TresVista
Catalyzing Your Impact

Third-Party Resource Handbook

TresVista as an Organization is growing by leaps and bounds. As bigger TresVista grows so does its relationship with different Persons, thereby increasing the number of contractors and subcontractors ("Third Party Resources") that TresVista engages, and is engaged with during the normal course of business. This Third-Party Resources Handbook ("Handbook") is brought into existence to introduce the Third-Party Resources hereinafter referred to as "Third-Party Resources") to TresVista applicable policies and help them to abide by them.

Disclaimer

The Third-Party Resources will be 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.

In order for the policies to remain current and relevant, the Handbook will be revisited at regular intervals and necessary modifications or additions will be made. In such cases, the eligible Third-Party Resources will be informed of any change.

Further, each Third-Party Resource shall be bound to observe and uphold all of the applicable 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 Agreement, the terms of the most recent Agreement shall prevail. Further, subject to Law, all representations and undertakings related to any and all benefits being or to be extended to a third-party resource pursuant to this Handbook are on a best effort basis and may be rolled back at the 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 will attract penal actions.

In case of conflict between this Handbook, the agreement between the Company and the Third-Party Resource's Employer, and the provisions of applicable Laws (now or thereafter), the applicable Laws will take precedence.

In case the conflict persists between the provisions of this Handbook and the agreement between the Company and the Third-Party Resource's Employer, the agreement will take precedence.

Table of Contents

About TresVista

1. About TresVista

1.1 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 the third-party Resources, both with an aspiration to exceed expectations.

This Handbook is applicable to all third-party Resources of TresVista's Indian entities.

1.2 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

1.3 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.'

1.4 Training

TresVista takes responsibility for the growth of its third-party Resources, by providing enriching and valuable opportunities to learn at every stage of their career. Training at TresVista plays a pivotal role in third-party resource 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 is carefully tailored to contribute to the success of the Company through focused learning that is strategic, measurable, and effective for every third-party resource.

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 training 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 third-party Resources across various levels. The objective of the program is to provide each third-party resource 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 third-party Resources of these training sessions in advance. It is mandatory to attend these training sessions and it should be noted that:

- Third-party Resources are required to plan their leaves accordingly
- It is the third-party resource's responsibility to notify the Supervisor in advance to manage work and training sessions
- In case a third-party resource misses training, they must notify the Training department or their Supervisors of the reason for not attending the training

Points to Note

- Team/department/function-specific training manuals are provided to the third-party Resources prior to each session
- Third-party Resources 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 third-party resource's exit, since it is Company property

Conduct and Ethics

2. Conduct and Ethics

Third-party Resources are expected to maintain high standards of professionalism as set by TresVista.

2.1 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 third-party resource(s) to achieve and maintain a high standard of ethics, professional conduct and work performance.

All third-party Resources should note that:

- High ethical standards must be recognized and valued
- Any unethical or illegal behaviour must be reported by the third-party Resources to their Supervisor
- 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 behaviour 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 willcooperate with any legitimate Law enforcement investigation of potential criminal activity

2.2 Adherence to Compliance Manual

TresVista expects all third-party Resources to adhere to the Compliance Manual which is an integral document covering all internal compliance policies of the Company. The third-party Resources are expected to:

- Conform the Compliance Manual and policies written therein, provided to them as a part of engagement terms;
- Be aware of, and adhere to all relevant compliance related policies of the Company during their engagement with TresVista and
- Perform their duties with care and diligence, using authority in fair and equitable manner

TresVista may take actions including, but not limited to, policy reminder, re-training, issuance of warning letter or termination of the engagement with the third-party resource who acts in contravention of TresVista's Compliance Manual and/or policies therein.

2.3 Inventions

The purpose of this policy is to protect TresVista's Intellectual Property rights i.e., to ensure that all third-party Resources of TresVista have appropriately assigned their invention rights and ownership to TresVista.

Policy

- TresVista is not required to designate any third-party resource as the author of any invention during the period of their engagement with the Company
- All Inventions created by a third-party resource during their period of engagement with the Company are exclusively owned, legally and beneficially, by the Company and are dealt with or assigned to account in such manner and/or on such terms as the Company considers appropriate
- In addition, a third-party resource must assign to the Company any rights, title and interest to Inventions created by them when not carrying out their duties, but which are materially connected with those duties and may be of material value to the Company
- A third-party resource must disclose all Inventions to their Supervisor and at the Company's request, must do all things that may be necessary and appropriate to establish a perfect record or document the Company's ownership of the Inventions including, but not limited to, the execution of the appropriate Copyright or Patent applications or assignments, the production of documents and evidence to the appropriate authorities, etc. and assist the Company in taking action in relation to any possible infringements
- All rights, title, ownership, and interest in any Intellectual Property (as defined below) arising out of or in connection with the third-party resource's engagement with the Company, whether or not created, conceived, or developed in the Company's premises or using the Company's property, and all other proprietary rights therein or otherwise subsisting now or in the future, shall vest solely with and be the property of the Company
- The third-party resource will execute all documents and perform all acts at the Company's request, without any additional remuneration or payments of any kind, to establish or preserve the Company's right to such Intellectual Property including execution of deeds of assignment or any other document as may be required during the course of their engagement or at any time thereafter. The third-party resource hereby appoints the Company and its nominated officers as their authorized attorney and agent to execute documents on their behalf for this purpose
- The third-party resource hereby irrevocably and unconditionally waive in favour of the Company all rights granted by the Indian Copyright Act, 1957 in connection with their authorship of any Copyright works in the course of their engagement with the Company, including without limitation any moral rights and any right to claim an additional payment with respect to use or exploitation by the Company of those works. It is clarified that Section 19(4) of the Indian Copyright Act, 1957 shall not apply to any assignment of Copyrights under this Agreement and the third-party resource hereby agrees not to raise and waive all rights to raise, any objection or claim before the Indian Copyright Board with respect to the assignment pursuant to Section 19A of the Indian Copyright Act, 1957
- **It should be noted that:**
  - A third-party resource does not and shall not at any time have any rights, title, or claim in or to any Inventions

- A third-party resource retains no right to use the Inventions. Further, they must not challenge the validity of the Company's ownership of the Inventions
- The decision on whether to Commercialize or market any Inventions developed by a third-party resource solely or jointly with others is within the Company's sole discretion and for the Company's sole benefit
- No Royalty is due to the third-party resource as a result of the Company's efforts to Commercialize or market any such Inventions
- If a third-party resource has any right to the invention that cannot be assigned to the Company as a matter of Law, such as moral rights, author's rights, rights of integrity or any similar rights, the third-party resource must unconditionally and irrevocably waive such rights in the invention, including without limitation, the right to the integrity of the invention that they may enjoy in respect of the said invention, in favor of the Company and further grant to the Company the right to modify the Inventions as the Company deems fit
- Further, a third-party resource must unconditionally and irrevocably waive the enforcement of such rights, and all claims and causes of action of any kind against the Company with respect to such rights, and agree, at the Company's request and expense, to consent to and join in any action to enforce such rights
- The third-party resource's salary is full compensation for their services and all present and future uses of Intellectual Property made by them in the course of their engagement and they will not make any claims against the Company or any of its affiliates with respect to such Intellectual Property; and
- The third-party resource shall not use, reproduce, or share in any manner whatsoever (including through social media) names, logos, trademarks, signs, signifiers or other representations of the Company, its affiliates, Clients, suppliers, and agents without the Company's prior written authorization; and
- The third-party resource shall not violate or infringe or disclose and use without written authorisation any third-party Intellectual Property rights during their engagement with Company
- The provisions of this clause shall survive the termination of the agreement

2.4 Conflict of Interest – Firmwide Applicability

TresVista is committed to conducting business in a manner that ensures Third-party resource'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 Third-party Resources to comply with Company guidelines and make all relevant disclosures to prevent any such conflicts of interest (actual, potential, or perceived)

Eligibility

This policy is applicable to all third-party Resources.

Particulars

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

- Owning more than 1% stake in a 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 engagement leading to monetary benefit:
  - Side business
  - Part-time engagement
  - Weekend jobs
  - Monetary benefit from any engagement 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 a third-party resource has vested interest
- Other types of conflict:
  - Failing to disclose that the candidate, the Company is considering hiring is an immediate blood relative or spouse
  - Failing to disclose information pertaining to immediate blood 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 third-party Resources 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 third-party resource, the steps necessary to resolve the conflict

2. **Procedure**

- Third-party Resources 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
  - Such instances can be raised with the COI Committee via a Helpdesk Ticket or via the following email ID coicommittee@tresvista.com
- 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 third-party resource within one month of the case being presented
  - In the interim, the concerned third-party resource shall refrain from participating or continuing with the conflicting arrangement
  - The third-party resource 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 third-party resource 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 third-party resource. Failure to abide by this may result in Termination with Cause (refer to section 6.1 of this Handbook)

3. Exceptions

- An event or any act of a third-party resource that does not jeopardize the primary interest of the third-party resource 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

2.5 Personal Relationships

Third-party resources 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), favoritism, 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 relationship 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)

Points to Note

- Third-party Resources must avoid any circumstances that could be viewed as a conflict of interest or act as a cause of potential sexual harassment
- Third-party Resources must immediately notify their respective Supervisors 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 third-party resource
  - Belonging to a different team/department
- Upon disclosure, the Company, to the extent possible, takes efforts to accommodate the parties involved via:

- Reassignments/transfers to different teams/departments
- Any other actions, as applicable

- Failure to disclose such relationships may result in Disciplinary Action
- Inappropriate Public display of affection in the office is strictly prohibited

2.6 Anti-Sexual Harassment Policy

TresVista aims to foster a professional, open and trusting workplace. The purpose of this policy is to safeguard women against sexual harassment at the workplace. Sexual harassment against women in any form is an offence under this policy and is punishable in accordance with the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act 2013 ("Act") and the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Rules, 2013 ("Rules"), and any other applicable legal provisions.

Definition

Sexual harassment of a woman includes sexually determined behavior that is unwelcome to the woman at whom such behavior is directed (whether directly or by implication). Sexual harassment includes actions such as:

- Physical contact and/or advances
- Making sexually colored remarks
- Showing pornography and/or any pornographic material
- Any other unwelcome physical verbal, or non-verbal conduct of a sexual nature
- Any unwelcome sexual advances, demand for sexual favors, either implicitly or explicitly in return for betterment in engagement and working conditions, Promotions, assignments, evaluations in connection with any duties at the Company
- Any unwelcome sexual advances, demand for sexual favors, either implicitly or explicitly with the threat that if a woman does not agree it would affect her career and engagement prospects with the Company
- Any unwelcome act of a sexual nature or any conduct of a Person in authority or otherwise, which outrages the dignity or modesty of a woman and is likely to affect her health or safety and/or create a hostile and/or intimidating work environment
- Any conduct of unwelcome sexual nature and which has the purpose or effect of unreasonably interfering with a woman's work performance
- Any act, advances, explicit or implied, which is of a sexual overtone which the Aggrieved Woman considers to be an act of outraging her modesty or dignity through a virtual communication is also considered to be an act of sexual harassment

Scope

- This policy is applicable to all third-party Resources of the Company in India, including those who are citizens of India but may be situated in a different country in the duration of their engagement with the Company
- For the purpose of this policy:
  - "Employees" include everybody on a regular, temporary, full-time, part-time, ad hoc, daily wage basis, and also extends to trainees, probationers, apprentices, third-party Resources on contract, Persons employed through contractors/agents, consultants or any other service provider and even Persons working on a voluntary basis or without any form of remuneration, irrespective of whether they are working out of Company premises or any other place where they are fulfilling their obligations as per their agreement
  - "Workplace" includes:
    - All offices and premises of the Company where its business is conducted including but not limited to a virtual setup which is available to a third-party resource at the residential place, or at a place where the third-party resource is currently residing at the time when such acts of sexual harassment took place
    - Any place visited by a third-party resource in discharge of the duties towards the Company or where the third-party resource is present in a work-related context or in a professional capacity, including training programs, conferences, off-site meetings and events, work related functions, office parties, business or field trips organized by the Company
    - Places visited when conducting the business of the Company in interaction with third parties and also transportation provided by the Company for undertaking such a journey
- An Aggrieved Woman has the right to complain against sexual harassment regardless of:
  - Her age or her engagement status with the Company
  - The sex of the Alleged Perpetrator
  - Where such harassment occurs
- In case the Alleged Perpetrator is not a third-party resource of the Company, and Aggrieved Woman is a third-party resource, the Company takes all steps necessary and reasonable to assist her with additional support and preventive action, including, where requested in writing by the complainant, cause to initiate action against the respondent under the Indian Penal Code, 1860 or, where relevant, cause a representation to be made to the Employer of the respondent

Points to Note

- All third-party Resources of TresVista are encouraged to report sexual harassment experienced by them or brought to their knowledge to the Internal Committee (IC)

- Confidentiality of information of a complaint against sexual harassment (including name of the Aggrieved Woman, details of the complaint and all related matters) must be maintained at all times. Violation of this requirement is punishable by Law
- Information without particulars, specifically with regard to the identity of the parties involved, may be used by the Company where required for authorized purposes under the Law
- Supervisors are responsible for ensuring awareness of this policy within their teams
- Supervisors must report an issue to the IC if an occurrence of sexual harassment is brought to their notice, within forty-eight (48) hours of receipt of such notice
- As a part of the anti-sexual harassment initiative, third-party Resources must undergo trainings and workshops aimed at spreading awareness

Non-Retaliation

- All complaints against sexual harassment must be made in good faith. A good faith complaint means that the Person making the complaint has provided all the information they possess, that they believe their complaint to be true and that they have made the complaint because the acts mentioned in it violate this policy
- The Company takes a Disciplinary Action against any Person responsible for or involved in any attempt of retaliation (that is, negative behavior aimed at a Person because of a Person's association with an inquiry into sexual harassment) against the complainant, a witness or any Person involved in an inquiry into sexual harassment, including termination, and any other applicable appropriate legal action
- Any form of victimization or retaliation must be immediately reported to the IC

Raising A Complaint and Redressal Mechanism

1. Internal Committee

- Case proceedings for complaints against sexual harassment are undertaken by an Internal Committee ("IC") at TresVista
- The IC can be reached at the following email IDs, depending on the third-party Resources' location:
  - Mumbai, icmumbai@tresvista.com
  - Pune, icpune@tresvista.com
  - Bengaluru, icbengaluru@tresvista.com
  - Gurugram, icgurugram@tresvista.com
- The names and email addresses of the IC members are listed on the posters at all the office locations

1.1. Constitution of the Internal Committee

- The Internal Committee must have four (4) members, of which two (2) members must be women

- The herein above composition of the Internal Committee is in line with the provisions of section 4 (2) of the Act, which mandates the below:
  - **Presiding Officer**: Woman employed at a senior level at the workplace from amongst the Employees
    - In case a senior level woman Employee is not available, the Presiding Officer shall be nominated from other offices or administrative units of the workplace
    - Additionally, in case the other offices or administrative units of the workplace do not have a senior level woman Employee, the Presiding Officer shall be nominated from any other workplace of the same Employer or other department or Organization;
  - **Members**: Not less than two (2) members from amongst Employees preferably committed to the cause of women or who have had experience in social work or have legal knowledge
  - **External Member**: From amongst non-governmental Organizations or association committed to the cause of women or Person familiar with issues relating to sexual harassment
  - At least one-half of the members nominated to the Internal Committee must be women
- The Company ensures that the composition of the Internal Committee is in line with the herein above specified provision of the Act, as amended, at all times

1.2. Disqualification, resignation, or termination of membership of Internal Committee

- A third-party resource/member ceases to hold office as a member of the Internal Committee if she/he ceases to be a third-party resource of the Company. Further, any member is disqualified by the Company, at its own sole discretion, from acting as a member if she/he:
  - Is found guilty of committing an act of sexual harassment or any other act of moral turpitude;
  - Contravenes section 16 of the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013;
  - Has been convicted for an offence or if an inquiry into an offence under any extant Law is pending against her/him;
  - Is found guilty in any disciplinary proceedings or if a disciplinary proceeding is pending against her/him;
  - Has so abused her/his position as a member of the Internal Committee so as to render her/his continuance in office prejudicial to public interest
- In the event of any disqualification, resignation, or termination of appointment of any member, the Company, with respect to an outgoing employee, forthwith notifies a substitute employee and with respect to the external member, makes best efforts to find an external member as quickly as possible
- Notwithstanding the aforesaid, the Company is entitled, at its sole discretion and at any time, to terminate the appointment (as member of the Internal Committee) of any employee and appoint a substitute thereof

1.3. Recusal by Member

Any Internal Committee member who believes that his/her objectivity may be compromised for any reason may apply to the Internal Committee to recuse him/herself from an investigation. The Internal Committee considers whether to accept such requests and if accepted, appoints a replacement Internal Committee member for an investigation in accordance with the Law and/or this policy and notify all concerned parties

1.4. Functions of the Internal Committee

The Internal Committee has the following responsibilities:

- Implementation of the policy relating to prevention of sexual harassment at the workplace;
- Conducting inquiries in accordance with this policy and applicable Laws in force in India, relating to the prevention of sexual harassment;
- Organizing workshops or interactive programs to spread awareness on the issue of sexual harassment as well as this policy amongst the third-party Resources of Company; and
- Keeping a record of all complaints received and the actions taken by the Internal Committee and Company thereon

1.5. Decisions

The Internal Committee decides through unanimous decisions taken by all the members.

1.6. Redressal Mechanism

- Any third-party resource/individual who wishes to make a complaint alleging an act of sexual harassment, would have do so to the Internal Committee in the manner described below. The procedure of redressal of such a complaint is also provided below
- The IC has the powers of a Civil Court while conducting an inquiry and acts in accordance with the principles of natural justice and all parties are given the Opportunity to be heard

2. Raising a Complaint

- A written complaint to the IC (email IDs mentioned above) with a detailed record of the incident/s (such as dates, time, locations, description of the incident and any other relevant information) is mandatory for initiation of an inquiry
- No Disciplinary Action is taken against anyone on the basis of a verbal complaint
- A written complaint made through an online mode of communication consisting of all the details pertaining to the act of sexual misconduct, including the description, time, date etc. whether made by an Aggrieved Woman or the below-mentioned people on her behalf is deemed to be a valid complaint. The complaint along with all the relevant communication, evidence, if any, can be uploaded as attachments in the email or through any other mode as communicated by the Company

- If the aggrieved Person is unable to make a complaint on account of their physical or mental incapacity, a complaint may be filed by the below-mentioned people:
  - Physical Incapacity (With the written consent of the aggrieved Person):
    - Relative or friend
    - Co-worker
    - An officer of National Commission for Women or State Women's Commission
    - Any Person who has the knowledge of the incident
  - Mental Incapacity:
    - Relative or friend
    - Special educator
    - Qualified psychiatrist or psychologist
    - Guardian or authority under whose care they are receiving treatment or care
    - Any Person who has the knowledge of the incident jointly with the above-mentioned people
- If an Aggrieved Woman feels that she needs support in making the complaint in writing, she may contact the IC for assistance
- An Aggrieved Woman may file a complaint within three (3) months from the date of the incident, and in case of a series of incidents, within three (3) months from the date of the last such incident. The IC, on its discretion can extend this time limit not exceeding three (3) months, the reasons to be recorded in writing, if it is satisfied that the circumstances were such that prevented the Aggrieved Woman from filing a complaint within the said period
- Third-party Resources must promptly inform the IC of incidences of sexual harassment, especially in cases where such incidences involve a threat to the security of a Person or the Company
- If the complaint is against a member of the IC, Employees must inform any other member of the IC
- The Company provides the Aggrieved Woman support to file a complaint with the police if she so desires
- Upon receipt of a complaint, whether in writing or otherwise, the IC is expected to respond to the Aggrieved Woman within five (5) working days as a best practice
- Within seven (7) working days of receipt of the written complaint, the IC informs the respondent in writing that a complaint has been filed against him or her and provide a copy of the complaint to enable the respondent to furnish a response
- The respondent is given ten (10) working days to furnish a reply in connection with the allegations of sexual harassment

3. **Malicious or false complaints and false evidence**

- A false complaint is a complaint that is known to be false by the Person making the complaint at the time the complaint is made
- A Person making a false complaint or providing false evidence in an inquiry into sexual harassment is subjected to Disciplinary Action, based on the recommendation of the IC
- A mere inability to substantiate a complaint, or provide adequate proof, does not lead to the complaint being considered as a false or malicious complaint

4. Conciliation

- In case the complainant wishes to settle the matter with the respondent without an inquiry, the IC may facilitate a conciliation between them
- No monetary settlement is made the basis for arriving at any settlement through such conciliation
- Any settlement that is arrived at between the parties during conciliation is recorded in writing and the IC provides copies of the settlement as recorded, to both the parties
- If a settlement is arrived at through conciliation, no further inquiry is required to be conducted by the IC and the matter is treated as closed
- The IC proceeds to make an inquiry into the complaint in cases where:
  - No conciliation has been requested by the complainant, or
  - No settlement has been arrived at between the parties and/or
- If the complainant informs the IC that any term or condition of the settlement arrived at earlier has been breached by the respondent

5. Inquiry

5.1. Process

- The IC follows the inquiry process as laid out in the Company's investigation Handbook. A copy of the investigation Handbook can be accessed on the common SharePoint link
- The IC hears both, the complainant as well as the respondent to record their statements
- Both parties may submit to the IC evidence and a list of witnesses to support their statements
- The IC may summon the attendance of any Person and examine the Person on oath as well direct production of any document which may assist the IC in an inquiry into sexual harassment
- If either party remains absent during the inquiry proceedings for three (3) consecutive hearings, the same may be conducted ex-parte on the basis of material on record
- The IC must conclude the inquiry proceedings within a period of ninety (90) days from the date of the receipt of the written complaint

- The inquiry in the matter can be conducted through a virtual online session if any of the parties involved is working from home. The IC may conduct the inquiry on video calls and may also record it for audit purposes and references

5.2. Interim Actions

During the pendency of an inquiry:

- The IC may, based on the request of the complainant, recommend to the Company to transfer the complainant or the respondent to any other workplace or grant the complainant leave up to a period of three (3) months, in addition to any other paid leave she may be entitled to, under her terms of engagement. Neither the complainant nor the respondent has any choice of place of transfer as it is as per the Company's requirements
- If the IC is of the view that the presence of the respondent at the workplace is detrimental to the interest or to the conduct of a free and fair inquiry, it can recommend to the Company to place the respondent under suspension or leave pending completion of the inquiry:
  - Full salary is payable during such period of suspension pending inquiry
  - Such suspension order may also include an order prohibiting the respondent from accessing the Company's IT facilities, third-party Resources or third parties to enable a fair and objective inquiry
  - Supervised access is provided to information relevant to the respondent to prepare a defence in the inquiry and the Alleged Perpetrator may make any such requests in writing to the IC
- In case the IC determines it to be necessary, it may recommend counselling for the complainant to the Company, which is offered to her at the cost of the Company

5.3. Post Inquiry

- On completion of the inquiry, the IC submits the report of its findings to the Management of the Company along with all relevant documents, within ten (10) days from the date of closure of the inquiry proceedings, a copy of which is also made available to the complainant and the respondent
- If the allegations against the respondent have not been proved, the Company takes no action in the matter
- If the allegations have been proved, the Company takes appropriate action against the respondent within sixty (60) days of receipt the final report
- Proceedings conducted under the provisions of this policy, are considered to be disciplinary proceedings under the Company policy and no separate inquiries are required to be conducted

6. Disciplinary Action

As prescribed by the IC, Disciplinary Action may include the following:

- Rendering of a written apology
- Censure and reprimand
- Payment of a fine

- Demotion or withholding of Promotion
- Termination with Cause in keeping with section 6.1 of this Handbook
- Attending counselling
- Undertaking community service
- Monetary compensation to be paid to the complainant. The sum to be deducted is decided on the keeping in mind:
  - The mental trauma, pain and suffering of the complainant
  - The loss in career Opportunity of the parties
  - The medical expenses incurred due to sexual harassment, whether for physical or psychiatric treatment and the income and financial status of the respondent
- The amount may be deducted from the salary of the respondent or he/she may be instructed to make the payment directly to the complainant

Repercussions of sexual harassment may also result in initiating criminal charges, in addition to any action the Company may take, based on the recommendations of the IC. These actions are in addition to any legal recourse, and where any conduct or actions amount to specific offences under the Law.

2.7 Code of Ethics

The purpose of this policy is to define a set of principles for third-party Resources 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 third-party Resources and, in doing so, defines desired behavior. Third-party Resources 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

Third-party Resources 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 third-party Resources must understand and comply with any applicable Laws, rules, regulations, and internal policies.

Integrity

During and after the term of their engagement with TresVista, third-party Resources 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
    - A third-party resource'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, stepbrother and stepsister
        - Any other Person who is financially dependent on the third-party resource
    - For the purpose of this policy, the definition of 'dependent' has the meaning assigned to it under section 80DD of the Income Tax Act, 1961 (43 of 1961)
    - A third-party resource should check with the Compliance department if they are unsure of how to interpret above connections in their case
- 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

Morality

If a third-party resource commits any act, which:

- Is an offence involving moral turpitude under central, state or local Laws
- Might tend to bring the third-party resource 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 agreement for cause; in such cases no prior notice of termination is provided, upon written notice to the third-party resource.

Fair Dealing, Diversity and Equal Opportunity

- TresVista condemns discrimination in any form and aims to provide a healthy and dignified work environment for all third-party Resources
- Third-party Resources must treat all fellow third-party Resources and third parties with respect and merit irrespective of their sex, age, sexual orientation, marital status, caste, religion, color, race, nationality, or any disability they may have. Harassment and bullying are considered as gross misconduct and are prohibited
- Third-party Resources must create a culture of fairness and transparency, which includes treating those with whom we have professional relationships with respect and ensuring that third-party Resources 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 engagement, third-party Resources 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 engagement 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 engagement without the Company's prior written permission
- Such Confidential Information is solely and absolutely vested in and owned by the Company, and the third-party resource does not have or claim any right, title or interest therein
- Not divulge or disclose to any other third-party resource, the third-party resource'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 unpublished price sensitive information as defined in the SEBI's (Insider Trading) Regulations, 1992 (as may be modified/amended/re-enacted from time to time), in the manner and in terms of 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 engagement for whatever reason, deliver to the Company all working papers and/or other material and copies provided to the third-party resource pursuant to their engagement or prepared by the third-party resource during the term of their engagement, 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 third-party Resources) 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 Supervisor or other authorized third-party resource
- Confirm that all the files are precisely stored, deleted or destroyed as directed by the Supervisor or other authorized third-party resource 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 engagement

- Not at any time during the continuance of their engagement or on expiry or termination or cessation of engagement 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 engagement 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 engagement, without any restrictions regarding time (i.e., indefinitely) and are binding upon the third-party resource's heirs, assigns, executors, administrators and other legal representatives. Third-party resource'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 third-party resource'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 third-party resource 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 third-party Resources from using their own personal skill in any business in which they may lawfully be engaged after the termination of their engagement, provided such engagement is in compliance with exit formalities provided (Refer to section 6.2 of this Handbook)

Communication

During and after the term of their engagement, third-party Resources 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 third-party resource'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 3.9 of this Handbook)
- 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 third-party

Resources 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 third-party resource 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
- Third-party Resources 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
- Third-party Resources 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 third-party Resources, to be honest and upfront in advertising and marketing claims to avoid misrepresentation, exaggeration, ambiguity and reduce complexity & excel at execution

Ownership

During and after the term of their engagement, third-party Resources 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 third-party resource'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 third-party Resources are currently or potentially engaging in illegal, or unethical activities

Partnership

During and after the term of their engagement, third-party Resources 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

Third-party Resources must be cautious and do nothing that might endanger or harm TresVista's business associates in any way – whether they are fellow third-party Resources, vendors, visitors, etc. Third-party Resources 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

Third-party resource should work at TresVista in a professional manner with objectivity, independence of mind and appearance. Third-party Resources must impose an obligation on their fellow third-party Resources 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 Third-party Resources

Third-party Resources must treat fellow third-party Resources & 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

Third-party Resources must ensure that relationships with fellow third-party Resources & 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
- Third-party Resources 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

- Third-party Resources must make a judicious use of air-conditioning and heating devices and switch-off devices when not in use

Additional Compensation Arrangements

- Third-party Resources 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 section 3.8 of this Handbook
- Third-party Resources 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

- Third-party Resources 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
- Third-party Resources 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
- Third-party Resources 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
- Each third-party resource 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 third-party Resources 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., a third-party resource raising a concern regarding the dishonesty of a superior/a third-party resource from the top Management)

- Through this clause, TresVista is committed to support and enforce the Fraud and Whistleblower Policy, (mentioned in section 2.10 of this Handbook) which aids in the detection and prevention of Fraud. 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

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 third-party resource, their Supervisor 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
  - Monetary compensation to be paid to the Company
  - Termination with Cause in keeping with section 6.1 of this Handbook

Affirmation Process

Third-party Resources 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 third-party Resources. 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 third-party resource of TresVista, whether oral or written, confer any rights, privileges or benefits on any third-party resource, create an entitlement to continued engagement at TresVista, establish conditions of engagement, or create an express or implied engagement contract of any kind between third-party Resources and TresVista. Third-party Resources should also understand that this Code does not modify their engagement relationship, whether at will or governed by a written contract

2.8 Code of Conduct

The purpose of this policy is to define standards and set guidelines concerning acceptable behaviour from third-party Resources. 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, third-party Resources are expected to support the Mission, Vision, and PACT of TresVista.

Overview

All third-party Resources 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 third-party Resources 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.

Eligibility

This policy applies to all third-party Resources of TresVista. Each third-party resource 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 third-party Resources 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 third-party Resources are expected to comply with the policy when performing their duties
- Third-party Resources are expected to understand their obligations as per the guidelines defined in this policy
- Third-party Resources 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

- Third-party Resources must build and foster long-term relationships. This helps serve the Clients better and improves and upholds the Company's reputation
- Third-party Resources should provide Clients with valued services and deal with them fairly
- Third-party Resources must act with integrity and do everything possible to provide excellent service to them either directly or by supporting the work of other individuals
- Third-party Resources must not make any promises that cannot be fulfilled by them or the Organization
- Third-party Resources 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 third-party resource or TresVista

Disclosure to the Media

- The social media policy is a supplement and should be read in conjunction with this document. The purpose of the social media policy is to ensure that third-party Resources understand and comply with TresVista's disclosure requirements in terms of media interaction and public presentations. The detailed social media policy can be referred to under section 4.8 of this Handbook
- If third-party Resources 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, third-party Resources 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

- Third-party Resources must conduct themselves professionally and with personal integrity, both in and out of the workplace, reflective of TresVista values
- Third-party resource 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 imperative to avoid having alcoholic drinks while representing TresVista at social gatherings and parties
- Third-party Resources are expected to carry an official identity card, and any other document like business card, etc. as may be required to represent TresVista

Involvement in Out-of-Office Activities

- This clause helps third-party Resources 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

- Third-party Resources 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 third-party Resources 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
- 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 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

Third-party Resources 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 engagement and advancement opportunities to individuals without distinction or discrimination because of age, color, national origin, race, religion, caste, sex, physical or mental disability, or veteran status

- This clause applies to all third-party Resources and candidates for engagement and all aspects of the engagement relationship, including recruitment, hiring, compensation, benefits, training, transfer, and any other terms and conditions of engagement

Professionalism

Third-party Resources must show integrity and professionalism in the workplace.

Personal Appearance

Third-party Resources must follow the dress code and personal appearance guidelines as mentioned in the section 3.3 of this Handbook.

Respect in the Workplace

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

Communication with Former and Potential Third-party Resources

Third-party Resources should be careful in speaking with former and/or potential third-party Resources and not disclose Confidential Information about the Company, even if it is something that they may already know.

Legal and Social Responsibility

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

Sustainability and Environmental Protection

- TresVista continuously educates its third-party Resources on environmental issues and stimulates individual and local initiatives
- TresVista strives to continually reduce environmental impact and endeavors to reduce energy consumption and waste etc.

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

Protection of Company Property

- Third-party Resources should treat TresVista's property, tangible or intangible, with respect and care
- Third-party Resources should not misuse TresVista's equipment or use it frivolously
- Third-party Resources 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, third-party Resources must ensure that they return all Company property in their possession, including but not limited to records and equipment

Protection of Confidential Information

- Third-party Resources of TresVista should protect Confidential Information about the Company, Clients, etc. received during the term of their engagement
- For ensuring that Confidential Information is well protected, third-party Resources should disclose information only on a "need-to-know" basis
    - Details can be referred to in section 4.9 of this Handbook

Prohibition of Insider Trading

- TresVista restricts its third-party Resources from trading in Personal Accounts using price-sensitive information of Clients received during the term of their engagement for personal gain/benefit

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 third-party Resources understand and adhere to the Company's ethical standards and comply with legal obligations
- It restricts third-party Resources 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
- Third-party Resources 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

- Third-party Resources must refrain from sharing information that is private or proprietary to TresVista
- Third-party Resources must avoid posting derogatory comments about Clients, competitors, Employer, or their practices on social media
    - For more information, kindly refer to the section 4.8 of this Handbook
- Third-party Resources must align themselves with the Company's social media policy and plan before posting anything on social media platforms

Sexual Harassment

- TresVista does not tolerate sexual harassment, which involves the solicitation of sexual favors or the initiation of any unwelcome sexual advance by one third-party resource 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
- All Third-Party Resources throughout TresVista should treat one another with courtesy, dignity, and respect, regardless of gender
- Third-party Resources 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 Supervisor, 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 2.6 of this Handbook

Drugs, Alcohol and Smoking

- Third-party resource 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 third-party resource is permitted to smoke at the workplace
- Third-party resource whose behavior, judgment, or performance is impaired by drugs or alcohol should not report to work. Such third-party Resources 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 Termination with Cause

Workplace Violence

- Third-party Resources 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 third-party resource's safety or the safety of others must be immediately reported to the respective Supervisors

Violation

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 to the relevant authorities. Additionally, the third-party resource, the third-party resource's Supervisor or any other Person who was conscious of the breach is subject to the Disciplinary Action including but not limited to Termination with Cause.

2.9 Acceptable Usage Policy

The purpose of this policy is for the Firm to provide third-party Resources access to email facility and intranet, in order to boost third-party resource efficiency and streamline interaction with colleagues, customers, and business Partners. This policy defines and educates third-party Resources 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 third-party resource morale, risks arising from diminished corporate reputation, and compliance issues, etc.

Applicability

This policy applies to all users including third-party Resources having access to Information and IT Resources in TresVista.

Particulars

- Third-party Resources must agree to the terms and conditions set forth in this policy
- The activities mentioned in this policy are prohibited
- Third-party Resources 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, a third-party resource of TresVista is authorized to engage in any activity that is illegal under local, state, national, 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

Third-party Resources must:

- 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 Policy and other related policies within the Organization
- Access only those Resources, for which they are authorized and use information and 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 Supervisors immediately, in case they accidentally come across unsecured sensitive information that could affect the Client and their 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 not related to their work
- Not copy, collect, or propagate any TresVista data or documents outside the network

Work Area Security

- All third-party Resources must comply and cooperate with spot checks and audits
- Third-party Resources are responsible for visitors, contractors and Clients that they bring to the office premises
- It is their responsibility to immediately inform their Supervisors and raise an incident with the Compliance department in case they come across any unauthorized Person
- Third-party Resources 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 third-party Resources:

- The desktop ownership lies with the IT department and data ownership rests with the respective third-party resource
- Third-party Resources 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
- Third-party Resources must secure data on their systems by using passwords (power-on password, screensaver password etc.) and ensure compliance with the password policy

- Third-party Resources must not reveal account passwords to others or allow others to use their account (including family and other household members when working from home)
- Third-party Resources must not leave any Confidential Information on their system unattended
- Third-party Resources must not keep liquids or magnets on or near computer equipment
- Third-party Resources are not permitted to remove or transport computers from TresVista premises without the appropriates permissions
- Third-party Resources 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 third-party Resources. Third-party Resources 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 third-party Resources of TresVista

General Security Guidelines

The following activities are strictly prohibited, with no exceptions:

- Third-party Resources must not circulate, store and create obscene, vulgar, or inappropriate materials, jokes, pictures, chain letters etc. in any media/form
    - In case any third-party resource receives such material, they must immediately remove the material, and inform incident Management response team
- Third-party Resources must not use or aid by any means attempts to thwart access rights like stealing IP, hacking etc.
- Third-party Resources 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
- Third-party Resources 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 third-party resource's host, unless this activity is a part of the third-party resource'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 third-party resource'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 third-party Resources 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 third-party resource'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 attracts Disciplinary Actions as per the annexure.

2.10 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 third-party Resources 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 third-party Resources 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.: Third-party resource 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 a third-party resource, 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 third-party Resources and recognizes that they have a key role to play in the prevention, detection and reporting of Fraud
- Third-party Resources 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 Whistleblower' policies
  - Seek advice from their colleagues or Supervisors, 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 a third-party resource 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:
  - Third-party Resources 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
- 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 a third-party resource'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 the identity of the whistle-blowers must always be 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
- Disclosures expressed anonymously are generally not investigated

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 third-party Resources 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 it is known that false disclosures/complaints are made, then the complainant are subject to strict Disciplinary Action as the Executive Committee may deem fit

Protection

- Protection is provided to the whistleblower who has reported a Fraud, basis the assumption that the information, and any allegations contained in the report, are substantially true and the disclosure has not been made in the interest of personal gain
- 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 third-party Resources from unfair termination and unfair prejudicial engagement practices
- No unfair treatment is vetted out towards the whistle-blower by virtue of having reported a Fraud and they receive protection against:
  - Unfair engagement 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 attorney or 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 third-party Resources 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.

Working at TresVista

3. Working at TresVista

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

3.1 Work Hours 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 Third-Party Resource or as may be specified in their respective Agreement as it may be amended. The Third-Party Resource:
    - Shall be required to adhere to the office hours as may be intimated by the Company or as may be specified in with the Agreement
    - Understands and agrees that no compensatory offs are provided by the Company for working late and/or on weekends or Firmwide Holidays
    - Understands and agrees that the fees/compensation payable as part of his/her engagement includes the total consideration for the engagement and no separate overtime payments would be paid to the Resource unless otherwise agreed in the Agreement
  - The Company may, at its discretion, vary its working hours for any specific Third-Party Resource to meet its requirements ongiving the Third-Party Resource reasonable notice. If requested to do so by the Company or their Supervisor, the Third-Party Resource and their Supervisor(s) must keep such records and permit such monitoring or restrictions of the working time as the Company requires. In case any flexibility is required in the working hours due to any unavoidable circumstance, the same may be granted to the extent permitted by their Supervisor and acceptable to the Company

Working in Shifts

- **Shift Allocation:**
  - Shifts may be rotational and allocated at the discretion of the Supervisor or as per the Agreement
  - All shifts will be tracked through a monthly roster, created at the beginning of the month, and communicatedto the team
  - In case of any medical or unforeseen emergency, Resources may request a change in shift. Approval of such requests is at the discretion of the Supervisor
  - Supervisor may make changes to the roster, as required

- **Night Shift:** New Third-Party Resources may be allocated the night shift as agreed in the Agreement
- **Attendance and Leaves:**
    - As part of the shift structure, Third-Party Resources may be required to work on weekends and Firmwide Holidays
    - Weekly offs will be determined basis the shift allocated and Third-Party Resources working on Firmwide Holidays are eligible for rotational weekly offs, subject to the Supervisor's approval

Attendance

- The Third-Party Resource is expected to use the biometric on every entry and exit. Tailgating will be counted as noncompliance to office rules and will lead to consequences as per the consequence matrix of the Physical Security Policy
- For bandhs and other public transportation strikes, Third-Party Resources are expected to find alternative means of transportation. Absences due to bandhs and other public transportation strikes will be considered to be unpaid leaves, unless the Management/ HR Department notifies the Supervisor and declares such a day to be a Holiday

3.2 Hybrid Guidelines

TresVista at its discretion shall decide the days on which the third-party Resources must work from the office, and it will be intimated to them from time to time.

3.3 Dressing Guidelines and Personal Grooming

Third-party Resources must be dressed to create the impression of professionalism and perfection, characteristic of the culture andwork ethic at TresVista. As a minimum standard, attire must be clean, neat and professionally appropriate. Dress choice is a matter of personal discretion, taking into account requirements for any protective clothing and/or medical requirements while keeping in mind the professional environment. A manual with detailed guidelines on 'Formal Dressing'will be made available to the Third Party resource and the Supervisor .

Particulars

The dress code for each day is as follows:

- **Working from the office:** Unless a specific uniform attire is designated to Third-Party Resources by their Employer or as requested by the Company basis their roles, below provisions will be applicable,
    - **Monday – Thursday:** Business casual, although business formal is always acceptable
    - **Friday:** Casuals
- **Working from home (if applicable):**
    - **Friday Casuals:** Day to day operations, internal training, or webinars

- **Business Casuals:** External meetings, training, calls with senior Management/Clients and conducting internal meeting with more than ten (10) attendees

- **Weekends:** No dress code

If a third-party resource is found to be inappropriately dressed, they may be asked to leave with the day being marked as absent by their Supervisor.

3.4 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 used within the Company:

- **Direct Communication:** Third-party Resources are encouraged to speak directly to their Supervisors 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, third-party Resources should raise a Helpdesk Tickets with the respective departments. If third-party Resources are dissatisfied with the resolution, they may escalate it in accordance with the defined SLA matrix, saved on the SharePoint

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

3.5 Personal Information

A third-party resource may be required to submit personal documents before they join the Company.Third-party resource is responsible to ensure that their personal information is up to date; for instance, change in address or certification received. The documents may include but are not limited to the third-party resource's passport, PAN card, mark sheets, driving license, and experience letters. Management, the Corporate Finance Department, and HR Department have access to these documents.

All personal information is kept strictly confidential.

In the course of engagement with the Company, the Company may obtain or have access to certain information about the third-party resource or his/her engagement with any other Organization they are working with or any previous Organizations they have worked with, including but not limited to information about the role and performance, health, education, contact details, absence from work and information obtained from BackgroundVerification checks (collectively, 'Personal Information'). The Company will use personal information in connection withthe engagement with the Company, to provide the third-party resource with health and other benefits, and in order to fulfill its legal and regulatory obligations.

TresVista can leverage third-party resource's pictures and videos for the various marketing and communication materials and showcase various engagement initiatives, reflecting culture and growth of the Organization. The content will be used for (including but not limited to) internal communication (E.g., Company/department updates, Yammer posts, etc.), external communication (E.g., Company website, social media posts, PR notes/articles, Company newsletter, etc.), and other print and digital communications as deemed appropriate by TresVista.

The Company will use Personal Information in connection with the engagement with the Company, to provide the third-party Resources 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 third-party resource's personal information in a country (including the United States) or continent outside the country where the third-party resource works or lives, and may also transfer a third-party resource's personal information to its other group companies, insurers, and third-party service providers, as necessary or appropriate in the third-party resource's home country, the United States or other countries, 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 thecountry or continent the third-party resource works or lives).

The Company may also disclose a third-party resource's personal information when it is legally required to do so or to governmental, fiscal, or regulatory authorities. The Company may disclose personal information as noted above, including to any ofthe third parties and for any of the reasons listed above, without prior notice to the third-party resource. By receiving this Handbook, the third-party resource consents to TresVista for collecting, retaining, disclosing, and using personal information as outlined above and to transfer such information internationally and/or to third parties for these purposes.

3.6 Personal Use of Company Resources

The use of Company Resources for personal use is a privilege and not an entitlement, and may be revoked at any time. Such use must:

- Be limited, infrequent and reasonable
- Be lawful, ethical, and efficient
- Incur no or minimal additional cost to TresVista
- Not impact the third-party resource's productivity
- Not interfere with the operation of the Company, or contravene Law
- Not interfere with or distract any other third-party resource from their work

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

3.7 Phone Etiquettes

All third-party Resources are expected to be reachable on their cell phones even when not in office.

It should be noted that:

- Third-party Resources 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 third-party Resources 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

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

3.8 Gift Policy

The purpose of this policy is to define guidelines in order to restrict third-party Resources 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 third-party Resources 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

- Third-party resource 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
- Third-party Resources are not allowed to accept any gifts or give any gift from/to competitors
- It is prohibited, directly or indirectly, for any third-party resource 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
- Third-party Resources 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

- Third-party Resources need to take approval 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 INR 10,000	Intimation	Supervisor (VP/EVP) Compliance department
Up to INR 20,000	Prior approval	Supervisor (Head of Department) Compliance department
INR 20,000 above	Prior approval	Management Compliance department

- For FMS support staff, Supervisors must inform/seek approval on their behalf
- Compliance department reserves the right to ask third-party Resources to return the received gifts
- Post receiving approvals, all third-party Resources 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

Third-Party Resource Awareness

At TresVista, training is provided to all new third-party Resources as a part of the induction process and refresher training is conducted for the entire Company annually.

Compliance

- The Compliance department will verify 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 to the aforementioned policy shall attract Disciplinary Actions as defined in the annexures of this Handbook.

3.9 Organizational Hygiene

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

Eligibility

This policy is applicable to all third-party Resources.

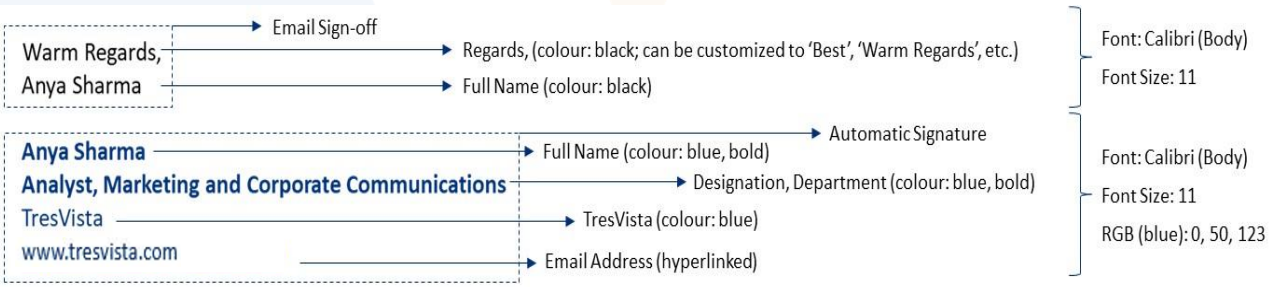
Particulars

Organizational Information and Materials

- Organizational information talks about the Organization, its values, culture, third-party Resources, services, Clients, business operations, partnerships, and activities and is accessible to all third-party Resources 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, third-party resource 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
- Third-party Resources 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

- Third-party Resources 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 third-party resource)
  - 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, third-party Resources 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:** Third-party Resources 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 Supervisors and accordingly set an out-of-office email, if deemed necessary
- **External Emails:** Third-party Resources 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 third-party Resources 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, third-party Resources 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, third-party Resources may choose not to use a background
  - Third-party Resources may choose to use the celebratory or milestone-related backgrounds sent firmwide
  - Third-party Resources 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

3.10 Brand Communication Guidelines

The purpose of this policy is to educate third-party Resources 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 third-party Resources

Particulars

Brand Tonality

- For any communication piece, third-party Resources 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, third-party Resources must be transparent, establish a
    two-way conversation, show that they are genuinely listening, and be approachable in their communication
  - It is expected that third-party Resources are straightforward but not rude in their communication
  - If the communication piece is light-hearted, fun, or celebratory, third-party Resources may structure their message accordingly and make the communication less verbose
  - Third-party Resources 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 ‘third-party resource’, except for process/policy-related communications

Guidelines for Inclusive Communication

- For any communication piece, third-party Resources 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’
  - Third-party Resources 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

3.11 Corporate Communication Policy

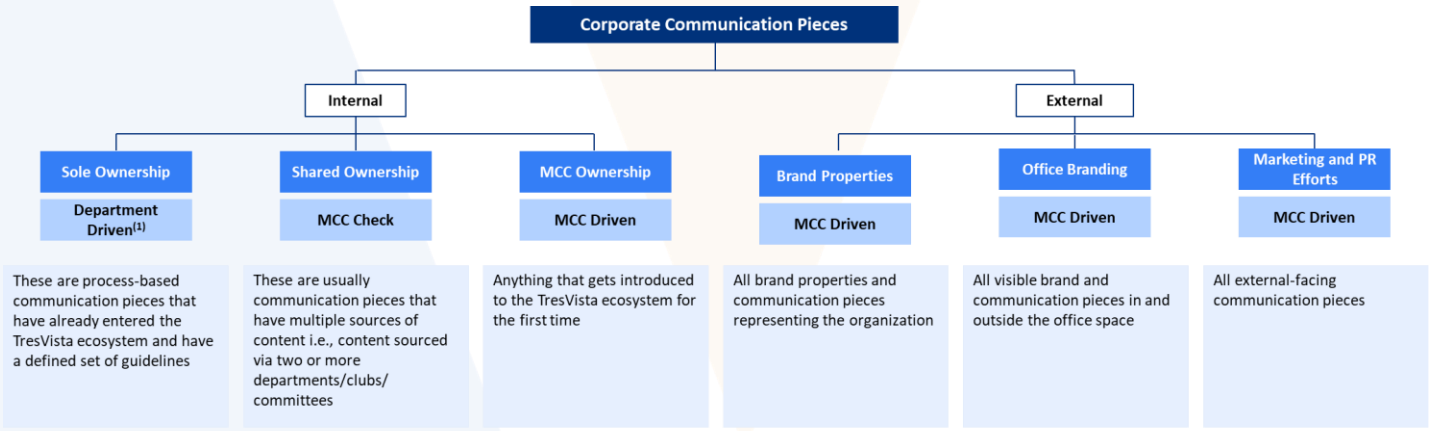
The purpose of this policy is to define guidelines for internal and external corporate communication pieces and have a central authority to help:

- 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

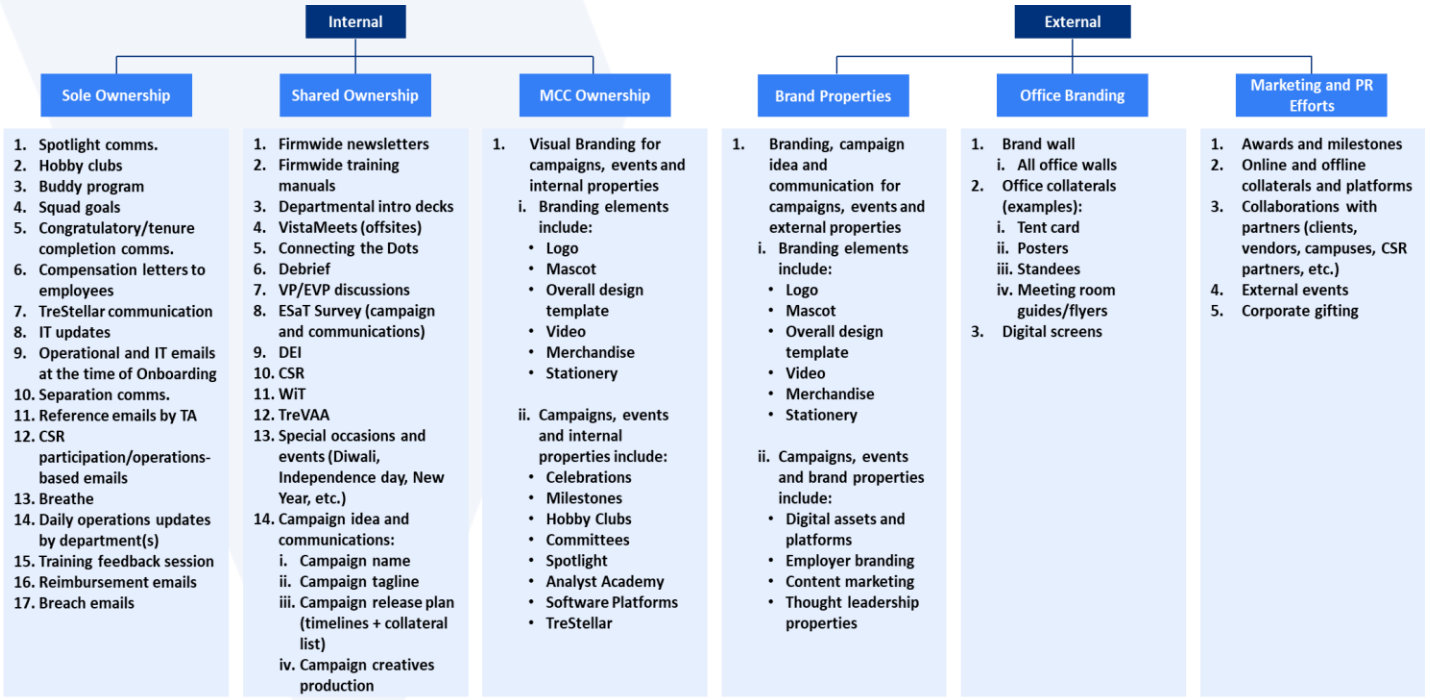
Corporate Communication Structure

The corporate communication structure at TresVista consists of two verticals, namely, internal, and external. For any communication, third-party Resources 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 3.10 of this Handbook
    - 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 third-party Resources 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 third-party Resources 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, third-party Resources can reach out to the MCC department and the team will inform third-party Resources 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, third-party Resources can reach out to the MCC department, and the team will accordingly inform third-party Resources 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 third-party Resources), 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:
  - Third-party Resources 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, third-party Resources can reach out to the MCC department and the team will inform third-party Resources 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 third-party Resources 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.

3.12 FMS support staff: Education Support Policy

The purpose of this policy is to provide monetary assistance to FMS support staff to help them support the educational expenses of their children.

Eligibility

The policy is applicable to FMS support staff if:

- The Labour Wages/Minimum Pay Act is applicable to them
- They are employed with TresVista on the Firm's payroll or third-party payroll without any gap in service due to voluntary resignation, termination, un-approved leaves, or absenteeism for:
  - A minimum period of three (3) continuous years to avail education support up to 12th Grade
  - A minimum period of ten (10) continuous years to avail education support for graduation and above

Particulars

- In one (1) academic year, the FMS support staff is eligible to avail the following benefits, per child, for up to two (2) children:
    - Up to 12th Grade: INR 30,000
        - In case the child is preparing for entrance/competitive exam in the 12th Grade, an additional INR 40,000 can be availed
    - For Graduation and Above: INR 70,000
- Fees are directly paid to the school, college, educational institute, coaching class, and/or private tutor, provided all required documents are submitted within the defined timeline

Procedure for Application:

- **Required Documents:** FMS support staff is required to submit the following documents at least one (1) month prior to the due date, to the FMS department, along with the child's birth certificate and bill/invoice received from school, coaching class, and/or private tutor:
    - **For School/Coaching Class:** Letter with fee details
    - **For Private Tutor:**
        - Letter with fee details
        - Bank details of the private tutor on their letterhead
        - Copies of PAN/Adhaar card of the private tutor
- **Approval Matrix:**
    - All such requests require approval from the Head of Department - FMS
    - Upon receiving the request, the FMS department must:
        - Inform the Corporate Finance Department of the application(s)
        - Seek necessary approvals on the application(s)
        - Share relevant approvals and documents with the Corporate Finance Department to process the payments
        - Share the payment confirmation with the Corporate Finance Department
        - Act as a point of contact for the Corporate Finance Department

Points to Note

- Continuous employment is calculated basis the FMS support staff's most recent date of joining
- If the FMS support staff resigns within six (6) months from the date of availing this benefit, the benefit amount is adjusted against the their full and final settlement

- Non-adherence to the application timelines (i.e., delay in submitting school fees invoice/schedule) leads to cancellation of the payable benefit amount
- Any payments made directly to the FMS support staff require prior approval from the Head of Department - FMS
- All the bills, supported by the original receipt, as applicable, should be submitted/emailed to the Corporate Finance Department within the defined timeline
- TresVista reserves the right to amend this policy basis business requirements

3.13 Travel and Security Policy

The purpose of this policy is to provide guidelines to all Third Party Resources exiting the office premises post the legally mandated timelines or post 9:00 PM, as applicable.

(A) For Female Third Party Resources Exiting Office Premises Post the Legally Mandated Timeline

(I) Mumbai, Pune, and Bengaluru

Eligibility

This policy is applicable to all female Third-Party Resources if they are exiting the office premises post the legally mandated timeline:

- Mumbai and Pune: 9:30 PM
- Bengaluru: 8:00 PM

Particulars

- The Company will provide transportation service to the female Third-Party Resources exiting post the legally mandated timelines, as applicable, for a safe commute to their residence
- First trip will be available thirty (30) minutes post the legally mandated timelines
- As a part of this service, female Third-Party Resources will be accompanied by a Company-appointed Male Representative, to their residence, as per the address mentioned in the Company records (DarwinBox)
- **Approval Matrix:**
    - Female Third-Party Resources can avail this service, Subject to the Manager approval. In the absence of Manager, the approvals will be sought as follows:
        - For Analyst and equivalent: Line Manager
        - For Associate and equivalent: Self-approval

- No separate approval will be required if VP and above female Third-Party Resources avail this service
- For female Third-Party Resources who are undergoing new hire training (NHT), the approval will be sought from the Training department

- It is mandatory for all female Third-Party Resources to exit from the reception area (where the security guard is available) when exiting the office premises post above-mentioned timelines

Procedure

- **For female Third-Party Resources exiting post the legally mandated timeline and opting for transportation service provided by the Company:**
  - A Helpdesk request must be raised with the FMS department under the category of 'Ground Transport Services' with the necessary details
    - Requests must be raised and approved by the Manager (as applicable) minimum ninety (90) minutes prior to the departure
      - In case female Third Party-Resources inform the FMS department about their requirement less than ninety (90) minutes prior to their departure, a justification will be sought from their Manager, post which, if possible, a cab will be booked on the spot, Subject to availability
    - Requests will only be initiated after receiving the necessary approvals, as applicable
    - Incorrectly raised requests may lead to a delay in processing the requests
    - Requests shared via any other platform (E.g., verbal requests, emails, Microsoft Teams, etc.) will not be processed
  - Addresses updated on DarwinBox will be referred by the FMS department at the start of each quarter
    - In case the current residential address differs from the one mentioned on DarwinBox, a softcopy of the updated address proof (E.g., rent agreement, Aadhaar card, PAN card, driving license, etc.) must be attached as a one-time activity, while raising the request, after which FMS department will update the address in their records
      - Female Third-Party Resources in the initial ninety (90) days from the date of joining are exempted from providing a softcopy of their updated address proof, in case of a change in their residential address. However, they are mandatorily required to fill in their updated address on DarwinBox by 3:00 PM on any given day
      - Post completion of the initial ninety (90) days, female Third-Party Resources must mandatorily provide a soft copy of their address proof in case of change in their address

- In case of deferring address from the one on DarwinBox or no proof of address change is attached while raising a request, it will not be processed further. Female Third-Party Resources are then required to plan the commute on their own in line with the guidelines specified under 'For female Third-Party Resources exiting the office premises post the legally mandated timeline but not opting for the transportation service provided by the Company'
- In case of change in address, female Third-Party Resources should ensure that their current address is updated on DarwinBox at the earliest
- In case the current address is not updated on DarwinBox by the beginning of the next quarter, female Third-Party Resources will still be required to attach the address proof while raising the request

- Female Third-Party Resources should update their personal and emergency contact details on DarwinBox as soon as there is a change in these details
- Once the travel request is approved by the Manager, the FMS department will share the following details via email closer to the departure time, as applicable:
  - Departure slot and pick-up location,
    - Female Third-Party Resources are required to be at the pick-up location five (5) minutes prior to their departure time
  - Details of the car (vehicle type, number, etc.)
  - Details of the driver and/or Male Representative (name, contact details, etc.)
  - Do's and don'ts to be followed during the trip
  - Link to the acknowledgement survey form which must be mandatorily filled in/responded by female Third-Party Resources on the safe arrival at their doorstep
- This service, across all office locations and drop distances (within a reasonable limit from the office premises), will be provided in intervals of 90 minutes, on a first come first serve basis
  - Multiple female Third Party-Resources residing on the same route can be accommodated in one trip
  - No in between stops/halts will be allowed from the office premises to the residential address
- This service will be provided Subject to the logistical requirements, such as availability of cabs, Male Representatives, etc.
- Conveyance reimbursements claimed by female Third Party-Resources for the days they opt for this service, will be rejected by the Corporate Finance department
- On days when female Third Party-Resources are working from another office location and wish to avail this service, they must include the following details while raising the Helpdesk request:

- Email approval from their Manager to work from another office location (as an attachment)
- Temporary address details

- Once female Third Party-Resources have been accompanied to their residence by the Male Representative, they must mandatorily:
  - Sign the travel receipt confirming that they have been safely dropped off at their residence
  - Respond and submit the acknowledgement survey form mentioned on the email shared by FMS department within fifteen (15) minutes of their arrival at their doorstep
  - A SPOC from the FMS department will call on the registered mobile number of the female Third Party-Resources to check on their safe arrival, if the response is not received within fifteen (15) minutes from the time they have been dropped off at their residence
  - In case the call is not answered, the FMS SPOC will call the emergency contact as mentioned on DarwinBox in next fifteen (15) minutes
  - In case emergency contact does not answer the call, the FMS SPOC will visit female Third Party-Resources address (as mentioned on the Helpdesk Ticket) in Person to verify their safe arrival

- **For female** Third Party-Resources **exiting post the legally mandated timeline but not opting for transportation service provided by the Company:**
  - A Declaration Register must be mandatorily signed at the office reception if the female Third Party-Resources exit the office premises post the legally mandated timeline and do not wish to opt for the Company provided transportation service
    - Female Third Party-Resources, undergoing new hire training outside office premises, must sign the Declaration Register kept at the training venue

Non-Adherence to the Policy

- The below mentioned breaches shall lead to Disciplinary Action which may include but not be limited to policy reminder, re-training, impact on review rating, issuance of warning letter, or termination:
  - Not informing the FMS department of the safe arrival via the acknowledgement survey form after opting for the Company-provided transportation service, and/or;
  - Exiting the office premises post the legally mandated timelines without signing the Declaration Register and have opted out of the Company-provided transportation service
- In case female Third Party-Resources do not utilize this service after the booking is confirmed, the applicable cancellation charges will be borne by them

(II) Gurugram

Eligibility

This policy is applicable to all female Third Party-Resources if they are exiting the office premises post 8:00 PM.

Particulars

- The company will provide transportation service to the female Third Party-Resources exiting post 8:00 PM for a safe commute to their residence (doorstep) and it is mandatory for the female Third Party-Resources to avail it. This is irrespective of them having commuted to work via their personal vehicle or have family members/friends who are willing to pick/drop them to their residence (doorstep)
- First trip will start 9:00 PM onwards to ensure safe commute of female Third Party-Resources from the office premise to their residence (doorstep)
- As a part of this service, female Third Party-Resources will be accompanied by a Company-appointed Male Representative, to their residence (doorstep), as per the address mentioned in the Company records (DarwinBox)
- Around 7:00 PM, the transport coordinator will check with all females in the office at that time, if they would be exiting post 8:00 PM and accordingly plan routes to minimize the wait time. In case an additional car is needed, necessary arrangements will be made by the transport coordinator. However, the female Third Party-Resources may have to wait till the car is available
- **Approval Matrix:**
    - Female Third Party-Resources can avail this service, Subject to the Manager approval. In the absence of Manager, the approvals will be sought as follows:
        - For Analyst and equivalent: Line Manager
        - For Associate and equivalent: Self-approval
    - No separate approval will be required if VP and above female Third Party-Resources avail this service
    - For female Third Party-Resources who are undergoing new hire training (NHT), the approval will be sought from the Training department
- It is mandatory for all female Third Party-Resources to exit from the reception area (where the security guard is available) when exiting the office premises post 8:00 PM

Procedure

- A Helpdesk request must be raised with the FMS department under the category of ‘Ground Transport Services’ with the necessary details

- Requests must be raised and approved by the manager (as applicable) minimum one hundred and twenty (120) minutes prior to the departure (Considering it takes approximately one hundred and twenty (120) minutes to procure a car from the vendor and for it to arrive at the office location). The cars will be available at 9:00 PM, however in case the cars are occupied, it will help the transport coordinator to plan the trips to ensure minimum wait time
    - In case female Third Party-Resources inform the FMS department about their requirement less than one hundred and twenty (120) minutes prior to their departure, a justification will be sought from their Manager
- Requests will only be initiated after receiving the necessary approvals
- Incorrectly raised requests may lead to a delay in processing the requests
- Requests shared via any other platform (E.g., verbal requests, emails, Microsoft Teams, etc.) will not be processed. If the request is shared verbally or on Microsoft Teams, etc., please ensure you raise a request on the Helpdesk for official records

- Addresses updated on DarwinBox will be referred by the FMS department at the start of each quarter
    - In case the current residential address differs from the one mentioned on DarwinBox, a softcopy of the updated address proof (E.g., rent agreement, Aadhaar card, PAN card, driving license, etc.) must be attached as a one-time activity, while raising the request, after which FMS department will update the address in their records
        - Female Third Party-Resources in the initial ninety (90) days from the date of joining are exempted from providing a softcopy of their updated address proof, in case of a change in their residential address. However, they are mandatorily required to fill in their updated address on DarwinBox by 3:00 PM on any given day
        - Post completion of the initial ninety (90) days, female Third Party-Resources must mandatorily provide a soft copy of their address proof in case of change in their address
    - In case of change in address, female Third Party-Resources should ensure that their current address is updated on DarwinBox at the earliest
    - In case the current address is not updated on DarwinBox by the beginning of the next quarter, female Third Party-Resources will still be required to attach the address proof while raising the request
- Female Third Party-Resources should update their personal and emergency contact details on DarwinBox as soon as there is a change in these details
- Once the travel request is approved by the Manager, the FMS department will share the following details via email closer to the departure time, as applicable:

- Departure slot and pick-up location,
    - Female Third Party-Resources are required to be at the pick-up location five (5) minutes prior to their departure time
- Details of the car (vehicle type, number, etc.)
- Details of the driver and/or Male Representative (name, contact details, etc.)
- Do's and don'ts to be followed during the trip
- Link to the acknowledgement survey form which must be mandatorily filled in/responded by female Third Party-Resources on the safe arrival at their doorstep

- This service, basis the drop distances (within a reasonable limit from the office premises), will be provided in intervals of one hundred and twenty (120) minutes, on a first come first serve basis (Considering it takes approximately one hundred and twenty (120) minutes to procure a car from the vendor and for it to arrive at the office location)
    - Multiple female Third Party-Resources residing on the same route can be accommodated in one trip
    - No in between stops/halts will be allowed from the office premises to the residential address
- Conveyance reimbursements claimed by female Third Party-Resources for the days they opt for this service, will be rejected by the Corporate Finance department
- When female Third Party-Resources from other office locations are working from the Gurugram office, and wish to avail this service, they must include the following details while raising the Helpdesk request:
    - Email approval from their Manager to work from another office location (as an attachment)
    - Temporary address details
- Once female Third Party-Resources have been accompanied to their residence (doorstep) by the Male Representative, they must mandatorily:
    - Sign the travel receipt confirming that they have been safely dropped off at their residence (doorstep)
    - Respond and submit the acknowledgement survey form mentioned on the email shared by FMS department within fifteen (15) minutes of their arrival at their doorstep
    - A SPOC from the FMS department will call on the registered mobile number of the female Third Party-Resources to check on their safe arrival, if the response is not received within fifteen (15) minutes from the time they have been dropped off at their residence (doorstep)
    - In case the call is not answered, the FMS SPOC will call the emergency contact as mentioned on DarwinBox in next fifteen (15) minutes
    - In case emergency contact does not answer the call, the FMS SPOC will visit female Third Party-Resources address (as mentioned on the Helpdesk Ticket) in Person to verify their safe arrival

Non-Adherence to the Policy

- Not informing the FMS department of the safe arrival via the acknowledgement survey form after opting for the company-provided transportation service shall lead to Disciplinary Action which may include but not be limited to policy reminder, re-training, impact on review rating, issuance of warning letter, or termination

In case female Third Party-Resources do not utilize this service after the booking is confirmed, the applicable cancellation charges will be borne by them

(B) For All Third Party-Resources Exiting Office Premises Post 9:00 PM

Eligibility

This policy is applicable to all Third Party-Resources if they are exiting the office premises post 9:00 PM.

Particulars

- Third Party-Resources exiting the office premises post 9:00 PM can continue to claim conveyance expenses per the Reimbursements Policy (Refer to section 4 of this Handbook, under the header of monetary policies)
    - Female Third Party-Resources exiting the office premises post the legally mandated timelines (9:30 PM for Mumbai and Pune, and 8:00 PM for Bengaluru) must mandatorily sign the Declaration Register, if they do not wish to avail the Company-provided transportation service
    - Female Third Party-Resources exiting the office premises post 8:00 PM in Gurugram will have to mandatorily opt for the Company-provided transportation service
- It is mandatory for all Third Party-Resources to exit from the reception area (where the security guard is available) when exiting the office premises post the legally mandated timelines (9:30 PM for Mumbai and Pune, and 8:00 PM for Bengaluru and Gurugram)

IT Systems and Securities

4. IT Systems and Securities

TresVista provides its Third-Party Resources with the latest and most effective information technology and urges them to use the infrastructure optimally and responsibly.

TresVista encourages the use of electronic communications to share information and knowledge to conduct the Company's business. To this end, TresVista supports and provides information technology facilities which include all hardware, software, and services that TresVista provides to its Third-Party Resources to help them carry out their day-to-day official work ("IT Facilities"). An exhaustive list of all IT Facilities that the Company provides to its Third-Party Resources from time to time basis for official purposes will be communicated b the Supervisor and/pr the Company.

The following sections cover the usage of all of TresVista's IT Facilities, whether owned or leased by TresVista or are under TresVista's possession, custody, or control; and all users, whether on TresVista's property, connected remotely via any networked connection or using TresVista's equipment.

If any Third-Party Resources is found in violation of any of the policies below, it will lead to repercussions as per the compliance matrix.

4.1 IDs and Passwords

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

Third-party Resources must change their system passwords once every 30 days. Password can be changed remotely using 'Ctrl+Alt+End' keys. Third-party Resources must be connected to the authorized VPN Client before changing the system password. Third-party Resources can raise a Ticket with the Software Department for issues related to Microsoft Dynamics 365.

4.2 Data Usage

- All third-party Resources are responsible for managing their use of information Resources and are accountable for their actions relating to information resource security
- Third-party Resources can access their respective network drives/share point sites on Company laptops when they are connected to the authorized VPN Client
    - Network drives/SharePoint sites are backed up per the pre-defined Backup Policy
- Third-party Resources 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
    - Third-party Resources 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

- Third-party Resources using Company laptops should not leave the device unattended keeping in mind TresVista's Data Security Policy

4.3 Software and Hardware

Software includes purchased or licensed business software applications, Company-written applications, Third-party resource 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. Third-party Resources must use TresVista's computers and networks only for legal and authorized purposes.

- For computers dedicated for use by a single Third-party resource end-user
- At the end of each workday or if a third-party resource 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 Third-party resource wishes to log on to the system remotely, they should log off and switch off the monitor
- For a computer shared by multiple Third-party resource 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 Third-party resource immediately upon completion of their computer session
- Third-party Resources are responsible for the laptops provided to them by TresVista. In case of theft or damage, the third-party resource must notify the IT and Compliance Department immediately through an email
- In case of damage, third-party Resources 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 Third-party resource to whom the assets are assigned

4.4 Internet Policy

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

Particulars

- TresVista recognizes the business need for providing internet access to its third-party Resources and it is not to be treated as a basic facility, privilege or right of a third-party resource
- Third-party Resources are eligible to use internet services based on their role and prior approval from their respective Heads of Department/Supervisor
- Formal guidelines are established in order to control and regulate the use of internet in the Organization
- TresVista specifically prohibits third-party Resources 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
- Third-party Resources 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
- Illegal use of Internet facility shall call for Disciplinary Action Consequence Management Matrix
- Any breach in this policy results in Disciplinary Action being taken against the third-party resource. The Disciplinary Action may range from warning letter to Termination with Cause, at the discretion of the Organization

4.5 Email

Email facility is provided to Third-party Resources 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 wrongful 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 third-party Resources using the following applications:
- Microsoft Outlook available from within TresVista premises and on Company-issued laptops
    - Mobile device Management application installed on Third-party Resources' compatible Personal Smartphones (Android/iOS)

Third-party Resources must:

- Not expect privacy, as the IT Department and Management may review any emails at any point in time
- Set up out-of-office replies as per their Supervisor'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 engagement of the Third-party resource, 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

4.6 Telecommunication

Smartphones

As per the designations/roles of the third-party Resources, it may be mandatory for some of them to have a smartphone with a valid talk-time and data plan at all possible times. The data plan on the personal phones of such third-party Resources must at least allow email communication. Internet browsing is optional.

4.7 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 third-party resource's smartphones, it is pushed through Microsoft Intune application which is a secure MDM platform managed centrally by the IT Department.

4.8 Social Media

The purpose of this policy is to define guidelines and best practices for Third Party-Resources 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 Third Party-Resources 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, Instagram, Snapchat)
- Video and photo sharing websites (e.g., Flickr, YouTube, BeReal, Pinterest)
- Blogs and Vlogs, 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, Reddit, Quora)
- Video on Demand (VOD) and Podcasting
- Status updates/profile bio on messenger services (e.g., Blackberry Messenger, WhatsApp, Telegram, Facebook Messenger, or any other instant messaging application)

- Geospatial Tagging (e.g., Foursquare, and other networking or check-in sites)
- Interviews, columns or talk shows (e.g., Television, print media or radio)

Applicability

This policy is applicable to all Third Party-Resources.

Particulars

- Third Party-Resources are not permitted to:
  - Use TresVista's name and refer or state that they are working at TresVista across any social media platforms or reveal any confidential/sensitive information in any form
    - If the Third Party-Resources wish to update their social media account (e.g. LinkedIn) with details of their current role, they may mention the name of the employer as 'Financial Services Firm' or 'Major Financial Services Firm'
  - Post any information about TresVista, that is confidential, propriety or related 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, Third Party-Resources should be vigilant that no further details are mentioned (e.g., working with the biggest Middle Eastern Non-Sovereign PE firm)
    - Third Party-Resources can refer to the Data Classification Policy and reach out to their Managers in case of any queries. In case of further queries Managers are required to redirect the Third Party-Resources to 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/Third Party-Resource 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 Third Party-Resource may be Subject to Disciplinary Action
- Tag the Company's official account in any of the posts or comments

- Third Party-Resources must refrain from engaging in inappropriate posts, including but not limited to threats of violence, dishonourable content such as racial, ethnic, sexual, religious, physical disability slurs, etc. shall not be tolerated in any form and may be subject to disciplinary action
- Third Party-Resources should be aware that the Company may observe content and information made available by them on social media platforms
- Third Party-Resources must refrain from publishing or engaging in rumours that can have a significantly adverse impact on the Company's reputation
- Third Party-Resources should use their best judgment in posting content that is neither inappropriate nor harmful to the Organization, other Employees, Third Party-Resources or Clients
- Third Party-Resources must refrain from any unauthorized brand, political advocacy, unauthorized endorsement or appearance of endorsement by TresVista; to be mentioned that do not reflect the interests of the company
- TresVista reserves the right to request the withdrawal of any posts, comments, or content from any social media platform (including internal platforms). Third Party-Resources must be aware that some forms of internet conduct may be open to criminal prosecution and lead to Disciplinary Actions
- Third Party-Resources can refer to the Social Media guidelines document and the compliance manual for additional recommendations for social media etiquette, compliance, and conduct

Exception to this Policy:

- **LinkedIn:**
  - Third Party-Resources from certain departments with prior permission can mention TresVista on various social media platforms due to their job profiles and KPIs (E.g. TA)
  - Third Party-Resources who have been granted with or are in possession of stock options of TresVista are permitted to mention TresVista on LinkedIn
- **Instagram:**
  - Instagram has an umbrella exception for the social media policy where all Third Party-Resources are allowed to mention and interact with the official TresVista account
  - Third Party-Resources are expected to follow the guidelines mentioned below while engaging with TresVista's official Instagram account:

- Third Party-Resources are allowed to mention TresVista as their employer on personal bio/profile
- Tagging or hash tagging TresVista on their posts, stories, highlights, reels, location, and other engagement features on Instagram
- Follow the official TresVista Instagram profile, comment, like, repost, and otherwise engage with the page using different features of the platform, and tagging fellow employees on the posts to increase engagement

- Third Party-Resources are expected to follow the general guidelines mentioned in the 'Particulars' section of this policy while engaging with TresVista's official Instagram account

Disclosure to the Media:

Third Party-Resources with prior permission are allowed to engage with external parties or participate in any external interaction while representing TresVista. External Interactions are defined as:

- Testimonial to Clients/Vendors/Prospective Clients/Potential Employees/CSR Partners/Other Affiliates
- Endorsements for Clients/Vendors/Prospective Clients/Potential Employees/CSR Partners/Other Affiliates
- Media Interactions, including but not limited to press quotes, interviews, guest articles, and any other spoken or written interaction with the media
- Webinars/Seminars/Podcasts/Workshops/Educational Talks/Lectures/Campus Engagement and Placement talks/Networking Events that they are attending as TresVista representatives

Third Party-Resources can reach out to Marketing and Corporate Communications department; in case they wish to appear for above mentioned interactions.

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
- Third Party-Resources are required to adhere to the guidelines mentioned in this policy and the Compliance Manual, when using social media with reference to the Organization
- Marketing and Corporate Communications department will conduct monthly audits to ensure adherence to this policy

Non-Adherence to the Policy

Any non-adherence to this policy shall lead to Disciplinary Action which may include but not be limited to policy reminder, re-training, impact on review rating, issuance of warning letter, or termination.

4.9 Confidentiality Policy

The purpose of this policy is to educate third-party Resources on the protection of Confidential Information of Company, Clients, etc. received by them during the course of their engagement.

Applicability

This policy applies to all third-party Resources of TresVista.

Particulars

- To ensure that Confidential Information is well protected, third-party Resources should only disclose information on "need-to-know" basis.
- Third-party Resources 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 third-party resource'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 third-party Resources must execute a Non-Disclosure Agreement (NDA) and submit it to the HR Operations team (ops@tresvista.com). In case third-party Resources are working out of office premises, they may submit NDA via email as prescribed by the HR Operations team

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 third-party Resources) also forms a part of the Internal Audit to ensure confidentiality

Non-Compliance

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

4.10 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 third-party Resources, who process, have access to, or store sensitive Client and Company data.

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.

Information

- 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

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, third-party Resources 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
- A designated data owner is responsible for managing all the data under their purview
- The data classification matrix provides classification on data as well as an overview of the access rights given to third-party Resources

Data Owners

- Data owners are at VP/EVP/SVP and equivalent designations
- Data owners are responsible for abiding by the appropriate sensitivity classifications as defined by the Client
- 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 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 sexual orientation, etc.

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 (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 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 third-party Resources within the Company. All such data is labelled as internal
  - The unauthorized disclosure, modification or destruction of this information could expose the Company, third-party Resources, or its business Partners to a moderate level of risk. (E.g., Company telephone directory, new third-party resource 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 third-party Resources 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, third-party Resources, 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., third-party resource 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 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
  - The IT administrator, in consultation with the data owner, conducts this evaluation and accordingly makes the necessary changes 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 third-party Resources 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 attracts Disciplinary Actions as defined in the annexures of this document.

4.11 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, third-party Resources, visitors, or vendors
  - Incidents or breaches that have occurred and those that were a ‘near miss’
- Third-party Resources 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:**
  - Third-party Resources are required to report all data privacy issues (including potential or suspected incidents or breaches) as soon as possible
  - In the event of a data privacy issue which involves a third-party resource or another Person within their team and/or area of responsibility, Supervisors 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 between the timeline of reporting and 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

Investigation and Resolution

- On intimation from third-party Resources, 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
Compliance	Compliance department requests.compliance@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.

4.12 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.)

Applicability

This policy applies to all the third-party Resources of TresVista.

Particulars

- **Procedure:** This policy outlines the procedure for managing:
  - Incidents that may occur within/outside TresVista premises, including those that involve service users, third-party Resources, 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 the compliance manual

Responsibility

- **Third-party resource:** Third-party Resources are required to report all incidents (including potential or suspected incidents) as soon as they become aware of it
- **Supervisor:** In the event of an incident involving a third-party resource or another Person within their team and/or area of responsibility, Supervisors 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 third-party Resources should report incidents to their Supervisors 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
  - Third-party Resources should observe and report suspected incidents as soon as possible
- **Incident Evaluation/Severity:** On intimation from third-party Resources, 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 third-party Resources 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 third-party Resources from performing a portion of their duties	Issue prevents the third-party Resources 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
  - A root cause analysis of the incident is done and recorded in the incident log on Helpdesk for future reference 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 nilay.vyas@tresvista.com	NA
IT	IT Department IT@tresvista.com	IT Department abdulbari.ansari@tresvista.com	NA
Human Resources	HR Department compensation2@tresvista.com ops@tresvista.com	HR Department charmi.shah@tresvista.com shruti.tendulkar@tresvista.com	HR Department faraaz.lodhi@tresvista.com minali.dalal@tresvista.com
Facilities Management Services (FMS)	FMS Department FMS@tresvista.com	FMS Department abdulbari.ansari@tresvista.com	NA

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 attracts Disciplinary Actions as per the annexure

4.13 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 (including concerned and relevant Third Party Resources).

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
  - Third-party Resources' access to Company data is limited based on third-party resource profiles as defined by IT department and the access is automatically enforced

Network Access Control:

- Unique third-party resource IDs and passwords should be used for every third-party resource to maintain individual accountability of internet, intranet, and e-mail resource usage (Details can be referred to in user ID and password below)
- Access to the network is provided to third-party Resources for the purpose of business operations and made available only from the third-party resource's Company device with a unique third-party resource 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 third-party Resources 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/SVPs (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 third-party Resources according to the whitelisting process. If approval is granted to use these systems and information, the third-party resource is required to login using the unique third-party resource ID and password
  - Generic logins are not permitted across TresVista, unless for exceptional circumstances with appropriate monitoring controls

User Registration/De-registration Control:

- When a third-party resource joins TresVista, the IT administrator on receipt of information from the HR Operations team (ops@tresvista.com), shares with the respective VPs/EVPs/SVPs (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 third-party resource's system
- If the VPs/EVPs/SVPs or equivalent deems it unfit or inappropriate for a third-party resource 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 a third-party resource is on leave for more than one (1) month, the respective VPs/EVPs/SVPs or equivalent informs the IT administrator to alter/remove the third-party resource's access rights. Such changes are reflected in the access matrix to accurately reflect access records
- On resignation/termination of a third-party resource, the IT administrator backs up the necessary user data which is to be archived and disables the login ID of such third-party Resources

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 Supervisors, 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 third-party Resources 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 IT Security Team, 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 (E.g., research work on social networking)
  - VPs/EVPs/SVPs and the IT Security Team 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 IT Security Team, 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

- VPs/EVPs/SVPs and the IT Security Team 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 a third-party resource 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 IT Security Team, 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 IT Security Team. However, third-party resource 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 third-party Resources through offline sync folder. Only IT administrator can manage accesses on the file sharing platform through web portal
  - Third-party resource must take acceptance of responsibility from the Client for revoking accesses (Details can be referred in Annexure C)
    - The template is available in Annexure C of this Handbook
  - VPs/EVPs/SVPs and the IT Security Team 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 third-party resource 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 third-party resource. 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 third-party Resources to work from other location/home
- To take remote access of the system, third-party Resources 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 third-party Resources 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 third-party resource's handset for accessing work emails along with limited access to the internet (Details can be referred to in section 4.13 of this Handbook)
- 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 a third-party resource 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 third-party Resources 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 third-party resource's device is remotely wiped if:
  - The device is lost
  - The third-party resource terminates his/her engagement
  - 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 section 4.15 of this Handbook

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

- Third-party resource user IDs and passwords help maintain individual accountability for the internet, intranet and email resource usage. Third-party Resources are responsible for all activities on their username/account ID
- Sharing or using another third-party resource's user IDs or passwords to obtain access to the internet, intranet or email is prohibited
- Third-party Resources 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 four (4) 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

Third-Party Resource Awareness

At TresVista, IT security training is provided to all new third-party Resources 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 attracts Disciplinary Actions as defined in the annexures of this Handbook.

4.14 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 third-party Resources 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 third-party Resources (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 last 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 third-party resource found to have violated this policy is subjected to Disciplinary Action, as determined by the Organization.

4.15 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 third-party Resources the privilege of accessing emails on their devices for their convenience.

Applicability

This policy applies to all third-party Resources of TresVista.

Particulars

Third-party Resources 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 third-party resource'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 third-party resource joins the Company, they must present their devices to 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 third-party resource's personal device remotely
- IT department does not provide support in case the device has issues with the hardware and operating system
- Third-party Resources have their official email ID configured through the MDM application (Mircosoft Intune) only on one device

Security

- Third-party Resources 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 third-party Resources 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
- Third-party Resources' 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
    - Third-party Resources can use their personal email ID during non-working hours to report such incidents to IT department at IT@tresvista.com
    - Third-party Resources 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 third-party resource is on leave and the old device cannot be submitted, the device owner must seek approval from their respective VPs/EVPs/SVPs (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
- The Compliance department also conducts surprise end user checks and other necessary periodic audits as and when necessary

Non-Compliance

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

4.16 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 third-party Resources of TresVista.

Particulars

- **Biometric Access:**
  - A biometric system is installed to restrict the access of third-party Resources 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 manual
    - The secured zones access matrix is available on SharePoint
- **Tailgating:** Third-party Resources are not allowed to tailgate and should use the biometric system while entering areas wherever access control is applicable
  - Third-party Resources 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 third-party resource, 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 third-party Resources:
    - 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, third-party Resources 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, third-party Resources need to seek prior approval from their Supervisor and the Compliance department via a Helpdesk Ticket
  - Third-party Resources are not allowed to carry any Company documents (including notepads) outside the office premises. In exceptional cases, if required, third-party resource 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	Supervisor Compliance department (Authorities reserve the right to ask third-party resource for details of project, etc.)

- **Bag Checks:**

- Bag checks are conducted periodically to prevent unauthorized movement of official documents outside office premises
- All official Client related print outs are taken on colored papers by default for easy identification and differentiation of work documents from personal documents
- Non delivery teams having access to white paper printers are subject to bag checks for all documents including white papers
- All official information should only be recorded on notepads provided by TresVista or which have the TresVista logo printed for easy identification and differentiation of work documents from personal documents. In case notepads which are not provided by TresVista, or do not have the TresVista logo are found with official information during bag checks, it is considered as a violation of this policy and third-party Resources may face Disciplinary Action
- All documents (including notepads) received as a part of training, or which have the TresVista logo printed should be carried outside the office premises only with prior approval by raising a Helpdesk Ticket. If such documents are found during the bag checks without approval, it will be considered as a violation of this policy and shall attract necessary Disciplinary Action
    - Personal documents can only be printed from the printers in the terminals/kiosks. If personal documents are printed on colored papers without prior approval and this is detected during a bag check, it will be considered as a violation of this policy and shall attract Disciplinary Action

- **Desk Security:**
- All third-party Resources 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
- **Visitor Access (Parents, Friends, Relatives of Existing/Prospective Joiners):**
    - Office visits can be held on any day of the week at the discretion of the confirmed third-party resource/Supervisor
        - Supervisors should encourage Prospective Joiners to visit the office and recommend that it is done in groups. However, the visit is finalized at the Supervisor's discretion/availability
    - Only adults (aged 18 and above) are permitted to visit the office premises

- Visitor responsibility:
    - Prospective Joiners and their friends/family/relatives: Respective Supervisors (VPs and above, given that it is a part of Supervisor engagement)
    - Friends/family/relatives of existing third-party Resources:
        - In case the third-party resource is confirmed, the third-party resource themselves are responsible
        - In case the third-party resource is on Probation or serving notice, the third-party resource's Supervisor is responsible
    - In cases wherein Supervisors are not based out of the same location, responsibility is assigned to the next Supervisor one level up/down, as defined below:
        - Prospective Joiners: One level down (Senior Associate/Associate and equivalent)
        - Existing third-party Resources (if on notice or on Probation): One level up (skip Supervisor)
- In case Supervisors of the prospective/existing third-party Resources (on notice or on Probation) are not based out of the same office location, their request cannot be considered under this policy

- **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 Supervisor
- **Points to Note:**
    - **Pre-visit Formalities:** FMS department needs to be informed of office visits latest by 4:00 PM, at least one (1) working day in advance, via a Helpdesk Ticket (Category: Gate pass for visitor/vendor/guest)
    - **Inside the Office Premises:**
        - Visitors can take a quick tour of the office, after which they are seated in the reception area and third-party Resources can reach out to the FMS department if they require any additional assistance (E.g.: Water, coffee, etc.)
        - Visitors are not permitted to enter areas that require additional access (E.g.: HR, Legal, Software cabins, etc.)
        - Visitors should adhere to the compliance guidelines defined by the Company, to the extent applicable (E.g.: Some processes such as Tailgating, biometric access, etc., are not applicable)
        - In order to visit the office premises, all visitors should be double vaccinated, carry proof of vaccination, and adhere to the safety guidelines defined by the Company, including but not limited to temperature checks, wearing masks in common areas (in accordance with the ongoing Company guidelines), etc.

Compliance

- The Compliance department conducts periodic checks on the following:
  - Desk security
  - Shredding of unattended documents
  - ID cards
  - Tailgating
  - Visitor's and vendor's register and visitor's pass file
  - Number of visitor/vendor IDs available at the reception against the number of IDs issued to the security
  - Bag checks and frisking of third-party Resources (female third-party Resources are frisked by another nominated female third-party Resources only)
- The department will also be conducting periodic Internal Audits, surprise checks, or any other checks as to ensure adherence to the policy

Non-Compliance

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

4.17 Policy for Material Non-public information

The purpose of this policy is to ensure that any Confidential Information about the Company, Clients, etc. received by third-party Resources during the course of their engagement 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) about any Company or any of its subsidiaries, and
- Disclosing MNPI to outsiders ("Tipping")

Objective

- Set out procedures to restrict third-party Resources from trading in Personal Accounts using MNPI for personal gain/benefit
- Educate third-party Resources about MNPI, Tipping and promote TresVista's ongoing commitment to compliance with all applicable insider trading Laws
- Assist third-party Resources in meeting their responsibilities in terms of complying with these Laws and internal policies

Scope

This policy applies to:

- All third-party Resources of TresVista
- All transactions in securities of a Client Company, MNPI of which the third-party resource has obtained during the course of their engagement with TresVista

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

- **Tipping:** For this policy, Tipping is defined as passing or providing access of MNPI about a Client Company by the third-party resource 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 third-party Resources 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
- Third-party Resources should share information on a need-to-know basis
- If a third-party resource 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 third-party resource 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 third-party Resources 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 third-party Resources during the term of their engagement
- If third-party Resources 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, third-party Resources are also required to adhere to the applicable policies /clauses detailed out in the Compliance Manual and the Third Party Resource Handbook

Treatment of MNPI

- Guidelines and procedures which form a part of this policy and the Compliance Manual 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 third-party resource becomes aware that MNPI is inadvertently disclosed by another third-party resource, 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 third-party Resources
    - Transaction holding period to ensure that no trades have been carried out by third-party Resources who are in possession of MNPI
    - Disclosures provided by third-party Resources 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., are considered for immediate Termination with Cause 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
- Third-party resource also incurs penalties for such violations by Tipping information to others, even if the third-party resource has not personally gained any profit from the other Person’s actions

Leave and Holidays

5. Leaves and Holidays

The leaves and Holidays shall be governed by the understanding between the Company and the third-party resource's Employer. The leaves applicable to the third-party resource will be as per the policy of their Organization as enumerated in the contract between the Company and the third-party Resources' Employer and as per applicable Laws.

Exit

6. Exit

TresVista aims to provide a smooth and consistent process for terminating the engagement, and it shall be governed in accordance with the terms of the Agreement between the Company and Employer of the Third-Party Resource.

6.1 Termination with Cause

The Company herein shall have the right to terminate for cause the engagement of a third-party resource for the following (inclusive and not exhaustive) grounds:

- Material failure to observe the performance standards set by the Supervisor or in carrying out their duties
- Unsatisfactory performance during training period
- Failure or inability to provide any undertakings as may be reasonably requested in accordance with policies, procedures and rules on the conduct that the Company expects from its Third-Party Resource within a reasonable period of time or any censure or fining of you by the relevant regulatory authority
- Misconduct as identified by the Supervisor
- Negligence in connection with or affecting the business of the Company or any Associated Company
- Wilful disobey of a lawful or reasonable order by a third-party resource
- Third-Party Resource found guilty of Fraud or dishonesty
- Serious or persistent breach or no observance of any of the Company's policies, terms and conditions asmentioned in this Handbook (as amended from time to time)
- Taking any bribes or improper gifts/ kickbacks
- Any action or behaviour that creates a potentially unsafe working environment
- Conduct which is likely to bring the Company, Management or Clients into disrepute or conviction of a criminal offence
- Refusal to submit to a drug test or failure in any drug test administered by an institution or named physician selected by the Company
- The information given by the Third-Party Resource in connection with their personal details and/or their past service is found to be untrue
- A third-party resource being actively involved in any other business or income generating venture, without prior approval from the Supervisor

- Third-Party Resource having solicited or accepted engagement elsewhere before providing notice of termination of engagement to the Company, without prior approval of the Supervisor
- Any prior regulatory fine or censure, litigation, crime, or involuntary termination of any prior engagement affecting the Third-Party Resource, or any report from the Company's background checking agency or referencing the Company considers unsatisfactory
- Third-Party Resource is away from work and on leave without any official notice for a period of 48 hours, and further refuses to respond to any communication attempted to find about his/her whereabouts
- Sexual harassment of a woman in the workplace in accordance with section 2.6

6.2 Exit Formalities

All exiting third-party Resources must complete a set of formalities prior to their last working day before they can be relieved from their services.

Exit Checklist

- Exit clearances are triggered on the third-party resource's last working day through DarwinBox. These clearances comprise of a list of formalities that need to be completed when Third-party Resource leaves the Organization. The clearances, with the required signoffs from the concerned stakeholders, must be completed on DarwinBox
- Third-Party Resources should mandatorily work from office on their Last Working Day
- Third-party Resources must return all Company property including, but not limited to, any Company equipment, storage devices, training manuals, keys, documents, correspondence, records, credit cards, and passes which are in their possession or under their control. They must sign the resource return form (as applicable) on their last working day

No Due Certificate

All third-party Resources are required to submit the third-party resource task sign-off on DarwinBox, on their last working day. Exit formalities are not processed for third-party Resources who fail or refuse to adhere to the obligations.

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. **Aggrieved Woman:** A woman who alleges that she has been subject to sexual harassment at the workplace
3. **Agreement or Offer Letter:** The agreement that specifically sets out the terms and conditions, and the scope of engagement of the third-party resource at TresVista
4. **Alleged Perpetrator:** One against whom allegations of sexual harassment have been made
5. **Client:** Persons or entities to which the Company has sold any Products or for which the Company has performed any services
6. **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
7. **Commercialize:** Manage or exploit in a way designed to make a profit
8. **Company/Organization/Firm/Employer:** TresVista and its subsidiaries and affiliates as below under "TresVista"
9. **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 third-party resource during the course of engagement 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 you, 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

10. **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
11. **Corporate Finance Department:** All Employees in the Corporate Finance Department at TresVista
12. **Contractual Employee:** The employee retained by a Company for a predetermined time and renumeration
13. **Declaration Register:** Register kept at the reception across all office locations for TresVista's female Third-Party Resources to sign in case they exit the office premises post the legally mandated timelines, as applicable for each location and choose not to opt for the Company-provided transportation service
14. **Dependent Parents:** Any legal guardians, or legally verifiable mother and father, whether biological or otherwise, of a third-party resource who are emotionally, physically or financially dependent on the third-party resource for the purpose of their subsistence. For the purpose of this policy, Dependent Parents shall not include in-law relatives of a third-party resource
15. **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 third-party resource, in whole or in part that arises during engagement with the Company, or that are otherwise made through the use of the Company's time or materials
16. **Disciplinary Action:** This indicates any action that can be taken on the completion of investigation proceedings including but not limited to a warning, imposition of fine, suspension from official duties or any such action as is deemed to be fit considering the gravity of the matter
17. **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
18. **FMS support staff:** Employees/Third-Party Resources hired for facility Management and operations
19. **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 3.8 of this Handbook
- Any similar or related inappropriate conduct

20. **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
21. **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 agreement and offer letter
22. **Holiday:** Firm-wide Holidays, or day offs as declared by the Firm

23. **HR Department:** All Employees in the human resource teams at TresVista
24. **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
25. **Intellectual Property:** All the Intellectual Property rights, whether registered or unregistered and includes all computer software, Patents, trademarks, trade names, service marks, service names, Copyrights, Inventions, other proprietary Intellectual Property rights, applications and registrations therefore and licenses or other rights in respect thereof necessary for use in connection with the business of the Company
26. **Internal Audit:** An independent service to evaluate the Company's internal controls, its corporate practices, processes, and methods
27. **Inventions:**
    - Developments, Know-how and Intellectual Property, which a third-party resource 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 trademarks, Patents, designs, Copyrights including design Copyrights, Inventions, service marks, internet domain names, processes, geographical indications, 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 or improvements upon or in addition to an invention, 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
28. **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 third-party Resources have become acquainted with during the term of their engagement), 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
29. **Law:** All applicable 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 in India

30. **Male Representative:** A resource appointed to acCompany TresVista's female Third-Party Resources in case they exit the office premises post the legally mandated timelines, as applicable for each office location, and choose to opt for the Company-provided transportation service under the Travel and Security Policy
31. **Management:** The managing directors, and any other authorized third-party resource of TresVista
32. **Supervisor:** Any individual designated as such by the Organization from time to time. For the purpose of this document, Supervisors refers to VPs and above, as applicable, unless mentioned otherwise
33. **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
34. **Non-Disclosure Agreement (NDA):** A legally binding contract between the Company and the third-party Resources that prevents sensitive information from being shared with unauthorized personnel
35. **Non-public information:** Any information about the Client Company that has not been publicly disclosed is considered as Non-public information
36. **Notice Period:** The party who is terminating engagement will give to the other advance notice in writing, with such notice not to be less than the period indicated in the third-party resource's offer letter or as specified in subsequent Promotion letters
37. **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 third-party resource of the Company for the Company or any Person for which the Company provides advisory, consultancy or Management services
38. **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
39. **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
40. **Permanent Employee:** The third-party Resources who work for and are directly on the payrolls of TresVista without a predetermined end date for the engagement at hand
41. **Perpetrator:** One against whom allegations of sexual harassment have been proved, based on the Inquiry conducted by the IC
42. **Person:** An individual, Firm, limited partnership, limited liability partnership, Company, association, corporation or other Organization

43. **Personal Account:** Any social media account created by third-party Resources for their personal use
44. **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
45. **Podcasting:** The practice of using the internet to make digital recordings of broadcasts available for downloading to a computer or mobile device
46. **Probation:** Period during which a Supervisor closely evaluates the progress and skills of a newly hired third-party resource, determines appropriate assignments and monitors other aspects of the third-party resource
47. **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
48. **Promotion:** The recognition of a third-party resource's effort, work contribution, and success. The third-party resource's designation and compensation structure will change with effect of a Promotion
49. **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
50. **Prospective Joiner:** People who are most likely join the Company in the near future
51. **RIS:** Research and Investment Services department is divided into smaller teams
52. **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 Third-Party Resources for the performance of their responsibilities at TresVista
53. **Royalty:** A sum paid to a patentee for the use of a Patent or to an author or composer for each copy
54. **Scrip:** A certificate entitling the holder to acquire possession of certain portions of public land
55. **Sensitive Personal Data:** Sensitive 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 sexual orientation, etc.

56. **SharePoint:** A common site through which all Third-Party Resources can access information including but not limited to TresVista Handbooks, templates, policies, training manuals, Organization chart, etc.
57. **SPOC:** Single point of contact
58. **Tailgating:** A physical act of security breach in which a third-party resource enters/leaves the office premises or secured zones without using biometric access
59. **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
60. **Third-Party Resources:** Resources hired by TresVista's sub-contractor
61. **Termination with Cause:** Termination of engagement without any notice considering the grounds mentioned in the section 6.1 of this Handbook
62. **Ticket:** A mode of communication used to raise requests/incidents via the 'Helpdesk Support' module on Microsoft Dynamics 365
63. **Tipping:** Passing or providing access of Material Non-public information about a Client Company by the third-party resource 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
64. **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"
65. **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
66. **Video on Demand (VOD):** Technology for delivering video content, such as movies and television shows, directly to individual customers for immediate viewing
67. **Whistle Officer**: This means an officer who is appointed to conduct a detailed investigation of the disclosure received from the whistle-blower and recommend Disciplinary Action

Annexure

Annexure A: Consequence Management Process

Any non-compliance with the requisite Practice/Process will attract Disciplinary Actions as specified in the Consequence Matrix:

A. Physical Security Policy - Nominal

Breach	Breach1	Breach2	Breach3	Breach4	Breach5 & Above
Tailgating	Policy Reminder	Monetary Impact - INR 1000/-	Monetary Impact - INR 2000/-	1) Third-party resource - Monetary Impact - INR 4000/- 2) Line Manager – Monetary Impact – INR 1000/-	1) Third-party resource - Monetary Impact - INR 8000/- 2) Line Manager – Monetary Impact – INR 2000/-
Failing to display ID cards	Policy Reminder	Monetary Impact - INR 1000/-	Monetary Impact - INR 2000/-	1) Third-party resource - Monetary Impact - INR 4000/- 2) Line Manager – Monetary Impact – INR 1000/-	1) Third-party resource - Monetary Impact - INR 8000/- 2) Line Manager – Monetary Impact – INR 2000/-
Carrying personal documents outside in colored paper without approval	Policy Reminder	Monetary Impact - INR 1000/-	Monetary Impact - INR 2000/-	1) Third-party resource - Monetary Impact - INR 4000/- 2) Line Manager – Monetary Impact – INR 1000/-	1) Third-party resource - Monetary Impact - INR 8000/- 2) Line Manager – Monetary Impact – INR 2000/-

Drawer keys unattended / Drawers unlocked	Policy Reminder	Monetary Impact - INR 1000/-	Monetary Impact - INR 2000/-	1) Third-party resource - Monetary Impact - INR 4000/- 2) Line Manager – Monetary Impact – INR 1000/-	1) Third-party resource - Monetary Impact - INR 8000/- 2) Line Manager – Monetary Impact – INR 2000/-
Computer unlocked	Policy Reminder	Monetary Impact - INR 1000/-	Monetary Impact - INR 2000/-	1) Third-party resource - Monetary Impact - INR 4000/- 2) Line Manager – Monetary Impact – INR 1000/-	1) Third-party resource - Monetary Impact - INR 8000/- 2) Line Manager – Monetary Impact – INR 2000/-
Clicking Pictures in office premises	Policy Reminder	Monetary Impact - INR 1000/-	Monetary Impact - INR 2000/-	1) Third-party resource - Monetary Impact - INR 4000/- 2) Line Manager – Monetary Impact – INR 1000/-	1) Third-party resource - Monetary Impact - INR 8000/- 2) Line Manager – Monetary Impact – INR 2000/-
Documents unattended at desk & Printer	Policy Reminder	Monetary Impact - INR 1000/-	Monetary Impact-INR 2000/-	1) Third-party resource - Monetary Impact - INR 4000/- 2) Line Manager – Monetary Impact – INR 1000/-	1) Third-party resource - Monetary Impact - INR 8000/- 2) Line Manager – Monetary Impact – INR 2000/-

Visitor unattended	Policy Reminder	Monetary Impact - INR 1000/-	Monetary Impact-INR 2000/-	1) Third-party resource - Monetary Impact - INR 4000/- 2) Line Manager – Monetary Impact – INR 1000/-	1) Third-party resource - Monetary Impact - INR 8000/- 2) Line Manager – Monetary Impact – INR 2000/-

B. Physical Security Policy - Severe

Breach	Breach 1	Breach 2
Carrying Client document outside office premises without approval	Warning Letter	Termination
Carrying documents with TresVista logo outside office premises without approval	Warning Letter	Termination
Carrying Company assets outside office location	Warning Letter	Termination
Employee bringing their laptop without prior approval	Warning Letter	Termination

C. Confidentiality Policy - Severe

Breach	Breach 1	Breach 2
Discussing/sharing Client related information/any Company proprietary data outside the Organization without legitimate reason	Warning Letter	Termination

Use of TresVista/Client information for personal benefit	Warning Letter	Termination
Discussing/sharing Client related information/ Illustration with individuals internal to the Organization without legitimate reason	Warning Letter	Termination
Sharing user ID password of Client Portal/tools with unauthorized employee	Warning Letter	Termination
Sharing user ID password	Warning Letter	Termination

D. Gift Policy - Severe

Breaches	Breach 1	Breach 2
Accepting gift from business associates within the Firm	Warning Letter	Termination
Accepting gift from Vendors/Outsiders for personal benefit	Warning Letter	Termination
Accepting gift from Client above the threshold	Warning Letter	Termination

E. IT Security, Acceptable Usage & Personal Device Policy - Nominal

Breach	Breach1	Breach2	Breach3	Breach4	Breach5 & above
Damage of Company asset	Policy Reminder	Monetary Impact - INR 1000/-	Monetary Impact - INR 2000/-	1) Third-party resource - Monetary Impact - INR 4000/-	1) Third-party resource - Monetary Impact - INR 8000/-

				2) Line Manager – Monetary Impact – INR 1000/-	2) Line Manager – Monetary Impact – INR 2000/-
Falling prey to phishing attack	Policy Reminder	Monetary Impact - INR 1000/-	Monetary Impact - INR 2000/-	1) Third-party resource - Monetary Impact - INR 4000/- 2) Line Manager – Monetary Impact – INR 1000/-	1) Third-party resource - Monetary Impact - INR 8000/- 2) Line Manager – Monetary Impact – INR 2000/-

F. IT Security, Acceptable Usage & Personal Device Policy - Severe

Breaches	Breach 1	Breach 2
Download/Using password of Microsoft Intune in unauthorized device	Warning Letter	Termination
Clicking screenshot of TresVista/Client data	Warning Letter	Termination
Communicating of TresVista/Client data over WhatsApp etc.	Warning Letter	Termination
Use of Privilege access for non-business purpose/personal benefit	Warning Letter	Termination
Employee accessing the folder, domain, website and emails which is unauthorized	Warning Letter	Termination
Falling prey to phishing attack via communication e.g.: Office landline, telephone call etc.	Warning Letter	Termination

G. Incident & Data Privacy Policy - Severe

Breaches	Breach 1	Breach 2
Privacy breach Data type - Internal - Data within TresVista	Warning Letter	Termination
Privacy Incident Restricted and Confidential - Data within TresVista	Warning Letter	Termination
Privacy Incident Internal, Restricted and Confidential - Data outside TresVista	Warning Letter	Termination

Annexure C: 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)