
56. **Probation:** Period during which a Manager closely evaluates the progress and skills of a newly hired Employee, determines appropriate assignments and monitors other aspects of the Employee
57. **Product:** Any financial services related work including but not limited to valuation, investment research; industry landscaping, due diligence, financial modelling, investment recommendations, consulting, portfolio management, capital raising, and M&A advisory services, or any other work the Company performs for its clients
58. **Promotion:** The recognition of an Employee's effort, work contribution, and success. The Employee's designation and compensation structure will change with effect of a promotion
59. **Prospective Client:** Persons to which the Company has:
    - Maintained or established contact or other information regarding that person for the purpose of soliciting or potentially soliciting the sale of any products

- Solicited for the purpose of selling any products within the last two (2) years preceding the time of determination as to whether a person is a prospective client for the purpose of this policy

60. **Prospective Employee:** People who are most likely join the Company in the near future
61. **Requisition:** An official order laying claim to the use of property or materials
62. **Resources:** Including but not limited to Company property (tangible or intangible) such as IT facilities, stationery, printing facilities, emails, databases/software, conference rooms, recreation room, pantry, training manuals, fax machines, manpower, etc., whether owned by TresVista or not provided to or used by Employees for the performance of their responsibilities at TresVista
63. **Resource Shortage:** Resource shortage could be absence or unavailability of resources like capacity, IT infrastructure etc. impacting the operational efficiency
64. **Reviewee:** The Employee receiving the review
65. **Reviewer:** All Employees evaluating and giving feedback to the reviewee
66. **Reward program:** Reward programs are the point-based programs loyalty programs designed to increase customer engagement and purchases in exchange for discounts and other benefits
67. **RIS:** Research and Investment Services department is divided into smaller teams
68. **Royalty:** A sum paid to a patentee for the use of a patent or to an author or composer for each copy
69. **Scrip:** A certificate entitling the holder to acquire possession of certain portions of public land
70. **Separation:** It is a process under which an Employee formally notifies their decision to separate from the firm. The process is managed through DarwinBox
71. **Separation Date /Last Working Day:** Last working day of the Employee as approved and notified by the HR Operations team (ops@tresvista.com)
72. **Sensitive Personal Data:** Sensitive personal data (special category data) means any information consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation, etc.
73. **SharePoint:** A common site through which all Employees can access information including but not limited to TresVista handbooks, templates, policies, training manuals, organization chart, etc.
74. **SPOC:** Single point of contact

75. **Subject:** This means a person or group of persons against or in relation to whom fraud is reported or evidence is gathered during an investigation under this policy

76. **Tailgating:** A physical act of security breach in which an Employee enters/leaves the office premises or secured zones without using biometric access

77. **Technical Issues:** Any disruption in the IT infrastructure or software made available by TresVista that can potentially affect the work

78. **Termination Date:** The date on which the termination of an Employee's employment with the Company becomes effective and, for the avoidance of doubt not the date on which notice of termination is given

79. **Third Party:** An individual or an entity who is directly/indirectly involved in an existing business relationship between two parties, of which one is TresVista

80. **Third-Party Resources:** Resources hired by TresVista's sub-contractor

81. **Ticket:** A mode of communication used to raise requests/incidents via the 'Helpdesk Support' module on Microsoft Dynamics 365

82. **Tipping:** Passing or providing access of Material Non-Public Information about a client Company by the Employee to any individual who does not have a confidential relationship with the client Company or have a valid reason to be in possession of such information

83. **TresVista:** TresVista Financial Services Pte. Ltd., TresVista Financial Services Pvt Ltd, TresVista Analytics LLP, TresVista INC, and TresVista UK Ltd. along with their affiliates are collectively referred to as "TresVista"

84. **TresVista Branding:** Any branding material, trademark, tagline, logo/name owned by TresVista (whether registered or not) or presence of TresVista on any offline or digital collateral whether inside or outside the office space

85. **Video on Demand (VOD):** Technology for delivering video content, such as movies and television shows, directly to individual customers for immediate viewing

86. **Whistle Officer**: This means an officer who is appointed as a designated point of contact for internal whistleblowing disclosures and who is responsible for conducting a detailed investigation of the disclosure received from the whistle-blower and recommending appropriate steps, including disciplinary action

Annexure (Monetary Policies)

I. Business Travel: Allowance Limits

II. Particulars	Amount (Pounds)
Accommodation [1]	300
Daily Allowance [2]	100
Host Allowance	100
Conveyance	Actuals
Client Welfare	50
Travel Insurance	Actuals
Food	Actuals

1) Includes accommodation cost per night

2) Food and conveyance cost refers to per day allowance

Annexure (Risk-Oriented Policies)

Personal Account Dealing Declarations

A. FORM – A: INITIAL HOLDING DECLARATION

Department:
Name:
Designation:
In submitting this declaration, I affirm that:
(a) I have read and understood the Personal Account Dealing Policy of the Company
(b) I agree to be bound by the Personal Accounts Dealing Policy so long as I remain an Employee of the Company
(c) At present, I am/ my connections deal in securities as defined in the Personal Accounts Dealing Policy and are operating _____ (mention number) trading account(s).
At present, I am/ my connections do not deal in securities as defined in the Personal Accounts Dealing Policy
Following are the details of the account(s):

Beneficiary Name	Client ID / Customer Account Number	Bank / Broker Name	DP ID

Declaration:
I hereby confirm that, all the information given by me is true and correct and I undertake to notify you immediately of any change in the above facts. I also confirm my understanding that I may be subject to disciplinary action, up to and including termination of my employment, for any false or tampered submission.
Place: Date:

B. FORM – B: DISCRETIONARY PMS DECLARATION

Department:
Name:
Designation:
I, hereby declare that vide agreement dated _____, I maintain my portfolio under Discretionary PMS with _____ (Name of firm). I hereby further declare that all the trading activities undertaken in the said account are solely done by Mr. /Ms. _____ (name) and I do not have any involvement in the investment decision(s).
Declaration:
I hereby confirm that, all the information given by me is true and correct and I undertake to notify you immediately of any change in the above facts. I also confirm my understanding that I may be subject to disciplinary action, up to and including termination of my employment, for any false or tampered submission.
Place: Date:

C. FORM – C: TRADING ACCOUNT OPENING/CLOSING DECLARATION

Department:
Name:
Designation:

I_____ (Name), hereby declare that I have / my connections have opened/closed the below mentioned trading account (s).

Beneficiary Name	Client ID / Customer Account Number Opened/Closed	Bank / Broker Name	Trading Account Opening / Closing Date

Declaration:

I hereby confirm that, all the information given by me is true and correct and I undertake to notify you immediately of any change in the above facts. I also confirm my understanding that I may be subject to disciplinary action, up to and including termination of my employment, for any false or tampered submission.

Place: Date:

D. FORM – D: FOREIGN HOLDING DECLARATION

(Note: Please strike off wherever not applicable)

I ---------- (Name), hereby declare that:
(a) I have read and understood the Personal Account Dealing Policy of the Company
(b) I agree to be bound by the Personal Accounts Dealing Policy so long as I remain an Employee of the Company and
(c) At present, I am/ my connections are operating _____ (mention number) trading account(s).

Following are the details of the said account(s):

Beneficiary Name	
Trading Account Number	
Bank / Broker Name	
Bank / Broker Code	

Beneficiary Name	
Trading Account Number	
Bank / Broker Name	
Bank / Broker Code	

(If more than two trading accounts are operational, please provide above details in separate sheet)

Encl: Statement of declaration submitted with respective enforcement agency

In submitting this declaration, I affirm that the information disclosed above is complete, accurate and to the best of my knowledge not misleading.
Signature:
Designation:
Date:

Acceptance of Responsibility from Client for Intimation of Access Revocation

(Email Template)

Dear _____ (Please mention client name).
In accordance with TresVista's compliance requirements, drop box access is only given to the whole domain address and not to personal email ID's. This being an exceptional case we'd request you to nominate a senior authority from your organization to inform us if at all and whenever Mr./Ms._____ (please mention names of Employees) exit your organization so that we can revoke the Dropbox access given to their personal email ID's.

Please revert with your acceptance to this arrangement and a name of the nominated authority.

Thanks for your understanding and co-operation.

Regards,

_____
(Name)

(Designation)