India Handbook

Table of Content

Welcome

It is our privilege to welcome you to Tredence Analytics. We wish you every success in your new job, and we hope that you quickly feel at home. This Handbook was developed to describe some of the expectations we have for all our employees and what you can expect from us. We hope that your experience here will be challenging, enjoyable, and rewarding. Again, welcome!

Disclaimer

This Employee Handbook ("Handbook") is a compilation of personnel policies, practices, and procedures currently in effect at Tredence Analytics.

The Handbook is designed to introduce you to our Company, familiarize you with Company policies, provide general guidelines on work rules, benefits and other issues related to your employment, and help answer many of the questions that may arise in connection with your employment.

The Company reserves the right to modify any of our policies and procedures, including those covered in this Handbook, at any time. We will seek to notify you of such changes by email and other appropriate means. However, such a notice is not required for changes to be effective.

Employee Handbook Acknowledgement

The employee handbook has been vetted by the Human Resources team and acknowledged by the COO.

General Guidelines for The Employees

You will be introduced to your Manager, Team Members & Teams across the floor

New Joiner Info

- You will receive an email with the new employee ID
- HR will also mail the new Joinee information that needs to be completed and submitted
- Welcome kit will be shipped to your address post your joining

Salary Account Creation

- The salary account needs to be either HDFC / IDFC account only
- The HR team on Day 1 will schedule a call with HDFC and IDFC for the bank account creation between 3pm to 4pm every Monday and Thursday
- Employees will need to share their bank account details on the MS form shared by the HR Operations team on or before the 15th of the month

Payroll

- Our payroll cut-off is 15th of every month, hence if you join us on or post 16th of the month you will receive your salary along with next month payroll
- You need to ensure you have shared your bank account details as well as declared your investment before the 15th of the month on the system

Provident Fund

You will be handed over the PF forms i.e., Form 2, Form 11. PF sample copies (guide to fill) will be shared by the HR Team.

- Fill Form 2
- Fill Form 11 (Fill Form 11 which requires all the previous employer details)
- Fill Form 13 – Process flow for online transfer will be shared with you
- Also share your UAN number for PF (in case you don't have one we would create one for you)
- Share your PF passbook copy

HRIS

You will receive a login ID & password email for our HRIS tool SuccessFactor from the HR team on your Day 2 and you will need to ensure you are uploading all your personal information on the system within a week of your joining.

CODE OF CONDUCT

This Code of Conduct applies to all employees (permanent and contractual) of Tredence and its subsidiaries or group companies and defines the manner as well as standard of business conduct that should be followed. This Code of Conduct is globally applicable and all national, as well as international offices come within its purview.
It encompasses the business practices, processes and procedures that Tredence operates within the framework of, to ensure ethical decision-making. Employees must go through it in detail and conduct themselves in accordance with the guidelines shared here.
It also our endeavor to share answers for specific situations that an employee might encounter on the job. Please reach out to the HR Partner if you face a situation that you might be able to find in this code of conduct and need guidance on how to proceed.

UNDERSTANDING AND USING THE CODE

At Tredence, we believe in empowering our employee. It is, therefore, each employee's responsibility to ensure that he or she fully understands and complies with all aspects shared in this Code of Conduct. This is a guiding document to upload the vision and values that Tredence stands for. Employees who observe any negligence to comply with any aspect of it, should report it to their manager or HR teams. We want to ensure the highest standards of integrity with the help of our employees. Any failure to comply with this Code could result in disciplinary action, which could range from termination to legal implications.

INCLUSIVE WORK ENVIRONMENT

The organization is committed to providing an inclusive, free, and open work environment to all its employees. The organization does not discriminate based on caste, tribe, ethnicity, origin, religion, age, disability, or sexual orientation. Employees must understand the value of this freedom and not misuse it in a way that impacts business or their individual productivity. Some instances where such freedom will be perceived as being misconstrued are –

1. Use of discriminatory or offensive language
2. Repeated failure to follow company policies
3. Harassment of any employee based on bias, prejudice
4. Lack of commitment towards overall organizational goals

In all these instances, the organization will take strict action with respect to the employee in question depending on the seriousness of the offence.

PREVENTION OF HARASSMENT

Tredence is committed to providing a safe work environment that respects human dignity. Tredence maintains a safe environment and expects all it employees to conduct themselves in a manner that does not cause mental or physical harassment to others in the organization. There are detailed policies on what constitutes harassment and the procedure to be adopted for corrective action. Please go through that for more details.

CONFIDENTIALITY

During the time of joining the company, all employees are required to sign and abide by a confidentiality agreement, which is legally binding. Employees need to follow the ethical practices believed in, by the company.

1. All non-public information or data related to business, or the organization is considered confidential information. Employees cannot use or share this for any other purpose except to conduct the company's business. If such data is used by an employee for personal financial or non-financial gain it will be considered unethical and illegal.
2. Some employees may need to know certain confidential information due to the nature of their roles. This could be financial or technical information. This cannot be shared outside the workplace and will stand as applicable for ex-employees as well.
3. Insider trading is not permitted and that applies to all its employees. Employees are not allowed to trade in the market, based on information that an employee obtains because of working at Tredence or at any of the client locations.
4. Employees cannot carry official documents in their possession unless those are required for a business meeting. All such materials must be returned at the time of separation from the company.
5. Photo copying or extracting of official documents is offence.

ORGANIZATION'S ASSETS

Tredence assets should be handled responsibly. Care must be taken to not damage, lend it or lose any of it that the employee. Misusing of the assets can result in the necessary disciplinary action.

In the event of loss or theft of an organization asset or if you become aware of misuse of company assets, one must immediately report it to his/her manager and the HR team.

The organization's electronic and telephonic systems should be used for business- related purposes only. Employees have the responsibility to use these in a professional, ethical, and lawful manner. This is also applicable for company property which includes company flat, company car and so on.

BRIBERY

Employees must not engage in any form of bribery, giving or taking, either directly or through any third party.

GIFTS AND HOSPITALITY

The organization believes in transparent and equitable management of all relationships. No act such as gifting or accepting gifts should be followed which can result in unethical or biased decision making. Tredence treats favours or bribery as a serious integrity issue and will need to necessitate strong action if any employee is seen to follow this.

Employees must not offer or give any gift or hospitality:

1. Which could be regarded as illegal or improper, or which violates the recipient's policies; or
2. to any public, clients (including past and prospective clients), or government officials or representatives, or politicians or political parties.
3. Employees may not accept any gift or hospitality from our business partners if:
4. It is in cash; or
5. there is any suggestion that a return favor will be expected or implied.
6. Any other gift that is received in kind shall be informed to CFO for decision on disbursement. Approval may be sought from CFO through an email. As a policy, we encourage donating such gifts to needy social cause organizations.

The organization is committed to maintaining high ethical standards and conducting business responsibly. No employee is permitted to demand or offer bribe in any form. Tredence strongly prohibits offering and accepting any form of business courtesies from or to clients, vendors, external partners and so on.

OFFERING AND ACCEPTING BUSINESS COURTESIES

While on business employees are permitted to accept non-branded gifts or courtesies to the amount of INR 2000 or USD 50.

Any gifts or courtesies accepted beyond this value should be branded.

COMMUNICATION AND PUBLISHING

It is expected that employees focus on responsible communication and avoid negative or disparaging comments about the organization, its people, and its businesses, on open or external forums. Sharing such feedback should be with appropriate authorities internally, and not with customers, vendors, and suppliers or in public places or events.

Also, any presentation, article, blog, white paper, or publication that contains confidential information of the organization must be approved by the employee's Manager before being published. The organization's logo cannot be used without prior approval. In case an employee wants to share specific insights about his or her expertise area, he/she must add the disclaimer that the same is author's opinion and not the organization's.

SMOKING, DRUG ABUSE, ALCOHOL

The organization wants to respect individual choices but also keep the workplace safe and accessible to all. Smoking within the office premises is prohibited except for the designated smoking zones. Following the notification by the Ministry of Health & Family Welfare, Government of India, it is prohibited to smoke cigarettes and other tobacco products in public places.

Smoking, chewing betal leaves, usage of drugs, and consumption of alcohol in any form is strictly prohibited and are not permitted on the office locations across the world.

Should any employee be reported to be under the influence of during work hours, necessary action will need to be initiated.

NON-COMPETE CLAUSE

Employees are prohibited from -

1. Propositioning for business opportunities that they got to know of in their roles as Tredence Employees, for themselves
2. Using the Company resources or information, or their position as employees, for personal gain; and
3. Actively applying or seeking employment with Tredence clients or competitors. Employees cannot be accepting an offer of employment, from any clients of Tredence during their employment with the company. This is applicable for a period of 1-year after leaving the organization

CONFLICT OF INTEREST & PERSONAL RELATIONSHIP

Employees must avoid all forms of conflicts of interest that can impact business and the organization's reputation. They cannot take up secondary employment while they are part of the organization. He or she cannot pursue any activities that will interfere with their work responsibilities.
Tredence places the responsibility on individual employees to withdraw from decisions were owing to their personal relationships, there might be either real or perceived conflict of interest.
In the above context, personal relationship shall include all relationships not just restricted to the one's established by blood, marriage, or legal action. Examples include the employee's: spouse / siblings/ cousin/relative/partner/friend.

- Individuals with real or perceived conflict of interest should not work in the same team or business unit
- Individuals should withdraw from exercising managerial/supervisory responsibilities within the same team / Business Unit. The onus is on the employee to disclose these cases to his or her Manager, HR Partner.
- In the event of involvement in a relationship with a co-worker where there may be real or perceived conflict of interest, the employee shall disclose it immediately to his or her Manager, HR Partner.

HEALTH AND SAFETY

Maintaining the health and safety of all our employees is our responsibility. We must ensure that we keep our workplaces and surroundings free to hazardous material or objects. Smoking is allowed only in designated spots in the interest of health and safety of all employees. Our infrastructure is also designed to support this.

FINANCIAL INTEGRITY / RECORD KEEPING

We believe that our financial integrity is of paramount importance. Our focus is to ensure that our financial records follow the prescribed accounting standards, and we fulfil our commitment to our stakeholders, internal and external. All employees must endeavor to follow this approach in all their financial dealings related to the organization. Record keeping must be aligned to our financial integrity principle. Any employee who believes that such integrity has been compromised should report it to the HR / Compliance team immediately.

SOCIAL MEDIA

Being responsible on social media is the primary responsibility of the employee. Sharing negative comments or confidential information about the company or its people, on social platforms is a serious offence. Use of wrong verbiage or foul language on the same platforms, through company WhatsApp groups or cyber-stalking will also be treated as violations which will have serious repercussions. Employees are not permitted to publish/post any pictures or blogs that reveal details of clients or projects on any social media posts including LinkedIn.

COMPETITION, ANTI-TRUST AND FAIR-TRADE PRACTICES

Tredence believes in full compliance with all the applicable antitrust, competition and fair-trade practices. We set our market prices without any bias or intervention from competitors or other non- related parties, using the fair market price approach. Our arrangements with our customers and suppliers are also defined in a fair manner. All employees, who are in roles that require them to be in touch with competition, or determine pricing need to be aware of all possible competition laws that will apply for their geography.

INTELLECTUAL PROPERTY

Tredence's intellectual property is all around you

- Trademarks (Logo and slogan)
- Copyrights (Creative designs, software, and analytics)
- Patents (Innovations and Inventions)

You must show respect for the laws governing copyrights, fair use of copyrighted material, trademarks and other intellectual property whether owned by Tredence or others. Tredence strives to never infringe on the rights of others, so you are always expected to obtain any necessary permission required by third party before using that party's intellectual property.

HOW TO REPORT A VIOLATION

All employees should know that it is their responsibility to maintain the Code. They should bring up any practices or actions that are non-compliant as per this, to their managers or the HR Partner/Compliance teams.

Employees can also email to hr.operations@tredence.com. The violations will be properly investigated in a non- biased and confidential manner. No employee should worry about retaliation or being victimized because they reported the violation.

BENIFITS

Leave Policy

Objective:

Tredence Analytics Solutions Pvt. Ltd. believes taking time-off for purposes including vacation, personal exigencies, recuperation from illness or for any other requirements is good for our employees since it gives them a chance to recharge and refresh

Scope:

This policy applies to all members of Tredence Analytics Solutions Pvt. Ltd. India herein referred to as "employees'". (For the purpose of this policy, "employees'" stands for all working at Tredence Analytics Solutions Pvt. Ltd. - full time regular employees', only)

What the policy stands for: The policy is divided into the following sections:

Section I – Guidelines
Section II – Types of Leaves & Entitlement
Section III – Leave Details
Section IV – India Holiday List 2023
Section V – Leave Application Process
Section VI - Annexure

Section I. Guidelines

1. Tredence Analytics Solutions Pvt. Ltd. shall follow the calendar year for leave administration i.e., January to December.
2. When Tredence Analytics Solutions Pvt. Ltd. members are based onsite, they will be governed by the onsite country public holiday schedule and not as per India public holiday.
3. All leaves must be applied by you and approved by your manager on the HRIS tool (Success Factors).
4. You can carry forward Earned Leaves up to a maximum of 30 days in the next calendar year and any balance shall get lapsed.
5. All compensatory offs will be at the discretion of the manager and will neither be encashed nor carried

forward to the next calendar year. Any compensatory off accrued must be availed within 2 weeks or they shall lapse.

6. The Compensatory Leave in lieu of duties performed on Saturdays/Sundays/Holidays under manager's approval should be claimed within a maximum period of 2 weeks from the date of the weekend/holiday worked. This is granted on the condition that there will be no accumulation of such compensatory leave and it is to be availed of within 2 weeks.
7. No leaves would be granted in case the employee is serving notice period, except in case of an emergency or ill health.
8. All grievances related to the leave policy will be directed to HRBPs.

Section II. Types of Leaves, Entitlement & Eligibility

- **Privilege Leaves**

Sl. No.	Type of leave	Entitlement	Eligibility
1.	Earned Leaves	16 working days/ calendar year	Prorated from date of hire
2.	Sick Leaves	6 working days / calendar year	Prorated from date of hire
3.	India Holidays	10 working days/ calendar year (8 fixed/ 2 optional)	Date of hire

- **Special Leaves**

Sl. No.	Type of leave	Entitlement	Eligibility
1.	Maternity Leaves	182 Calendar Days	Date of hire
2.	Paternity Leaves	5 working days	Date of hire
3.	Compensatory Off	At managers discretion	Date of hire
4.	Bereavement Leave	13 Calendar Days	Date of hire
5.	Miscarriage Leave	42 Calendar Days	Date of hire

Section III. Leave Details

Earned Leaves: We offer 16 paid days of earned leaves each calendar year for the time away from work for rest and relaxation.

Casual/Sick Leaves: We offer 6 paid days of sick leaves each calendar year for recouping for health issues or deal with personal exigencies

India Holidays / Festive Leaves: Tredence Analytics Solutions Pvt. Ltd. is closed for 10 holidays each year. Out of these 10 holidays **(8 holidays are fixed and 2 holidays are optional).** The holiday list is shown in Section IV below.

Maternity Leaves: All female employees are entitled to a maximum of 26 weeks of maternity leave. Employees are also entitled to one additional month of paid leave in case of complications arising due to pregnancy/delivery, based on a written recommendation from the physician.

Female employees who enter the maternity stage and gives birth to a baby, can avail the creche & day care facility from the day of birth of the baby until the baby turns 18 months old. Please contact HR team for more information on day care.

Female employees can avail adoption leave of 12 weeks paid time off for a child below 8 months of age. For queries, please reach out to HR team.

Miscarriage Leaves: All female employees are entitled to a maximum of 6 weeks of miscarriage leave.

Paternity Leaves: The father is entitled to take 5 working days of paid time-off from Date of Birth of the child.

Compensatory Off: We offer compensatory off for the work carried over a weekend/holidays as per the India Holiday list. The eligibility of compensatory offs would depend on your managers' discretion. Employees can avail the compensatory off within a maximum period of 2 weeks from the date of the weekend/holiday worked.

Bereavement Leave: Employees can avail 13 calendar days in case of demise of immediate family members (Parents/In-laws, Spouse, Children, Immediate Siblings). Employees can avail 5 working days in case of Demise of Grand-parents and pets.

Section IV. India Holiday List

Employee is entitled to **10 India Holidays**, out of which

- **8 fixed holidays**
- **2 optional holidays**

Fixed Holidays: There will be **8** Fixed Holidays, based on the city out of which the employee operates

FIXED HOLIDAY LIST - 2023 (Bangalore)			
Sl. No.	**Occasion of Leave**	**Date**	**Day**
1	Republic Day	26/Jan/2023	Thursday
2	Labour Day	01/May/2023	Monday
3	Bakrid	29/Jun/2023	Thursday
4	Independence Day	15/Aug/2023	Tuesday
5	Gandhi Jayanthi	02/Oct/2023	Monday
6	Kannada Rajyothsava	01/Nov/2023	Wednesday
7	Diwali	13/Nov/2023	Monday
8	Christmas	25/Dec/2023	Monday

FIXED HOLIDAY LIST - 2023 (Chennai)			
Sl. No.	**Occasion of Leave**	**Date**	**Day**
1	Republic Day	26/Jan/2023	Thursday
2	Tamil New Year's Day	14/Apr/2023	Friday
3	Labour Day	01/May/2023	Monday
4	Bakrid	29/Jun/2023	Thursday
5	Independence Day	15/Aug/2023	Tuesday
6	Gandhi Jayanthi	02/Oct/2023	Monday
7	Diwali	13/Nov/2023	Monday
8	Christmas	25/Dec/2023	Monday

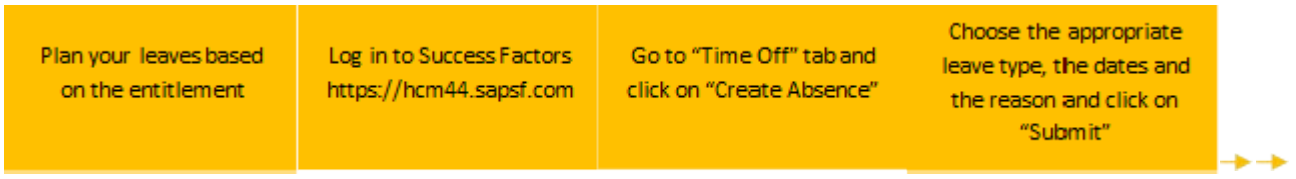
FIXED HOLIDAY LIST - 2023 (Gurugram)			
Sl. No.	**Occasion of Leave**	**Date**	**Day**
1	Republic Day	26/Jan/2023	Thursday
2	Holi	08/Mar/2023	Wednesday
3	Bakrid	29/Jun/2023	Thursday
4	Independence Day	15/Aug/2023	Tuesday
5	Gandhi Jayanthi	02/Oct/2023	Monday
6	Dussehra	24/Oct/2023	Tuesday
7	Diwali	13/Nov/2023	Monday
8	Christmas	25/Dec/2023	Monday

Optional Holidays: Employee can select up to a maximum of **2** Optional Holidays out of the below List.

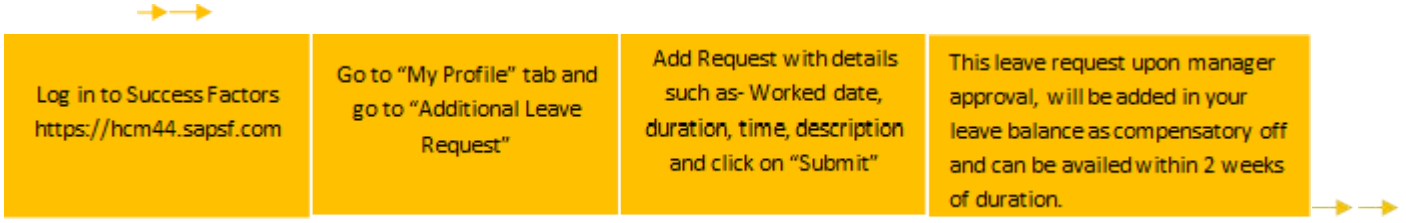
OPTIONAL HOLIDAY LIST – 2023			
Sl. No.	**Occasion of Leave**	**Date**	**Day**
1	Thiruvalluvar Day	16/Jan/2023	Monday
2	Uzhavar Thirunal	17/Jan/2023	Tuesday
3	Holi	08/Mar/2023	Wednesday
4	Chandramana Ugadi/Gudi Padva/Telugu New Year's Day	22/Mar/2023	Wednesday
5	Bhagat Singh Martyrs Day	23/Mar/2023	Thursday
6	Ram Navami	30/Mar/2023	Thursday
7	Mahaveera Jayanthi	04/Apr/2023	Tuesday
8	Good Friday	07/Apr/2023	Friday
9	Dr B.R. Ambedkar's Birthday	14/Apr/2023	Friday
10	Labour Day	01/May/2023	Monday
11	Buddha Purnima	05/May/2023	Friday
12	Maharana Pratap Jayanti	22/May/2023	Monday
13	Rath Yatra	20/Jun/2023	Tuesday
14	Shaheed Udham Singh's Martyrdom Day	31/Jul/2023	Monday
15	Parsi New Year	16/Aug/2023	Wednesday
16	Onam	29/Aug/2023	Tuesday
17	Raksha Bandhan	30/Aug/2023	Wednesday
18	Janmashtami	06/Sep/2023	Wednesday
19	Varasiddhi Vinayaka Vrata	18/Sep/2023	Monday
20	Ganesh Chaturthi	19/Sep/2023	Tuesday
21	Id-E-Milad	28/Sep/2023	Thursday
22	Maha Navami, Ayudhapooja	23/Oct/2023	Monday
23	Vijayadashami/Dussehra	24/Oct/2023	Tuesday
24	Balipadyami, Govardhan Puja / Hindu New year	14/Nov/2023	Tuesday
25	Bhai Dooj	15/Nov/2023	Wednesday
26	Gurunanak Jayanthi	30/Nov/2023	Thursday

Section V. Leave Application Process

Leave Application Process – All type of Leaves:



Leave Application Process – Compensatory Off/Leaves:



Section VI. Annexure

Examples of leaves in each type of leaves:

Earned Leaves: relaxation (Employee accumulates 4 days of leaves every quarter on pro rata basis from DOJ).

Q 1: Jan to Mar: 4 leaves

Q 2: Apr to Jun: 4 leaves

Q 3: Jul to Sep: 4 leaves Q 4: Oct to Dec: 4 leaves

Example:

If you join in the month of Jan, you will get 4 leaves for the quarter If you join in the month of Feb, you will get 2 leaves for the quarter If you join in the month of Mar, you will get 1 leave for the quarter

Sick Leaves: (Employee accumulates 1.5 specific days of leave every quarter on pro rata basis fromDOJ)

Q 1: Jan to Mar: 1.5 leaves

Q 2: Apr to Jun: 1.5 leaves

Q 3: Jul to Sep: 1.5 leave

Q 4: Oct to Dec: 1.5 leave

Example:

If you join in the month of Jan, you will get 1.5 leaves for the quarter If you join in the month of Feb, you will get 1 leaves for the quarter

If you join in the month of Mar, you will get 0.5 leave for the quarter

Compensatory Off:

Example:

If you work in office or from home for 1 day on a weekend, then you will be eligible for 1 compensatory off

If you work in office or from home for 2 days on a weekend, then you will be eligible for 2 compensatory off

If you work in office or from home on a holiday as per the holiday list, then you will be eligible for compensatory off against the holiday

Rev. No.	Rev. Date	Prepared by	Approved by
1.	1-Jan-15	HR Team	India – HOA
2.	25-Aug-15	HR Team	India - HOA
3.	8-Dec-15	HR Team	India – HOA
4.	1-Jan-16	HR Team	Sr. Mgr. - Delivery
5.	1-Jan-17	HR Team	India – HOA
6	1-Jan-18	HR Team	HR-Principal
7	31-Dec-18	HR Team	HR-Principal
8	1-Jan-19	HR Team	HR-Principal
9	1-Jan-20	HR Team	HR-Principal
10	1-Jan-21	HR Team	HR-Principal
11	1-Jan-22	HR Team	HR- Senior Director
12	15-Feb-23	HR Team	HR- Senior Director

Expense Reimbursement Policy

Objective:

Tredence Analytics Solutions Pvt. Ltd. believes that all employees should avail the benefit of claiming expenses incurred during official assignments. This policy lays down guidelines for what constitutes as expense reimbursement

Scope:

This policy applies to all members of Tredence Analytics Solutions Pvt. Ltd. India herein referred to as "employees". (For the purpose of this policy, "employees" stands for all working at Tredence Analytics Solutions Pvt. Ltd. - full time regular employees, only)

What the policy stands for: The policy is divided into three sections:

Section I – Type of expenses
Section II – Guidelines
Section III – Reimbursement Process

Section I. Type of expenses

1. Expenses on food during interview meetings and lunch with clients
2. Travel (travel bills) by taxi, train or flight for client meetings, visa interviews and any other official work
3. Expenses on office stationery, medicines
4. Expenses on team outings like food, water, petrol and entry tickets

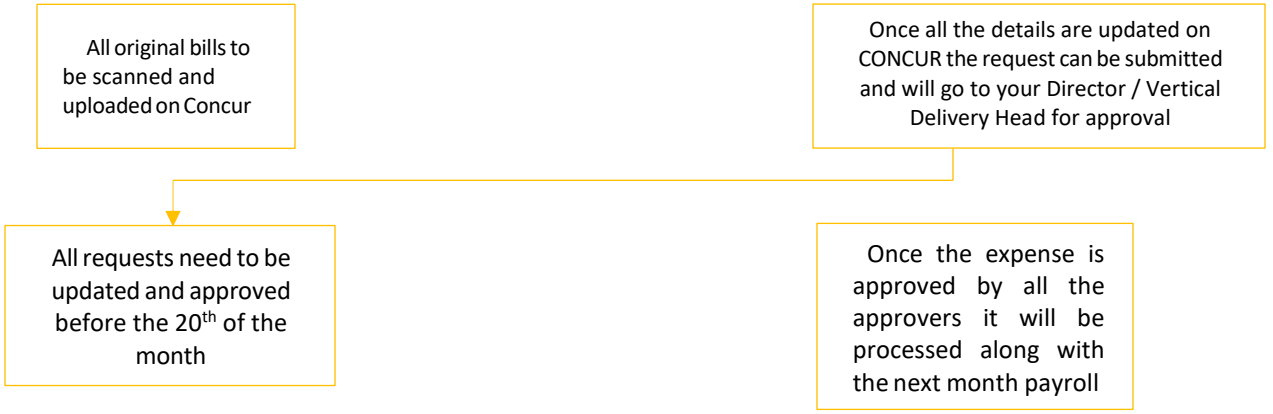
Section II. Guidelines

1. Reimbursement of expenses will be made on actuals
2. Only original bills should be submitted for reimbursement of expenses with all the required details
3. If a bill is not available for claiming an expense, the expense should be approved by the employee's senior manager on an email (print out of the email approval can then be attached to reimbursement

slips)

4. You should take your Director/Senior Managers signature on all the bills before submission, if the Director/Senior Manager is travelling or onsite or on leave, an email approval from him/her is required that can be attached to the reimbursement slip
5. All expenses should fall under the type of expenses mentioned above.
6. The reimbursement claims should be made within 1 month from the date of actual expense. E.g. expenses incurred in January can be submitted in February, but not in the month of March
7. No liquor bills will be reimbursed as part of reimbursement.
8. All grievances related to the dinner reimbursement policy will be directed to the Finance team
9. All reimbursements to be submitted by the 20th of the month on Concur

Section III. Reimbursement Process



Relocation Policy

Within India

Objective

Tredence believes that any employee who is asked to relocate within India for business purpose, should avail the benefit of claiming for relocating expenses. This policy lays down guidelines for what constitutes as relocation expenses

Scope

This policy applies to all members of Tredence Analytics Solutions Pvt. Ltd. India herein referred to as "employees". (For the purpose of this policy, "employees" stands for all working at Tredence Analytics Solutions Pvt. Ltd. - full time regular employees, only)

What the policy stands for: The policy is divided into the following sections:

Section I – Type of expenses
Section II – Guidelines
Section III – Reimbursement Process

Section I. Type of expenses

a. Travel tickets (3 tier AC Train or bus)
b. Hotel accommodation for 14 days from the day one checks-in will be booked by Tredence (Exclusions during hotel stay: laundry bills, dinner, lunch or snacks bills, cab/taxi bills & Liquor)

NOTE: Please note for any reason, the stay will not be extended beyond 14 days

Sr. No.	Details	Level	Expenses
1	Expense Limit	L1, L2	INR 10,000
2	Expense Limit	L3, L4	INR 25,000
3	Expense Limit	L5 & above	INR 50,000

1. If one travels by their own bike/car (fuel & toll expenses) at the time of relocation (Inclusions during travel: expenses for food, water and snacks), will be reimbursed on actuals
2. No liquor bills will be reimbursed as part of relocation expenses

Section II. Guidelines

1. Relocation reimbursement of expenses will be made on actuals
2. Only original bills should be submitted for relocation reimbursement of expenses
3. The expenses should be claimed as per the predetermined approved expense limit as per the guidelines notified during the interview process and details mentioned on the offer letter
4. The reimbursement of expenses incurred while relocation will be applicable only while relocating from the current city of residence to the city of relocation
5. If at any given point of time the employee decides to quit the organization or is serving notice period, within a period of 1 year from his DOJ, the relocation expenses (Section I) shall be recovered from the employees' full and final settlement
6. The predetermined expenses should be borne by the employee before claiming for relocation
7. The reimbursement claims should be made within 1 month from the date of actual expense
8. All grievances related to the relocation expense reimbursement policy will be directed to HR team

Section III. Reimbursement Process

All bills need to be uploaded on Concur

Once the request is submitted on Concur the same will go to the Reporting Manager / TA Head for approval

Once the TA head / Reporting Manager approves the request will go to the Finance team for validation

All requests should be submitted and approved on Concur by the 20th of each month

The expenses will be reimbursed to the employee towards the month end

Any country to India

Objective

Tredence Analytics Solutions Pvt. Ltd. (Tredence India) believes that any employee who permanently migrates from any country to Tredence India office locations in India should avail the benefit of claiming for relocating expenses. This policy lays down guidelines for what constitutes as relocation expenses.

Scope

This policy applies to all members of Tredence Analytics Solutions Pvt. Ltd. herein referred to as "employees". (For the purpose of this policy, "employees" stands for all working at Tredence Analytics Solutions Pvt. Ltd. - full time regular employees, only)

What the policy stands for: The policy is divided into following sections:

Section I – Type of expenses
Section II – Guidelines
Section III – Reimbursement process

Section I. Type of expenses

1. Travel: Travel tickets will be booked by the admin team
    a. Taxi/cab bills from home to airport, bus station or train station will be reimbursed on actuals
    b. Expenses can be reimbursed for food and water on actuals while relocating will be reimbursed on actuals (No liquor bills will be reimbursed)
2. Lodging: A maximum of 14 days of guest house accommodation will be provided to the employee at the time of joining by the travel desk (You need to check in to the hotel on Day 1)
3. If you don't, you would be responsible for any cancellation fees. (In case you plan to cancel or change the booking, you are requested to let HR & the admin team know 48 hours in advance)
4. Local Travel: 14 days of UBER for business travel up to INR 500 per day, for the first 14 days, on actuals will be reimbursed
5. Business travel: From home/hotel to office and back

Section II. Guidelines

1. If at any given point of time the employee resigns or is serving notice period, within a period of 1 year from the employees' relocation date, the relocation expenses (Section 1) shall be recovered from the employees' full and final settlement
2. Two (2) weeks advance of salary, if required, will be offered to the employee at the time of joining. This will be offered to take care of initial expenses before settling down and the same would be adjusted along with the monthly salary payout
3. Relocation reimbursement of expenses will be made on actuals
4. You need to check in to the hotel on Day 1. If you don't, you would be responsible for any cancellation fees. (In case you plan to cancel or change the booking, you are requested to let HR & the admin team know 48 hours in advance)
5. The expenses should be borne by the employee before claiming for relocation expenses
6. The reimbursement claims should be made within 1 month from the date of actual expense
7. All grievances related to the relocation expense reimbursement policy will be directed to HR team

Section III. Reimbursement process

All bills need to be uploaded on Concur

Once the request is submitted on Concur the same will go to the Reporting Manager / TA Head for approval

Once the TA head / Reporting Manager approves the request will go to the Finance team for validation

All requests should be submitted and approved on Concur by the 20th of each month

TREDENCE ACADAMY OF LOTS OF LEARNING

'U Learn V Pay' Policy

Objective

Tredence believes that any employee who seeks to learn and expand his / her skill sets using online courses, should avail the benefit of a reimbursement process for successfully completed courses. This policy lays down guidelines for what constitutes as 'U Learn V Pay' (ULVP).

Scope

This policy applies to all members of Tredence herein referred to as "employees". (For the purpose of this policy, "employees" stands for all working at Tredence - full time regular employees.

What the policy stands for

1. You can use this policy to learn and develop new skills through online courses
2. The course can be related to Analytics, Technology or anything that interests you.
3. You must sign up for and pay for the online course yourself
4. The policy applies only to online courses and not to part time or full-time courses offered by institutes or colleges
5. The course fees limit is up to INR 10,000 for India location and $150 for US location.
6. In case the course cost exceeds INR 10,000 for India location and $150 for US location, please seek approval from your manager prior to registering for the course. Mark tall@tredence.com in these communications.
7. Any reimbursement that exceeds the above limits of INR 10,000 for India location and $150 for US location, Tredence reserves the right to recover the cost in case you separate from Tredence within 1 year from the date of reimbursement

To enroll your course in ULVP, fill the below form:

ULVP Enrollment Form

To reimburse the course fee:

For India Employees:

- Please take a printout of the course completion certificate
- Fill the reimbursement slip
- Attach the certificate with the slip
- Get the slip signed by your Director
- Submit to Finance team

REWARDS AND RECOGNITION

Rewards & Recognition Policy

Objective

Tredence acknowledges all employees for their contribution in delivery excellence, client impact, business growth and building the organization. We aim to recognize every effort that makes an impact on ground and set up an example for the other team members. We regard the value system of Tredence as a core definition of who we are, as such we encourage you to recognize every behavior that aligns with Tredence core values and be recognized in turn.

Scope

All full-time regular employees are eligible to receive these awards/gifts.

Performance Appraisal Guidelines & Process

Objective

Tredence believes that any employee who has been a part of Tredence over a period should be given a fair chance of proving his ability with a systematic approach. This document lays down the process & guidelines for what constitutes as a Performance Appraisal of an individual employed with Tredence.

Scope

This policy applies to all regular employees of Tredence who have all the eligible documented pit-stops herein referred to as "Appraisee'".

What the policy stands for: The policy is divided into two sets of guidelines:

Section I – Guidelines
Section II – Process

Section I. Guidelines

1. Appraisee – The individual who will be evaluated under Performance Appraisal Cycle
2. Appraiser – The individual who will initiate & monitor
3. Director – Head of portfolio, who will oversee the Performance Appraisal of teams falling under respective portfolio
4. An Appraisee will have to fill in the Pit-stops/Goal Document once in 3 Months to ensure that Appraisal meets his/her manager and is evaluated on the goals that have been set
5. Onus completely lies on the Appraisee to get his pit-stop scores filled in both the self-rating scores and ensure the manager fills his rating. Final documented pit- stop goal document is to be shared with HR team by the Appraiser by the 6th Working Day of the corresponding month

6. Goals in the Goal Document are set up at the beginning of the 6-month cycle or when employee joins the company. It is then the Manager's responsibility to ensure the Goal Document is shared with his team and the KRA's are explained to them clearly.
7. Ensure that while filling up Goal sheet the relevant KRA is referred to, based on designation.
8. If there is a conflict, respective Principal will pitch in and resolve
9. HR Team, if required will be part of the conversation and act as the evidence.

Section II. Performance Appraisal - Process

Appraisee collates the feedback for the last 6 months

Appraiser fills out the goal document of Appraisee which includes all bimonthly pitstop discussions and the final consolidated score sheet in June / Dec

The points mentioned in the goal doc are discussed and agreed by both the Appraiser and Appraisee – Employee's manager and Principal

Once finalized the Appraisee can look into it once again and share any final inputs

If there are no changes the KRA doc stands accepted and is applicable for Performance Appraisal cycle

Compliance

Privacy and Confidentiality Policy

Objective

Tredence believes that any employee should be aware of the nuances of privacy and confidentiality when they become part of Tredence. This policy lays down guidelines for what constitutes as privacy & confidentiality policy

Scope

This policy applies to all members of Tredence Analytics Solutions Pvt. Ltd. India herein referred to as "employees". (For the purpose of this policy, "employees" stands for all working at Tredence Analytics Solutions Pvt. Ltd. - full time regular employees, only)

The policy is divided into the following sections:

Section I – Basic Clauses
Section II – Guidelines
Section III – Violation Redressal Process

Section I. Basic Clauses

The employees sign an Acceptance Usage Policy (AUP) on the day they join. Please refer Annexure 1 for details

Section II. Guidelines

- All employees must sign Acceptance Usage Policy (AUP)on joining
- This agreement will be signed by both the employee and the Co-founder & Head of Analytics
- All grievances related to the Privacy and Confidentiality policy will be directed to HR team

Section III. Redressal Process

- Reach out to the employee (notice, call, summons, etc.), either within or outside the firm and take appropriate actions as per the local laws
- Legal in case it's required, depending upon the severity of the issue

Intellectual Property Policy

Objective

Tredence believes that any employee should be aware of the intellectual property policy when they become part of Tredence. This policy lays down guidelines for what constitutes as intellectual property policy

Scope

This policy applies to all members of Tredence Analytics Solutions Pvt. Ltd. India herein referred to as "employees". (For the purpose of this policy, "employees" stands for all working at Tredence Analytics Solutions Pvt. Ltd. - full time regular employees, only)

The policy is divided into the following sections:

Section I – Intellectual property
Section II – Violation Redressal Process

Section I. Intellectual property

1. Introduction
2. Scope
3. Definitions
4. Purpose
5. Ownership of IP
6. Protection of IP
7. Exploitation of IP
8. Role and Responsibilities

1. Introduction:

The policy is to encourage the generation of intellectual property (IP) that has a potential value in both

service and financial terms. Tredence has a responsibility, via general obligations issued by, to ensure that innovations, including novel treatments, devices, data, software, training materials or a new management system, are disseminated as widely as possible for the benefit of all Tredence employees. This process may include publishing the IP in the public domain or exploiting it through commercial channels in order to potentially acquire monetary gain.

2. Scope:

This policy applies to all staff employed at Tredence on either a permanent or temporary contract.

3. Definitions:

Intellectual Property (IP) is any form of original creation. It is any patent, copyright, database right, registered design, unregistered design rights, design specifications, drawings, software or any other IP protection or right and any application for such protection and all rights in any discovery, improvement process, secret process, know-how or other confidential information.

4. Purpose:

To ensure the benefits of any innovations are maximized, this policy sets out the rules for the ownership, protection, and exploitation of IP.

5. Ownership of IP:

It is Tredence' s intention to maintain a balance between wishing to benefit from potentially valuable IP and the provision of a creative working environment for employees in which they can be encouraged to innovate and to declare such innovation to Tredence. As a rule, IP created by an individual in the course of his /her employment, or training arising out of his/her employment, belongs to their employer (Tredence) and any benefits accrued in the work will belong to Tredence. If Tredence does decide to commercially exploit and protect IP rights, then it may be appropriate for the employee who created or developed the IP to have a share in the benefits for example through a royalty income or other recognition. In certain circumstances the Tredence may decide not to take up its rights and ownership may be assigned to the employee.

With the assistance of legal team, from time to time, arrangement will take place for an audit of Tredence activity to identify IP of potential commercial value. All members of staff are required to

cooperate fully with any such audit.
Where employees have joint contracts with other organizations, where appropriate, a partnership agreement on IP will need to be developed. In general, the organization with the main contract will be responsible for protecting the IP rights and for any commercialization. Ownership of IP generated because of activity of organizations hosted by the Tredence will be subject to agreements set out in the relevant host arrangement contracts, and relevant collaboration agreements with partner organizations. However, income from IP which is attributable to the Tredence will be subject to the provisions of this policy.

6. Protection of IP:

IP can be protected by legal rights such as patents, copyright, design rights and trademarks although acquiring such rights can be costly and time consuming. Patents can be costly to obtain, and further guidance should be obtained from the leadership team at Tredence. Do not involve external parties in the development of the IP, unless approved by the legal team at Tredence. Keep potential IP as secret as possible and resist pressure to announce or publish details until the matter has been discussed with the legal team. For Research and Development (R&D) that may be funded wholly or in part by external bodies. Employees should ensure that they understand their legal position and their obligations relative to IP within these contracts

7. Exploitation of IP:

Exploitation of IP involves both costs and risks. Consequently, it will by no means always be appropriate or cost effective to seek to protect and exploit potential IP. In most cases copyright will suffice, although in cases where patenting or licensing may be the most appropriate option, the legal team (with advice from our legal team where appropriate), will undertake negotiations on behalf of the inventor and Tredence.
For the avoidance of doubt, the Tredence acknowledges and accepts that in the case of any inconsistency, it is bound by its legal responsibilities and obligations to staff contained within the general law that cannot be varied by these conditions. In the event of any dispute about the interpretation of this policy, employees have recourse to the Tredence grievance procedure to resolve the dispute.

8. Role and Responsibilities:

- Managers. All Managers within Tredence are responsible for ensuring that all staff they manage can access copies of this policy. Managers are also responsible where applicable for bringing this policy to

attention of employees, and for ensuring that the legal are contacted.

- All Staff. If an employee develops an idea or concept, which may have commercial potential, they must report this to their Senior Manager, who should contact the legal team at the earliest opportunity and before the disclosure of the idea to any party outside Tredence.

Section II. Violation Redressal Process

- Reach out to the employee (notice, call, summons, etc.), either within or outside the firm and take appropriate actions as per the local laws
- Legal assistance in case it's required, depending upon the severity of the issue

Conflict of Interest Policy

Objective

Tredence believes that any employee should be aware of the conflict-of-interest policy when they become part of Tredence. This policy lays down guidelines for what constitutes as conflict-of-interest policy

Scope

This policy applies to all members of Tredence Analytics Solutions Pvt. Ltd. India herein referred to as "employees". (For the purpose of this policy, "employees" stands for all working at Tredence Analytics Solutions Pvt. Ltd. - full time regular employees, only)

The policy is divided into the following sections:

Section I – Conflict of Interests

Section II – Violation Redressal Process

Section I. Conflict of interest

This conflict-of-interest policy is designed to help employees of Tredence identify situations that present potential conflicts of interest and to provide Tredence with a procedure that, if observed, will allow a transaction to be treated as valid and binding even though employee has or may have a conflict of interest with respect to the transaction. In the event there is an inconsistency between the requirements and the procedures prescribed herein and those in the law shall control.

1. **Definitions.**
   - A. A Conflict of Interest is any circumstance described in Part 2 of this Policy.
   - B. A Responsible Person is any person serving as an officer, employee, or member of the board of directors of Tredence.
   - C. A Family Member is a spouse, domestic partner, parent, child, or spouse of a child, brother, sister, or spouse of a brother or sister, of a Responsible Person.
   - D. A Material Financial Interest in an entity is a financial interest of any kind that, in view of all the circumstances, is substantial enough that it would, or reasonably could, affect a Responsible Person's or Family Member's judgment with respect to transactions to which the entity is a party. This includes all forms of compensation. (The board may wish to establish an amount that it would consider to be a "material financial interest.")

E. A Contract or Transaction is any agreement or relationship involving the sale of purchase of goods, services, or rights of any kind, the providing or receipt of a loan or grant, the establishment of any other type of pecuniary relationship or review of a charitable organization by Tredence. The making of a gift to Tredence is not a Contract or Transaction.

2. Conflict of Interest Defined.

For purposes of this policy, the following circumstances shall be deemed to create Conflicts of Interest:

Outside Interests.

i. A Contract or Transaction between Tredence and a Responsible Person or a Family Member.
ii. A Contract or Transaction between Tredence and an entity in which the Responsible Person or a Family Member has a Material Financial Interest or of which such person is a director, officer, agent, partner, associate, trustee, personal representative, receiver, guardian, custodian, conservator, or other legal representative.

Outside Activities.

i. A Responsible Person competing with Tredence in the rendering of services or in any other Contract or Transaction with a third party.
ii. A Responsible Person having a Material Financial Interest in; or serving as a director, officer, employee, agent, partner, associate, trustee, personal representative, receiver, guardian, custodian, conservator, or other legal representative of, or consultant to; an entity or individual that competes with Tredence in the provision of services or in any other Contract or Transaction with a third party.

Gifts, Gratuities and Entertainment.

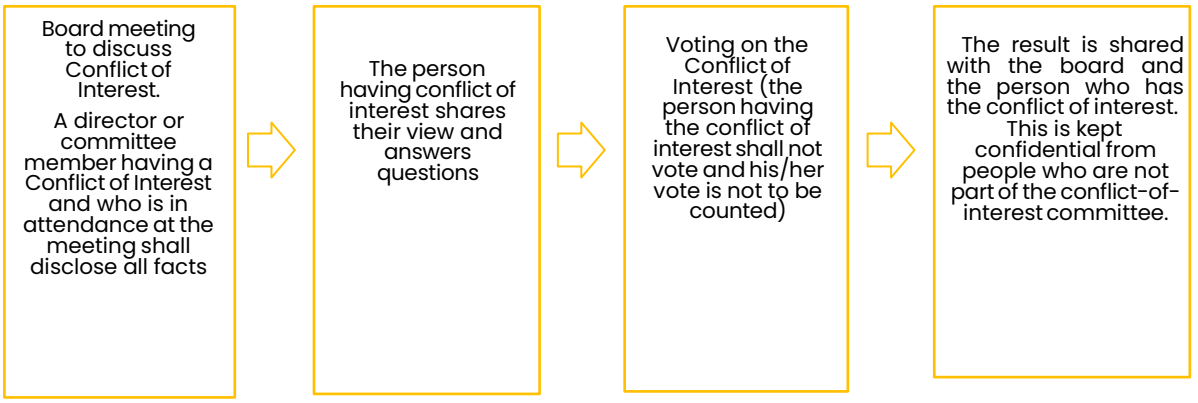
A Responsible Person accepting gifts, entertainment, or other favors from any individual or entity that:

i. Does or is seeking business with, or is a competitor of Tredence; or
ii. Has received, is receiving, or is seeking to receive a loan or grant, or to secure other financial commitments from Tredence.
iii. Is a charitable organization. This does not preclude the acceptance of items of nominal or

insignificant value or entertainment of nominal or insignificant value that are not related to any transaction or activity of Tredence.

iv. A person who has a Conflict of Interest shall not participate in or be permitted to hear the boards or committee's discussion of the matter except to disclose material facts and to respond to questions. Such person shall not attempt to exert his or her personal influence with respect to the matter, either at or outside the meeting.

Violation Redressal Process



Prevention of Sexual Harassment

Objective:

Tredence is an equal employment opportunity company and is committed to creating a healthy working environment that enables employees to work without fear of prejudice, gender bias and sexual harassment. The Company also believes that all employees of the Company, have the right to be treated with dignity. Sexual harassment at the workplace or other than workplace if involving employees is a grave offence and is, therefore, punishable.

Scope:

This policy applies to all members of Tredence herein referred to as "employees'". (For the purpose of this policy, "employees'" stands for all working at Tredence - full time regular employees', only)

What the policy stands for: The policy is divided into the sections below:

Section I– Guidelines
Section II– Internal Complaint Committee (ICC)
Section III– Redressal Process
Section IV– Confidentiality
Section V– Access to Reports and Documents
Section VI– Timeline
Section VII– Possible Disciplinary Actions
Section VIII– Protection to Complaint Victim
Section IX – Training
Section X– Additional Information and Committee Details
Section XI– Do's and Don'ts
Section XII– Overriding Effect

Section I. Guidelines

Anti-Sexual harassment at workplace is applicable to:

- Every employee across the Company – permanent, temporary, consultant, on training and on contract
- An alleged act of sexual harassment that has occurred during or beyond office hours
- An alleged act of sexual harassment, which has taken place within or outside the company premises
- All the employees, workers, and trainees (whether in the office premises or outside while on assignment)
- Where sexual harassment occurs to a Tredence employee as a result of an act by a third party or outsider while on official duty, Tredence will take all necessary and reasonable steps to assist the affected person in terms of support, readdress and preventive action
- Drop an email to *posh@tredence.com* for any complaints w.r.to to sexual harassment
- This policy is only applicable when either or both the alleged harasser and the victim are employees of the company. It is not applicable when both the alleged harasser and the victim are third parties

The workplace includes:

- All offices or other premises where the Company's business is conducted
- All company-related activities performed at any other site away from the Company's premises
- Any social, business or other functions where the conduct or comments may have an adverse impact on the workplace or workplace relations

1.1 WHAT IS SEXUAL HARASSMENT?

According to the Act, sexual harassment is any unwelcome sexually determined behavior, such as: -

- Physical contact
- A demand or request for sexual favors
- Sexually colored remarks
- Showing pornography
- Verbal abuse or 'joking' that is sex-oriented

- Any other physical, verbal, or non-verbal conduct of a sexual nature

What Behavior May Be Harassing?

Written:

- Unwelcome suggestive, sexually explicit or obscene letters, notes, emails or invitations from manager, colleague, client or patient

Verbal:

- Derogatory, sexually explicit or offensive comments, epithets, slurs or jokes.
- Inappropriate comments about an individual's body or sexual activities.
- Repeated unwelcome propositions or sexual flirtations.
- Direct or subtle pressure or repeated unwelcome requests for dates or sexual activities

Visual

- Sexually oriented gestures, display of sexually suggestive or derogatory objects, pictures, cartoons, posters or drawings
- Looking a person up and down ("elevator eyes")

1.2 Other Types of Discriminatory Harassment:

The Company's policy also prohibits verbal or physical conduct that denigrates or shows hostility or aversion toward an individual because of his or her race, colour, religion, sexual orientation, age, national origin, disability, or other protected classification, and that:

1. Has the purpose or effect of creating an intimidating, hostile, humiliating or offensive working environment.
2. Has the purpose or effect of unreasonably interfering with an individual's work performance, or otherwise adversely affects an individual's employment opportunities. While it is not possible to list all those circumstances that may constitute discriminatory harassment, the following are some examples of conduct which may constitute discriminatory harassment depending upon the totality ofthe circumstances including the severity of the conduct and its pervasiveness:

Epithets, slurs, negative stereotyping, or jokes, or threatening, intimidating or hostile acts that relate to race or other protected classification.

Written or graphic material that denigrates or shows hostility toward an individual or group because of race or other protected classification and that is circulated in the workplace or placed anywhere in the Company's premises such as on an employee's desk, workspace or on Company computer, email or voicemail.

Sexual harassment cases can be classified into two categories - quid pro quo and creation of a hostile working environment.

1. Under the quid pro quo (meaning this for that) form of harassment, a person or authority, usually the superior of the victim, demands sexual favours for getting or keeping a job benefit and threatens to fire the employee if the conditions are not met.
2. A hostile work environment arises when a co-worker or supervisor creates a work environment through verbal or physical conduct that interferes with another co- worker's job performance or creates the workplace atmosphere which is intimidating, hostile, offensive or humiliating and experienced as an attack on personal dignity. For example, an employee tells offensive jokes. No person shall indulge or caused to be indulged under instructions from superior in sexual harassment of co-workers. However, an employee who is sexually harassed can complain about the same even if there is no adverse job consequence.

Section II. Internal Complaint Committee (ICC)

The Company has instituted an Internal Complaints Committee for redressal of sexual harassment complaint (made by the victim) and for ensuring time bound treatment of such complaints.

In accordance with the sexual Harassment at Workplace (Prevention, Prohibition and Redressal) Act, 2013, the Internal Complaints Committee will comprise of the following:

- **Female Members** – Rekha Nair and Joycee Nair
- **Male Members** - Shobhit Kumar and Parag Lonhari
- **External Committee Member** – Vaneesha Jain

The Internal Complaints Committee is responsible for:

- Investigating every formal written complaint of sexual harassment
- Taking appropriate remedial measures to respond to any substantiated allegations of sexual harassment.
- Discouraging and preventing employment-related sexual harassment

Sr. No.	Employee Name	Contact Number	Designation	Email id
1	Rekha Nair	9820198652	Sr. Director HR	rekha.nair@tredence.com
2.	Joycee Nair	9741641007	Sr Manager	joycee.nair@tredence.com
3	Shobhit Kumar	7760205592	Sr. Director	shobhit.kumar@tredence.com
4	Parag Lonhari	9850953550	Vice President	parag.lonhari@tredence.com
5	Vaneesha Jain	7033446655	External Consultant	Vaneesha@sashaindia.com

Roles & Responsibility of Internal Complaints Committee (ICC) Member:

Duties of the Complaints Committee shall be as follows, namely:

- To process Complaints of Sexual Harassment and to take suitable action in the manner and mode particularly provided hereafter
- To do all such acts and things as may be necessary to carry out the objects of the Policy and comply with provisions of the Act

The Internal Complaints Committee shall have the powers of a civil court, which include the following:

- Summoning and enforcing the attendance of any person and examining him/her on oath;
- Requiring the discovery and production of documents; and
- Any other matter which may be prescribed by law

Section III. Redressal Process

All matters of harassment will be treated with sensitivity and discussed only with parties that have a legitimate business need-to-know. Confidentiality is very important and will be maintained to the extent permitted by the circumstances. Complaints will be promptly investigated, and appropriate action will result. Steps will be taken to ensure that the person reporting the activity does not face retaliation because of bringing the complaint to the attention of management or Human Resources. The legal and other consequences of Sexual Harassment and the written order constituting the Internal Complaints Committee will be displayed at the company portal and each location at prominent place.

III. **A) Informal Investigation/Reconciliation:**

The Complaints Committee may if, and only if so requested by the aggrieved person, try to resolve the matter informally by intervening and thereby permitting the parties to resolve the matter mutually before

the commencement of the formal enquiry proceedings. The person to carry out the Dispute Resolution Process shall be chosen from the Internal Complaints Committee by the aggrieved person.

III. B) Formal Investigation Process:

Step 1: Any employee who feels and is being sexually harassed directly or indirectly may submit a complaint of the alleged incident to any member of the Committee in writing with his/her signature within 3 months of occurrence of incident.

The Committee will maintain a register to endorse the complaint received by it and keep the contents confidential, if it is so desired, except to use the same for discreet investigation.

Step 2: The Committee will hold a meeting with the Complainant within seven working days of the receipt of the complaint, but no later than a week in any case.

Step 3: At the first meeting, the Committee members shall hear the Complainant and record her/his allegations. The Complainant can also submit any corroborative material with a documentary proof, oral or written material, etc., to substantiate his / her complaint. If the Complainant does not wish to depose personally due to embarrassment of narration of event, a lady officer for lady employees involved and a male officer for male employees, involved shall meet and record the statement.

Step 4: Thereafter, the alleged harasser may be called for a deposition before the Committee and an opportunity will be given to him / her to give an explanation, where after, an "Enquiry" shall be conducted and concluded.

Step 5: Both the complainant and the alleged harasser should be given a chance to cross examine witnesses. Company will provide the alleged harasser to cross examine witness within his/her presence.

Step 6: The Internal Complaints Committee shall conduct investigations in a timely manner and shall submit a written report containing the findings and recommendations to the Employer as soon as practically possible and in any case, not later than 10 days from the date of completion of inquiry. The Employer shall act upon the recommendation within 60 days of its receipt by him.

Step7: Based on the investigation report, the appointing authority will initiate disciplinary proceeding

In the event, the complaint does not fall under the purview of Sexual Harassment, or the complaint does not mean an offence of Sexual Harassment, the same would be dropped after recording the reasons thereof.

In case the complaint is found to be false, the Complainant shall, if deemed fit, be liable for appropriate disciplinary action by the Management.

III. **C) False Complaint or Evidence:**

- Where the Internal Complaints Committee, after an inquiry, establishes that:
  - The Complaint against the Accused is false or malicious or is based on false evidence or the Complainant has produced a forged or misleading document; or
  - Any witness has given false evidence or has produced a forged or misleading document during the inquiry.
  - It may recommend to the employer to take action against the Complainant or witness (as the case may be) as per the applicable service rules.
- A mere inability to substantiate a complaint or provide adequate proof need not attract action against the complainant.
- Any Employee of Tredence who violates this Policy will suffer appropriate disciplinary action as per the findings of the Complaint investigation. If the investigation reveals that the Sexual Harassment has indeed occurred, the harasser shall be suitably disciplined.
- Conversely, anyone making a false or frivolous claim of Sexual Harassment shall also be subject to disciplinary action in accordance with the provisions of the Act.

Section IV. Confidentiality:

- It shall be the duty of all the persons and authorities designated under this committee to ensure that all complaints lodged under this chapter shall be strictly confidential.
- The name of the aggrieved person shall not be referred to in any records of proceedings, or any orders or Judgments given under this Act;
- The name of, neither the aggrieved person nor her identity shall be revealed by the press / media or any other persons whilst reporting any proceedings, case, order or Judgment under this Act

Section V. Access to Reports and Documents

All records of complaints, including contents of meetings, results of investigations and other relevant material will be kept confidential by the Company except where disclosure is required under disciplinary or other remedial processes

Section VI. Timeline:

Enquiry to be completed within 90 days.

Notwithstanding anything contained in any law for the time being in force an enquiry under this policy shall be completed, including the submission of the Enquiry Report, within a period of 10 days from the date on which the enquiry is commenced. Any delay in completion shall be done for reasons given in writing.

Section VII. Possible Disciplinary Actions:

- A letter of warning that will be placed in the personal file of the harasser
- Immediate transfer or suspension without pay or both
- Stoppage of increment with or without cumulative effect
- Reduction in rank
- Termination/dismissal from the services of the Company
- Any other action that the Disciplinary Authority may deem fit
- Filing a complaint before the relevant police station/court

Section VIII. Protection to Complaint / Victim:

The Company is committed to ensuring that no employee who brings forward a harassment concern is subject to any form of reprisal. Any reprisal will be subject to disciplinary action.

The Company will ensure that victim or witnesses are not victimized or discriminated against while dealing with complaints of sexual harassment.

However, anyone who abuses the procedure (for example, by maliciously putting an allegation knowing it to be untrue) will be subject to disciplinary action.

In case the Committee finds the degree of offence coverable under the Indian Penal Code, then this fact shall be mentioned in its report and appropriate action shall be initiated by the Management, for making a Police Complaint.

Section IX. Training:

All employees are required to complete the training on Prevention of Sexual Harassment each year. Employees will receive notifications from HR Team. New hire employees are required to complete the training on Prevention of Sexual Harassment during their Orientation program.

Section X. Additional Information and Committee Details:

For additional information on this Policy and associated processes, and for a list of the members of the Internal Complaints Committee, **please refer the FAQ documents for Employees and Managers.**

Section XI. Do's / Don'ts:

Do's:

- ✓ Become fully informed about sexual harassment
- ✓ Know that sexual harassment is a serious matter and is against the law
- ✓ Respect the sensitivities of others
- ✓ Report any sexually harassing behavior as soon as possible
- ✓ Know that you will not be punished for reporting the sexually harassing behavior
- ✓ Maintain confidentiality regarding any aspect of an inquiry to which you may be party

Don'ts:

- ✓ Ever allow ANYBODY (co-worker, subordinate, manager, etc.) to convince you that submitting or not submitting to sexual favors will affect your job
- ✓ Be afraid to report sexually harassing behavior
- ✓ Blame yourself or ignore the situation
- ✓ Listen to sexual jokes or allow anyone to make comments about your body or sex life
- ✓ Have anything sexual in nature posted anywhere in office environment, including a computer

Section XII. Overriding Effect

Notwithstanding anything stated elsewhere in this Policy, this Policy shall be subject to the provisions of the Act.

Exit Process – India

Objective

The purpose of this checklist is to ensure a smooth exit process for the employee while the employee is leaving Tredence.

Normal Exit:

HR:

- The employee resigns on our HRMS tool Success Factor
- The resignation needs to be approved by the Reporting Manager as well as the HRBP on Success Factor with the mutually agreed Last working day (LWD)
- HRBP sends the exit checklist to the employee 15 days prior to the LWD to seek clearance from all department before their last working day.
- On the day of exit: Employee will be requested to fill the exit feedback form on Success Factor and submit the same
- HRBP to terminate the employee on SuccessFactors post their LWD and send an email to the IT and support team to deactivate them from the system and remove from all DL's
- The salary for the last month goes on hold for all employees whose LWD is between the 9th of the current month to 8th of the next month
- The HR Operations team shares the full and final settlement input for ex-employee which has details of notice period treatment, leave encashment, gratuity, recovery if any etc.
- The Full and final clearance is done only once the asset is submitted by the resigned employee
- The Full and final is done once a month along with the monthly payroll
- The relieving letter is shared with the ex-employee once the Full and final settlement is credited or if there is a recovery from the employee is made to the organization

IT:

- IT Team to give final clearance on receiving the asset
- Employee will may either hand over the Laptop, laptop accessories, data card (if any provided) to IT team at office or courier it to the nearest office

Admin:

- Employee will either hand over his /her ID/access cards, mobile phones (If any provided) and pedestal keys (if any provided) in the nearest office or courier it to the nearest office
- Admin team will delete access card login

Termination:

Manager to intimate the HRBP immediately in case of following termination:

1. **Immediate Termination**

HR:

- The HR team will send an e-mail to employee's manager & support team regarding the termination of an employee
- The notice period is not required to be served
- The employee will be provided one-month salary payout
- The Full and final settlement process to continue as stated above

Note: We will not recover the joining/relocation bonus, if any of the employee is getting terminated within one year from his/her DOJ

IT:

- Employee will either hand over or courier the Laptop, laptop accessories, data card (if any provided) to the IT team at the nearest office
- IT Team needs to drop an email to the exiting employee's manager, asking him to share details in terms of blocking the employee's IT access, mail id, etc.

Admin:

- Employee will hand over his /her ID/access cards, mobile phones (If any provided) and pedestal keys (if any provided)
- Admin team will delete access card login

2. PIP – Performance Improvement Plan

HR:

- Employee will be put on an improvement plan in which he needs to improve his/her performance as per the goals designed by his/her manager
- The CAP period will be for one month and the manager will review as per the review intervals discussed during setting the CAP process (e.g.,7 days, 15 days and 20 days' intervals). At the time of review intervals, if the manager identifies that the employee is not adhering to the desired goals, he has the right to revoke the CAP process and terminate the employee immediately
- If the employee's performance improves the manger will decide on restraining the employee or terminate if the employee fails to improve
- If the employee does not improve, he will be terminated immediately
- HR team will also send an e-mail to the support team w.r.t. the exit and share inouts in the payroll file with the HR operations team
- The employee will be provided salary payout for the tenure within the CAP period only
- The full and final settlement process stays as updated for normal exits

Note: we will not recover the joining and relocation bonus, if any, if the employee is getting terminated within one year from his/her DOJ

IT:

- Employee will either hand over or courier the laptop, laptop accessories, data card (if any provided) to the IT team at the nearest office
- IT Team needs to drop an email to the exiting employee's manager, asking him to share details in terms of blocking the employee's IT access, mail id, etc.

Admin:

- Employee will hand over his /her ID/access cards, mobile phones (If any provided) and pedestal keys (if any provided)
- Admin team will delete access card login

3. **Absconding (Type 3)**

HR:

- Manager to inform the HRBP immediately on noticing uninformed / unauthorized absence for a continued period of 3 working days or more
- The HRBP to try reaching out to the employee through emails on personal and official mail id and on calls
- If the employee does not respond to the mails / calls the HRBP to send the showcase notice to the employee to report to work
- In case the employee does not report to work even with the notice, HRBP to raise termination for the employee
- If the employee responds to the notice and is ready to come to office and resign, we can treat this as immediate resignation
- The full and final settlement process will be done only if the employee has resigned, otherwise the employee will be terminated

IT:

- Employee will either hand over or courier the laptop, laptop accessories, data card (if any provided) to the IT team at the nearest office
- IT Team needs to drop an email to the exiting employee's manager, asking him to share details in terms of blocking the employee's IT access, mail id, etc.

Admin:

- Employee will hand over his /her ID/access cards, mobile phones (If any provided) and pedestal keys (if any provided)
- Admin team will delete access card login

ANNEXURE 1

ISG

Acceptable Usage Policy (AUP)

Tredence – Information Security Group (ISG)

Document Title	Acceptable Use Policy (AUP)
Document Number	TRE-ISMS-POL-002
Classification	Internal
Date	27/April/2022
Version	Version 1.2

Revision History

Version No	Date	Author	Approver	Document Changes
1.0	26/Feb/2022	Manoj Kuruvanthody	Manoj Kuruvanthody	Policy contents revamped in its entirety and fresh document created in coordination with ISG, Privacy, IT, HR, Legal and Marketing
1.1	27/Apr/2022	Neha Bhat Sharma	Manoj Kuruvanthody	Updated the template as a part of Tredence rebranding
1.2	20/Jul/2022	Neha Bhat Sharma	Manoj Kuruvanthody	Updated the 3rd Party Communication mechanisms under section 9

Contents

1. Purpose

Tredence and its affiliates ("Company" or "Organization") are committed to protecting its employees, partners, and thecompany ("Stakeholder(s)")from unauthorized, illegal or damaging actions by individuals, either knowingly or unknowingly.

Effective security is a teameffort involving the participation and support of employees, contractors, 3rdparty agencies orother affiliates ofthe organization who deal with information and/or informationsystems. It is the responsibility of every user to know these guidelines, and to conduct their activities accordingly.

The company provided internet, intranet or extranet related accesses, systems, applications and platforms, including but not limited to computing equipment, software, operating systems, storage media orplatforms, user, network orservice accounts providing various accesses and/or access to electronic mail, instant messaging and collaboration platforms ("Assets" or "Resources" or "Information Processing Facilities") arethe property ofthe organization. As thecase may be, the organization might also availthe usage ofClient, orany other3rd party provided assets tomeet its business objectives.All assets aretobe used for business purposes inserving the interests ofthe company, and of our Partners.The term Information Processing Facilities may attimes also construeas the physical facilities fromwhich the organization's business activities are conducted.

Thepurposeofthispolicy is to outlinethe acceptable useofthe organization's assets. Theserules are designed to protect interest of allstakeholders and assets in the organization. Incorrect or inappropriate use exposes the organization and/or stakeholders to risks including malware attacks, compromise of confidentiality, integrity or availability ofassets andnon-complianceto Customeror Client contractualobligations orrelevant Statutory or Regulatory Compliance mandates.

Additionally, the objective ofthis policy is to educateend users onthe acceptable usage and securityroleand responsibilities ofemployees, contractors and third-party users ("User(s)")of organization's information and information processingfacilities. All users are expected to adhere to the Information Security and Privacy Policies, including this Acceptable Usage Policy (AUP) in itstrueletter and spirit. Any queries on thesame shall be directed toInformation Security Group(ISG) at InfoSec@tredence.com

2. Scope

This policy applies to employees, contractors, consultants, and all the resources associated directly or indirectly with us; including all assets owned or leased to the organization. The recentchanges in the global threat landscape has in turn

affected how organizations operate, from within the organizational physical space, work remotely (e.g.: workfrom home), or in a hybrid model, thereby widening the scopeof thecomplianceexpectations to even includesecure operations from a remotework scenario as well.

3. General use and ownership

While the organization desires to provide reasonable level of privacy, users should be aware that the data which users read, modify or create on all assets remains associated directly or indirectly with the organization. Because of the need to protect the organization's network, management cannot guarantee the confidentiality of information stored on any network device belonging to organization.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

For Organizational Policy as well as Statutory and Regulatory compliance monitoring and its continuous maintenance purposes, the organization may monitor assets, data files, emails and any communication / traffic sent or received using the organization's assets in any format – oral, written or printed on paper, emails, instant messaging or other collaboration platforms etc. - which may be owned or managed by the organization though an individual, groups, affiliate firms, agencies, Clients, within or outside the organization's physical or logical boundaries, at any time, with or without prior notice to the users.

Organization reserves the right to audit, directly or through its authorized 3rd party agencies, any IT Assets owned or managed by the organization (e.g.: on behalf of the Client) on a periodic basis to ensure on going Information and Privacy compliance.

Actions prohibited by this Policy or controls could have exceptional scenarios specifically in cases where IT or Security teams might need to perform support, monitoring or investigation activities.

All users of the organization are policy-bound to adhere to the Information Security and Privacy policies ("Policy" or "Policies") including this Acceptable Usage Policy.

4. Cyber security responsibilities and expectations

- Detailed Policies are made available on the company intranet / Success Factors environment ("Portal(s)") for ease of reading and comprehension. Any queries can be directed to InfoSec@tredence.com or other Policy stakeholders as the case may be.
- In line with the detailed policies, below excerpts are made available for quick reading so the user may understand the spirit of the policy compliance expectations and ensure compliance on the same.
- Users must pay heed to all Information Security and Privacy Advisories sent by InfoSec@tredence.comto keep themselves abreast with the various Policy and Compliance expectations on the same.

5. Information Security andPrivacyPolicies and Procedures

- Data Security and Privacy is imperative to the success of every business.
- It is important that each user adhere to the defined and published Information Security and Privacy Policies and Procedures, so organization is able to comply with contractual commitments as well as maintain compliance against Statutory and Regulatory requirements.
- Users shall conform to their respective roles and responsibilities with respect to Information Security and Privacy.
- Users are responsible for protecting the data and information in their hands. Remember, "***Security is everyone's responsibility***"

6. Physical security

- All users shall ensure they wear the organization identity cards visibly all the times when at organization premises; and when applicable at certain events (e.g.: workshops, conferences etc.) as mandated by the management.
- Users must protect organizational assets from unauthorized access, disclosure, modification, destruction or interference and return the asset after business use.
- Users are prohibited from setting up or installing any personal hardware assets within the organization physical or logical security boundaries without prior IT clearance.

- Users must ensure that storage media of any kind such as, but not limited to, USB, CD's, hard disks – are brought into the organization only after Manager authorization and subsequent clearance after IT scans the media for possible malware. It must be noted that the use of personal electronic storage devices within the organization premises or on its network is strictly prohibited in order to prevent information leakages, Intellectual Property Rights (IPR) or Copyright violations, unauthorized disclosure of confidential information etc.
- For the sake of clarity, personal electronic storage devices may fall into these prohibited categories such as, but not limited to,
    - **Computer systems:** Computer systems can be used to store sensitive data and may introduce viruses into the network. Handheld computer systems can be of particular concern which may lack the security of its larger counterparts as their small size makes them easy to lose or steal. Examples include but are not limited to PCs, laptops, Tablet PC, electronic organizers and smart devices (e.g.: smart watches).
    - **Recording devices:** Audiovisual recording devices represent a threat for obvious reasons. Examples include digital cameras, PC cameras, video recorders that are restricted in organization and smart phones.
    - **Data Storage devices:** small storage devices and backup media could be used to transport large quantities of sensitive information. Typical examples could be data storage devices which are capable of transferring and copying data using Zip drives, CDRW drives, USB storage devices and any storage mechanisms that may allow data transfer between the organizational asset and the unauthorized device directly from the asset, through LAN cable connectivity, wirelessly or through Bluetooth connectivity options.
- Users must protect organizational assets from theft. Example scenarios such as in the following might be of special interest to users. Typical use cases would be using phones or laptops while travelling.
    - Use of mobile phones or laptops in public spaces where someone can oversee the device screen gleaning sensitive business contents
    - Momentary leaving of the laptop during airport baggage scanning
    - Working from non-Tredence environments such as current or prospective Client or vendor premises etc.
- An ideal approach to prevent laptop theft is to make use laptop cable locks to physically secure the laptop to a desk.

- All visitors and 3rd party personnel must be escorted during their presence within the organization and their actions monitored.
- Consultants and visitors must be advised on Policy restrictions and monitored for Security compliance by the user escorting the visitors.
- Users at no point in time must shift, open or tamper any organizational assets from its original state or configuration.
- In an event of damage or loss of an asset, the user will be held accountable for the incident and damages might be recovered from the user.

7. Desktop,laptop andmobile computing deviceusage

- All company provided assets, such as, but not limited to, desktop, laptop and mobile phones must be used for business purposes, for the benefit of the organization, and shall adhere to the Mobile Device Policy
- Specific provisions allocated to users, such as, but not limited to, exemptions on access to,
    - certain internet portals
    - local administrator privileges on endpoint or other systems or applications
    - USB access to systems must be used strictly for business purposes alone to avoid data loss or theft.
- Users must keep electronic as well as paper assets away from food and drinks to avoid spillage and damage
- If provided, users must ensure laptop data cards are used only for business purposes and not accessed or used by unauthorized individuals
- Do not install any software without approval from IT. In case of any deficiency, personnel who is having access to systems will be held responsible and warning letter will be issued.
- Users are strictly prohibited from making changes to or disabling any IT or Security controls in the assets in an effort to circumvent data protection schemes or uncover security loopholes. Examples are as follows, but not limited to, changing default configuration, disabling anti-virus, enabling / disabling certain services in the system etc.
- Users must not share their session for another unauthorized individual to use except for cases where IT Support needs to troubleshoot. Business exceptions to this, if any, must be approved by the Manager prior to such actions.
- Users must not use another system or application which they are not authorized to use.

- Users must not knowingly perform an act which will interfere with the normal operation of computers, terminals, peripherals, or networks. These shall consist of the following, but not limited to, the user knowingly running or installing on any computer system or network, or sharing with another user, programs intended to damage or to place excessive load on computers or the network. The tools or software in this context may or may not include computer viruses, trojan horses, and worms, hacking or cracking tools, packet sniffers etc.
- Users must not attempt to break into other organizational or Client systems or applications through unethical means and cracking codes of illegally downloaded applications. It must be noted that, such initiatives are strictly controlled through Information Security Group (ISG) subject to the organization's Information Security and Privacy control requirements.
- Users must ensure they do not perform activities on systems or applications to,
    - deliberately waste computing resources
    - gain unauthorized access to resources
    - attempt to obtain additional resources which is not authorized or,
    - deprive an authorized user from using official resources.
- Users must not attempt to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files, folders, software or system without the explicit agreement of the owner.
- Users will be granted access to the organizational network through mobile phones only after the user enrolls the device into the organizational Mobile Access Management (MAM) solution and the device meets the Security Compliance requirements. On this regard, mobile phones without dated operating systems or 'jail broken' (or 'rooted') phones will be automatically blocked from connecting to the network.
- Mobile devices connecting to organization wireless network should have an up-to-date anti-malware software installed and running; its network and internet activity will be monitored and must be restricted to official use only.

8. Personal devices

- Personal devices are permitted to be used in a Bring Your Own Device (BYOD) context wherein the user can access organizational resources through their personal mobile phones or laptops with controlled accesses

9. Electronic email, instantmessaging and collaboration platforms

- Electronic email, instant messaging and collaboration platforms ("communication mediums") shall be used purely for business purposes. Products and platforms such as Microsoft suite of products are made available on official devices and environments. Any changes or additions to the same will be notified to the users from time to time.
- Use of organization's communication mediums must be treated by all users as a privilege and not as a right.
- Unauthorized use of the communication mediums is not permitted which includes, but not limited to, transmitting or storing offensive material; sexual implications, gender specific comments, defamatory statements, or any other comment that offends someone's religious or political beliefs, national origin, or disability; compromising the security of information contained in Company computers; conducting or soliciting for political, personal, religious or charitable causes or other commercial ventures outside the scope of the users' employment and users' responsibilities to the organization.
- Any use of 3rd party / unauthorized products or platforms for official communications are strictly prohibited including 3rd party file sharing sites
- Client related engagement's which involve connectivity to external environments should ensure the following controls such as, but not limited to,
    - Prevention of print screen between the remote environment (e.g.: Client side) and the local machine (e.g.: Tredence laptop)
    - Prevention of copy / paste of data or files between the two environments to and fro
    - Prevention of cross-domain emailing (a feature where Tredencians provided with Client credentials can email only within the Client's domain alone and not to another other email domains (e.g.: Gmail, Yahoo! etc.)) and,
    - Strict internet content filtering

Note: These may apply vice versa as well, if remote access to Tredence environment are to be considered inbound from a third-party

- Organization's email systems should be mainly used for business purposes and users must restrict personal use of the same to bare minimum.
- The language used on all communication mediums should be consistent with other forms of business communications.

- Users must not upload or email organizations or Client's sensitive and/or confidential data to any 3rd party web sites or to their own personal email ID's created on free email sites on the internet.
- Users shall exercise due care while using the communication mediums by following the Information Labelling and Classification Policies.
- The communication mediums must not be used for any illegal activities or to create, send, receive, or store any offensive or disruptive messages, or materials that infringe the copyright or other intellectual property rights of the organization, Clients or any third parties.
- All Personally Identifiable Information (PII) / Personal Health Information (PHI) must be transmitted outside organization for official purposes through encrypted means only. This shall include methods as follows, but not limited to, encrypting the file, access restricting the email itself – with or without timebound restrictions – and using an encrypted email communication channel (e.g.: TLS encryption) between the organization and the recipient email gateways.
- Downloading and usage of Chat software organization's assets is not permitted unless explicitly need for business purposes. This too shall only be allowed for us post IT and ISG clearances.
- Organization reserves the right to audit, retrieve and read any messages transiting through its communication mediums without prior notice.
- Users must avoid opening any mail from unknown users or sources and avoid downloading or opening suspicious attachments or clicking on suspicious links.
- Users must be watchful at all times regarding phishing emails or even URLs received through various communication mediums such as SMS, WhatsApp, Telegram etc. as that could compromise the security posture of the environment.
- Users must only disclose information or messages obtained from the communication mediums to authorized recipients on a need basis.
- Users are not authorized to retrieve or read any communications that are not intended for them.
- Users should not attempt to gain access to other employee's messages without the user's explicit permission.
- Users must not auto-forward emails to external (non-Tredence) mailboxes as

that could lead to sensitive or confidential data leakage. However, email auto-forwards shall be permitted on specific business reasons post Manager approval.

- Users must not use any organizational communication mediums to harass users in any manner.
- Users must ensure that they do not send personal advertisements, invitations, forwarding chain letters, mass mailing or religious mails to large groups
- Users must not post any documents / materials on electronic bulletin boards without proper approvals.
- Users must avoid subscribing to internet mailing lists which could lead to spamming of the mailbox.
- All electronic communications must be secured so that only authorized users have access to the same using security controls such as, but not limited to, password protection, encryption etc. On any queries on this topic, users may reach out to IT.Support@tredence.com

10. Internet Usage

- Internet usage shall be restricted to business purposes; however, users may use their judgement on the best use as part of their day to day activities so as to ensure non-business usage of internet is kept to the bare minimum.
- Users should strictly avoid visiting nonbusiness, offensive unethical sites which violate organization security policies.
- Users must not try to circumvent proxy controls to misuse internet facilities.
- Users are strictly prohibited from downloading songs, movies, humor clippings, unauthorized software, pornographic and/or other non- business or any other non-productive materials.
- Internet access controls are in place to detect and stop users from visiting unauthorized websites which may host harmful content or infect Tredence assets with malware. Such sites may host contents such as, but not limited to, malicious code or software, illegal documents, pornography etc. however, it must be noted that in an event a harmful site is found to be accessible, users are expected to close the browser immediately and report the same to Incident_Management@tredence.com

- Mobile devices connecting to the organization wireless network must not be used to visit unauthorized, illegal or malicious sites.
- Users are not permitted to download any illegal or unauthorized documents or software nor download or install code / software from websites. Any business requirements on the same shall be routed through IT.Support@tredence.com

11. Teleworking and Remote Access

- To permit flexibility and thus ease of use and operations, the organization has permitted teleworking and remote access to all its users. It must be noted that, teleworking as an option of work is an HR Policy matter and HR may review and revise the same basis business circumstances.
- Remote access into organizational resources are provided basis business requirements
- Users must only use pre-approved methods of remotely connecting to organizational or Client assets.

12. Servers,file storage, printers,photocopiers and scanner usage

- Use of these devices shall be strictly for business purposes alone
- To ensure due care to the environment, paper must be used sparingly and thoughtfully, and only if absolutely needed – while printing
- Documents while being scanned may be sent only to organizational email IDs
- Storage of files and folders in servers must be utilized to store only content for business purposes

13. Videoconferencing, Voice Over IP (VoIP) networks and PSTN

- Video conferencing, VoIP and PSTN provisions provided by Tredence must be used for business purposes
- As the technology capabilities grow globally as well as within Tredence, Tredence IT may provide newer tools (e.g.: Microsoft Teams) to leverage for all business purposes
- It may be noted that, external video conferencing invites from current or prospective Clients or vendors, or from conference or workshops producers may

involve utilizing other conferencing and/or collaboration platforms. If in doubt, the user may connect with IT.Support@tredence.com for clarifications

14. Use of authorized software

- Users are advised to strictly use Tredence provided software at all points of time and are prohibited from using any software such as, but not limited to, unlicensed or shareware or freeware without prior approvals from the user's Manager and subsequent IT clearance. It is imperative that users do not violate terms of any applicable software licensing agreements or copyright laws.
- Users must not download software on their own from the network or internet. Any business requirements that necessitate download and/or install must be routed through IT Helpdesk with a business case approved by the Manager on a case-to-case basis.
- Users should not distribute software as they do not have the right to do so. Contact IT Helpdesk on all software requirements.
- Any need use a software which is not available within Tredence, the user may reach out to IT.Support@tredence.com to assess the requirement and provision the same.

15. Classification of assets

- Users are requested to follow the Data Classification and Labelling Policy so as to ensure data is rightly classified and controlled through its usage lifecycle

16. Handling of information in public and internet

- Users must be cautious while handling business specific information in public spaces. This includes the following scenarios, but not limited to,
    - handling calls which might be of business importance
    - working on mobile phones or laptops

where someone could overhear a business sensitive conversation or might be able to view the contents on the mobile phone or laptop screen in turn resulting in a sensitive data leakage.

- Users must not post any proprietary information of the organization or Client on the internet such as, but not limited to, file sharing sites, discussion forums, email, newsrooms or bulletin boards. Any violation to these could attract severe disciplinary repercussions up to termination from employment including with legal consequences.
- Users must be aware that their digital presence (internet), and social media in particular, could many a times be subject to readers online tying that to the organization of employment. Therefore, it is critical for the users to exercise extreme caution while conducting themselves online to prevent confidentiality breaches as well as reputational or financial damage to the organization or its Clients; in turn resulting in impact to the brand image.
    - Users must not solicit to any activity or purpose which is not expressly approved by the organization management and attempt to reveal or publicize proprietary or confidential information of the organization or of its clients' to any other third party.
- Users must not represent personal opinions on internet as those of the company.
- During the course of their employment, if the employee is reached out by external parties, to respond to various internal and/or sensitive topics with respect to the business, they must strictly forward all such queries or media interactions to the Tredence spokesperson / Marketing Team.

17. Clear disk and Clear screen Policy

- Users must lock their computer system by using (Ctrl + Alt + Del) keys followed by "Lock Computer" or (Windows Key + L) when moving away from their workstation/laptop instead of waiting for the screensaver to lock the screen automatically.
- Users should not leave unattended hard copies of sensitive information or media near the workstation areas or their respective cubicles / tables / desks and ensure they lock all confidential documents and personal items in drawers or lockers before moving away from their workspace.
- Employees must keep a clean desk and remove / shred unnecessary papers if no more required.
- Employee must not print sensitive documents to a far-off printer where they have

to go a long way to collect after giving the print command as printed document might become accessible to another user next to the printer. The best practice is to ensure all print commands are given using PIN protection so the user can input the PIN before the printer prints the document so the user may collect the same immediately and safely

- Employee must not display sensitive information (passwords, IP addresses, customer sensitive information, and personal data) on dashboard or post it (sticky notes) in their cubicle which could lead to unauthorized accesses.

18. Introduction of malicious code

- Users must not download unauthorized code onto organizational assets as it might lead to vulnerabilities being introduced into the overall application software being built or maintained.
- Before being put into use, ensure any open-source code, complies with open source licensing requirements and also undergoes a vulnerability assessment so as to detect and mitigate vulnerabilities in a timely manner before the application software product release
- If in doubt, users may write to InfoSec@tredence.com

19. Password use, its re-use, authentication and authorization

- Users are assigned a unique "User ID" for their login into various business systems, applications and platforms and strictly use the same for all business requirements.
- Users are required to follow all relevant policies and procedures related to access control.
- Users shall ensure that they choose a password that is hard to guess and complies with the Password Management Policy.
- Users shall keep their passwords confidential and shall not divulge it to anybody, under any circumstances, nor shall they write it down or record it and leave it anywhere that it can easily be found by someone else.
- Authentication of user credentials to business systems and applications together with various levels of authorization shall be strictly used for only business purposes.

- Users must never obtain another credential (e.g.:User credential, system or application access credentials etc.) which they are not authorized to use.
- Users must not use any common account unless it's operational necessity and appropriate approvals are in place.
- At any event, if the user thinks that the password is compromised, the user must immediately reset the password. Additionally, if in suspicion of a Cyber Event, the user must immediately report the same to Incident_Management@tredence.com
- Users with privilege access must ensure their access rights are perused only for the defined business purposes alone for which the access was originally granted.

20. Return of assets

- Users are required to return any and all assets provided by the organization once the need for business use ceases. Few example scenarios could be,
    - if the user is transferring out of a certain project or,
    - is separating from the organization.
- Examples of actions taken can be as follows, but not limited to,
    - Return of company provided mobile phone and/or laptop
    - Systematically complete all the needed knowledge transfer and associate document transfer to authorized personnel who will work in that area

21. Use of proprietary information

- Users will be privy to business sensitive information as part of their day-to-day work.
- All users are expected to strictly ensure all business information is kept confidential through-out its usage lifecycle. This might include the following, but not limited to, o Organizational or Client Intellectual Property (IP)
    - Know-how of various business processes, tools and technologies
    - Documentation, software code and applications

This is applicable during as well as post-employment with Tredence.

22. Business Continuity Planning and Disaster Recovery (BCP-DR)

- Business Continuity Planning (BCP) is critical to ensure the availability of all critical resources if the business experiences adverse events which could otherwise hinder its day-to-day operations.
- Disaster Recovery (DR) is considered in a post BCP scenario wherein a predefined set of actions are considered to recover the business back so it may return to a Business As Usual (BAU) state.
- All users are required to support the organization in its efforts on BCP- DR.
- Client specific operations might have a need to have tailored BCP-DR approaches which requires to be adhered to.
- Users are expected to ensure all sensitive or business critical data is stored on a central data store (e.g.: Microsoft OneDrive, secure file servers with stringent access controls etc.) which is securely access controlled. This many a times might be a Business Continuity Planning (BCP) expectation too, for the organization and/or Client as applicable. On any queries pertaining to data storage, users may reach out to IT.Support@tredence.com

23. Security monitoring

- Organization maintains the right to review, audit, intercept, access, monitor, delete and disclose all messages created, received, sent, or stored on its communication mediums and assets in any form.
- All data within the organizational assets and all copies of messages created, sent, received, or stored on the system are (and remain) directly or indirectly associated with the organization the property of organization
- All access into and within the Tredence will be monitored for Policy compliance and associated monitoring purposes
- Access into Tredence and environment is permitted only for authorized users
- All assets in the environment are licensed and/or directly or indirectly proprietary to Tredence or that of the Client's

- By accessing and using Tredence assets, the user consents to system monitoring towards Information Security and Privacy compliance, law enforcement and other purposes; monitoring shall be exempted in situations superseded by the law of the land
- Unauthorized use of the environment may subject the user to disciplinary proceedings including, but not limited to, criminal prosecution and penalties and any equitable relief
- A login banner with the above advisory is also provided for user reference and compliance

24. Reporting Security or Privacy events, potential weaknesses or risks

- User must report Security or Privacy events or potential weaknesses or risks to the Information Security Group (ISG) immediately via any of the following methods,
    - Email to Incident_Managemen@tredence.com
    - Create a ticket and mark it to ISG
- Inform organization Helpdesk immediately if you think that your workstation may have a virus.

- Ensure that you use only the system which is allocated to you Report any SPAM mail received to infosec@organization.com
- Any new/change requirement in the service/resources should be done through IT service desk portal.

25. Disciplinary action

- Any misconduct pertaining to or in violation to the abovementioned policy will be adequately governed by HR disciplinary procedures
- Users in violation of these policies may be subject to disciplinary proceedings including, but not limited to, criminal prosecution and penalties and any equitable relief

26. Document ownership and updates

- Information Security Group (ISG) is the owner of this document and is responsible to keep

this document up to date as needed.

- On a case to case basis, ISG may consult with relevant stakeholders such as Privacy Office, IT, HR, Legal, Finance, Facilities, Physical Security and Delivery on subsequent revisions.

27. Review frequency of this document

Thedocumentwillbe reviewedonneed basisorat leastannually for any updates as required.

28. References

- ISO 27001:2013