

SAP FORM

1 SAP ID (Office Use Only)

2 Temp ID

3 Date of Joining Process.....

4 NameMirza.Ahad.Begh..... GenderMale..... / F.....

5 Date of Birth ...31./01/..1996..... 6 Place Of Birth ...Raebareli..(U.P).....

7 Marital StatusUnmarried (Unmarried/married/Widow/Widower/Divorcee)

7 (a). Date of MarriageNo..... 7 (b). Spouse DOB.....No.....

7 (c). Spouse NameNo..... 7 (d). Spouse OccupationNo.....

7 (e). No. Of ChildrenNo.....

8. PermanentAddress...ANWAR..NAGAR..COLONI.RATAPUR..RAEBARELI..(U.P).....PIN.....229001.....

9. Mobile No. ...8423136920..... 10. Land Line No. (If Any)

11. Father's Name ..Mirza..Ayub.Begh..... 12. Father's Date of Birth

13. Father Occupation ...Bussinessman..... 14. PAN

15. Blood Group.....B+..... 16. Emergency Contact no.....

17. E mail IDmdahd44@gmail.com.....

18. Education

Qualification	Board / University Name	Year of Passing	Area of specialization/ Stream	Degree / Diploma	% Age / Rank
High School	ICSE	2012	ALL	10TH	50.43%
Intermediate	ISC	2014	PCM, HINDI, ENGLISH	12TH	45.20%
Graduate Degree	CSJMU KANPUR UNIVERSITY	2019	SCIENCE	B.SC	50.00%
Post Graduate Degree					
Diploma	NIELIT	2016	ALL	COMPUTER APPLICATION & MULTILINGUAL DTP	70%

19.

Nomination Form	Name of Nominee	Nominee Address	Relationship with the member	Date of Birth	Nominee %
PF (pg-9)	1 MIRZA AZIB BEG	ANWAR NAGAR COLONY RATAPUR RAEBARELI (U.P)	BROTHER	14.08.1997	100%
Gratuity (pg-14)	1 MIRZA AZIB BEG	ANWAR NAGAR COLONY RATAPUR RAEBARELI (U.P)	BROTHER	14.08.1997	100%
GPA (pg-16)	1 MIRZA AZIB BEG	ANWAR NAGAR COLONY RATAPUR	BROTHER	14.08.1997	100%

			RAEBARELI (U.P)			
ESI (pg-17)	1	MIRZA AZIB BEG	ANWAR NAGAR COLONY RATAPUR RAEBARELI (U.P)	BROTHER	14.08.1997	100%
General Nomination	1	MIRZA AZIB BEG	ANWAR NAGAR COLONY RATAPUR RAEBARELI (U.P)	BROTHER	14.08.1997	100%

20. Work Experience

Name of Employer / City	Date of		Designation	Salary details	
	Joining	Leaving		At Start	While Leaving
MIRZA AHAD BEGH	01-07-2018	21-08-2020	C.S.E	11000	15000

21. Bank Account No. ...37350100008841.....
...BARB0FGIETX.....

IFSC CODE

Bank NameBANK..OF..BARODA.....(RAEBARELI).....

22. Mother's NameHUSNA..PARVEEN.....
.....45.....

23. Mother's Age

All of the above mentioned details are true to the best of my Knowledge

Mirza Ahad

Employee Signature

Date

Joining Docket for Agent Staff

Name: MIRZA AHAD BEGH

SAP ID:

Date of Joining:

Welcome To Aegis Customer Support Services Pvt. Ltd.

Documents Checklist for Personnel File

SN	Documents @ Joining	Mandatory / Desirable	Tick if Available
1	Resume	Mandatory	YES
2	Interview Assessment Sheet	Mandatory	
3	Score Sheet	Mandatory	
4	Candidate Information Sheet	Mandatory	
5	Offer Letter (Acknowledgement Copy)	Mandatory	
6	Appointment Letter (Acknowledgement Copy)	Mandatory	
7	Age Proof	Mandatory	YES
8	Photo ID Proof	Mandatory	YES
9	Pan Card Copy	Mandatory	YES
10	Photographs (2)	Mandatory	YES
11	Address Proof	Mandatory	YES
12	Educational Proofs (All education docs as per the declaration in CIF)	Mandatory	
13	Previous employment proof	A-- Combination of 2 and 4 B--Combination of 4 and 5 C--Combination of 1 and 4 D--Combination of 1 and 5 (In case DOJ is mentioned on the salary Slips) E--only relieving letter would do in case DOJ is mentioned	Any one of these is acceptable
	1. Relieving letter		
	2. Accepted copy of Resignation		
	3. Offer Letter		
	4. Appointment letter		
	5. Last 3 months salary slips		
14	Nomination form for Hospitalization reimbursement	Mandatory	
15	ESIC Form 1 (Photocopy)	Mandatory	
16	PF Form 2 (Photocopy)	Mandatory	
17	PF Form 11	Mandatory	
18	Form 12 B	Mandatory	
19	Gratuity Form F	Mandatory	
20	Medical Check up Report (If applicable)	Mandatory	

21	Background verification Report (If applicable)	Mandatory	
	Documents during Employment Life Cycle		
1	Transfer Letter	Mandatory	
2	Appraisal Form	Mandatory	
3	Increment letter	Mandatory	
4	Promotion Recommendation form	Mandatory	
5	Promotion letter	Mandatory	
6	Performance Improvement plan (CAP/ Termination letter)	Mandatory	
7	Salary revision Letter	Mandatory	
8	Re - Designation letter	Mandatory	
9	All Related emails	Desirable (Case to case Basis)	
	Documents during Separation		
1	Resignation Letter	Mandatory	
2	Resignation Acceptance Letter	Mandatory	
3	Exit Interview Form	Mandatory	
4	Relieving letter	Mandatory	
5	Copy of Show Cause Notice	Mandatory	
6	Letter of abandonment of services	Mandatory	
7	F & F Document	Mandatory	
8	Any related emails	Desirable (Case to case Basis)	
9	Copy of DD Received (For recovery cases)	Mandatory	
	Other		
1	Letter of Recovery of Dues	Mandatory	



Application Blank
(To be filled in block letters)

1. Name: MIRZA AHAD BEGH
 2. Present Address : ANWAR NAGAR COLONY RATAPUR RAEBARELI (U.P)
 3. Permanent : ANWAR NAGAR COLONY RATAPUR RAEBARELI (U.P)
 4. Residence Phone : 5. Mobile: 84231369206. E-mail(s) : mdahd44@gmail.com
 7. Date of Birth : 31-01-19968. Place of Birth : RAEBARELI9. Nationality : INDIAN
 10. Religion : ISLAM11. Gender : MALE12. PAN : CSPPB3052G
 13. Passport No..... 14. Blood Group : B+15. Height (in cms) : 164cm
 16. Weight (in kgs): 70 17. Are you physically fit? (If no, please give details)
 18. Bank Name: BANK OF BARODA19. A/C No: 3735010000884120. IFSC Code: BARB0FGIETX
 21. Aadhar : 790755098371
 22. Last Drawn CTC (Cost to Company).....

20. Family Particulars: Marital Status: Single Date of Marriage

Family member	Name(s)	Date of Birth	Occupation
Spouse			
Children			
Father	MIRZA AYUB BEGH		BUSSINESSMAN
Mother	HUSNA PARVEEN		HOUSE WIFE
Siblings	BROTHER	14-08-1997	STUDENT

19. Academic Qualifications (Start from latest qualification and end with SSC)

Degree / Diploma	Board / University	Year	% (Marks)	Subjects/Stream
Post Graduate				
Graduate	CSJMU KANPUR UNIVERSITY	2019	50%	B.SC
Intermediate	ISC	2014	45.20	PCM, ENGLISH ,HINDI
High School	ICSE	2012	50.43	ALL

20. Total Work Experience2.Years.....

21. Past Employment

Employer's name, annual sales and no. of employees	Last Designation	Period		No. of employees supervised
		From	To	
HOINMALSONS ENTERPRISES PVT.LTD RAEBARELI	CSE	2018	2020	150

22. Brief description of function and duties in last employment

Resolving the queries of customer ,figuringout the solution for their problem related to product ,promoting the product by contacting customer through call and Mail and maintains the company sales,purchase and stock data

24. Other Interests (sports / hobbies)Bike

Riding.....

25. Have you been interviewed/ selected by company before? If yes, please give details..No.....

26. Name, department and designation of friends & relatives employed with AegisNo.....

27. Name, department and designation of close relatives employed with competitorsNo.....

28. Are you associated with professional institutions? If yes please give details

Name and address of the institution	Position
N/A	N/A

29. Indicate your familiarity in languages (please tick)

Language(s)	Read	Write	Speak
HINDI AND ENGLISH	✓	✓	✓

30. References (please give references other than relatives)

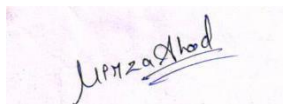
Name : MOHD SALEEM KHAN Company & Designation : Address : RAEBARELI (U.P) Tel No : 9066752237	Name : MOHD BILAL Company & Designation Address : : RAEBARELI (U.P) Tel No : 7078639955
--	--

31. Emergency Contact Details (Name, Address and Phone no. of the person)

.....MIRZA.AZIB.BEG...,ANWAR.NAGAR.COLONY.,RATAPUR..RAEBARELI..(U.P).Pin:-229001.....Mob:-
.9718165124.....

Declaration

I hereby certify that the information provided by me is true to the best of my knowledge. Any changes in the details furnished above will be intimated to you immediately.

A handwritten signature in blue ink, appearing to read 'M. P. Singh', written on a light pink background.

Signature Date :

Place : RAEBARELI



SAP ID: _____

LOCATION: RAEBARELI

EMPLOYEES' PROVIDENT FUNDS ORGANISATION

NOMINATION AND DECLARATION FORM FOR UNEXEMPTED/EXEMPTED ESTABLISHMENTS

Declaration and nomination form under the Employees Provident Funds (EPF) and Employees' Pension Scheme (EPS) (Paragraph 33 and 61 (1) of the Employees Provident Fund Scheme, 1952 and Paragraph 18 of the Employees' Pension Scheme 1995)

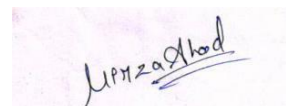
1. Name (IN BLOCK LETTERS): MIRZA AHAD BEGH
2. Father's/Husband's Name: MIRZA AYUB BEGH
3. Date of Birth: 31/01/1996
4. Gender: . MALE
5. Marital Status: UNMARRIED
6. Member ID/UAN:.
7. Date of Joining:
8. Address (Resident): ANWAR NAGAR COLONY RATAPUR RAEBARELI (U.P) Pin:-229001

PART-A (EPF)

I hereby nominate the person(s)/cancel the nomination made by me previously and nominate the person(s) mentioned below to receive the amount standing to my credit in the Employees Provident Fund, in the event of my death.

Name of the nominee (s)	Address	Nominee's relationship with the member	Date of Birth	Total amount or share of accumulations in Provident Fund to be paid to each nominee	If the nominee is a minor, name and address of the guardian who may receive the amount during the minority of the nominee
MIRZA AZIB BEG	ANWAR NAGAR COLONY,RATAPUR RAEBARELI(U.P) Pin:- 229001	BROTHER	14.08.1997	100%	NA

1. *Certified that I have no family as defined in para 2 (g) of the Employees Provident Fund Scheme 1952 and should I acquire a family hereafter the above nomination should be deemed as cancelled.
2. *Certified that my father/mother is/are dependent upon me.



***Strike out whichever is not applicable

Signature/Thumb impression of the subscriber

PART-B (EPS)

Para 18

I hereby furnish below particulars of the members of my family who would be eligible to receive Widow/Children pension in the event of my death in service.

Name and Address of the Family member	Date of Birth	Relationship with the member
MIRZA AZIB BEG	14.08.1997	BROTHER

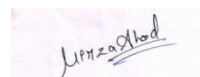
**Certified that I have no family as defined in para 2 (vii) of the Employee's Family Pension Scheme 1995 and should I acquire a family hereafter I shall furnish particulars there on in the above form.

I hereby nominate the following person for receiving the monthly pension (admissible under para 16 2 (a) (i) & (ii) in the event of my death without leaving any eligible family member for receiving pension.

Name and Address of the nominee	Date of birth	Relationship with the member
MIRZA AZIB BEG	14.08.1997	BROTHER

Date: _____

*



** Strike out whichever is not applicable

Signature/Thumb impression of the subscriber

CERTIFICATE BY EMPLOYER

Certified that the above declaration and nomination has been signed/thumb impressed before me by Shri/Smt./Ms. SYEDA HALIMA FAZILATH employed in my establishment after he/she has read the entries/entries have been read over to him/her by me and got confirmed by him/her.

For **AEGIS CUSTOMER SUPPORT SERVICES PVT LTD**

Place: RAMANAGARAM

Date:

Authorized signatory

AEGIS CUSTOMER SUPPORT SERVICES PVT LTD
3rd floor, Varun Towers-2, Begum pet
Hyderabad- 500 016, Telangana
Tel: 040-661660000



FORM – 1
DECLARATION FORM (Regulation – 11& 12)

To be filled by the employee after reading instructions overleaf. Two Postcard size photographs are to be attached with this form

A)	Insured Persons Particulars-	B) EMPLOYER'S PARTICULARS			
1	Insurance No. : «	9	Employer's Code No :		
2	Name. MIRZA AHAD BEGH	1 0	Date of Appointment	Day	Month
3	Father/Husband's Name. : MIRZA AYUB BEG			Year	
4	Date of Birth. : 31.01.1996	1 1	Name & Address of the employer: Aegis Customer Support Services Private Limited		
5	Sex : Male/Female : MALE				
6	Marital Status : M/U : UNMARRIED				
7	Present Address. ANWAR NAGAR COLONY, RATAPUR RAEBARELI (U.P) Pin code : 229001	1 2	In case of any previous employment please fill the det. As under		
8	Permanent Address. ANWAR NAGAR COLONY, RATAPUR RAEBARELI (U.P) Pin code : 229001 :		a. Previous Ins. No.:		
			b. Employer's Code No:		
			c. Name & Address of the Previous Employer :		
Branch Office:					
Dispensary :					

(C) Details of Nominee u/s 71 of ESI Act 1948/Ruls 56(2) of ESI (Central) Rules 1950 for payment of each benefit in the event of death.

Name	Relationship	Address
MIRZA AZIB BEG	BROTHER	ANWAR NAGAR COLONY, RATAPUR RAEBARELI (U.P)

Mirza Ahad
Signature of the Employer

Signature of the T.I./I.P

Family Particulars of Insured Person

SI No.	Name	Date of Birth/Age	Relationship With the employee	Whether residing with him/her		If No, State If No, State Residing
				Yes	No	
1						
2						
3						

ESI Corporation Temporary Insurance Card

Name		
Insurance No.		
Date of Appointment		

Branch Office		
Dispensary		
Employer's Code No.		
Employer's Name and		
Address		

Validity Dated _____

Signature of T.I./I.P.

Signature of Branch Manager with Seal

I hereby declare that the particulars given by me are correct to the best of my knowledge and belief. I undertake to intimate the Corporation any changes in the membership of my family within 15 days of such change.

FOR BRANCH OFFICE USE ONLY

INSTRUCTIONS

- Submission of Form-1 is governed by regulations 11& 12 of ESI (General) Regulations, 1950
- 'Family' means all or any of the following relatives of an insured person namely.
 - a spouse (ii) a minor legitimate or adopted child dependant upon the I.P. (iii) a child who is wholly dependent on the earnings of the I.P. and who is (a) receiving education till he or she attains the age of 21 years (b) an unmarried daughter: (iv) a child who is infirm by reason of any physical or mental abnormality of injury and wholly dependant on the earnings of the I.P. so long as the infirmity continues, (v) dependent parents (Please see section 2 clause 11 of the ESI Act 1948 for details)
- Identity Card is Non-transferable.
- Loss of identity Card is reported to the Employer/Branch Manager immediately.
- Submission of false information attracts penal action under Section 84 of the ESI Act 1948
- This form duly filled in must reach the concerned Branch Office within 10 days of appointment of an Employee. Delay attracts penal action under Section 85 of the Act, against employer.
- As an insured person you and your dependent family members are entitled to full medical card. The other benefits in cash include (1) sickness benefit (2) Temporary Disablement benefit (3) Permanent disablement Benefit (4) Dependents benefit and (5) Maternity benefit (In case of women employees) subject to fulfilments of contributory conditions
- For more details please visit website of ESIC at www.esic.org or contact Regional office or Branch Office.

1. Date of allotment of Insurance No. _____

2. Date of issue of TIC: _____

3. Name/No. of Dispensary : _____

4. Whether reciprocal Medical arrangements involved?
If yes please indicate _____

Signature of the Branch Manager

Family Particulars of Insured Person

S. No	Name	Date of Birth/Age	Relationship with the employee	Whether residing with him/her Yes / No	If No, State place of residing
1					

2					
3					

Form 'F' [Gratuity Form]
[See sub-rule (1) of rule 6]

Nomination

To **Aegis Customer Support Services Private Limited**

(Give here name or description of the establishment with full address)

1. Shri/Smt./Kumari...MIRZA.AHAD.BEGH.....whose particulars are given in the statement below,
(Name of employee)

hereby nominate the person(s) mentioned below to receive the gratuity payable after my death as also the gratuity standing to my credit in the event of my death before that amount has become payable, or having become payable has not been paid and direct that the said amount of gratuity shall be paid in proportion indicated against the name(s) of the nominee(s).

2. I hereby certify that the person(s) mentioned is a/are member(s) of my family within the meaning of clause (h) of section (2) of the Payment of Gratuity Act, 1972.

3. I hereby declare that I have no family within the meaning of clause (h) of section (2) of the said Act.

4. (a) My father/mother/parents is/are not dependent on me.

(b) My husband's father/mother/parents is/are not dependent on my husband.

5. I have excluded my husband from my family by a notice dated the to the Controlling Authority in terms of the provision to clause (h) of section 2 of the said Act.

6. Nomination made herein invalidates my previous nomination.

Nominee(s)

Sr. No.	Name in full with full address of nominee(s)	Relationship with the employee	Age of nominee	Proportion by which the gratuity will be shared
1.	MIRZA AZIB BEG	BROTHER	25	100%
2.				

Statement

1.	Name of employee	MIRZA AHAD BEGH
2.	Sex	MALE
3.	Religion	ISLAM
4.	Whether unmarried/married/ widow/ widower	UNMARRIED
5.	Department/Branch/Section where employed	
6.	Post held with Ticket or Serial No., if any	CSE
7.	Date of appointment	

8.	Permanent address	ANWAR NAGAR COLONY,RATAPUR RAEBARELI (U.P) Pin code : 229001

Place :RAEBARELI.....

Date :

Signature / Thumb impression of the employee: *Mirza Ahad*

Declaration by witnesses

Nomination signed / thumb impressed before me

Sr. No.	Name in full and full address of witnesses	Signature of witnesses
1.		
2.		

Place :

Date :

Certificate by the employer

Certified that the particulars of the above nomination have been verified and recorded in this establishment.

Employer's Reference No., if any

Date :

Signature of the employer / officer authorized:

Designation :

Name and address of the establishment or rubber stamp thereof. :

Acknowledgement by the employee

Received the duplicate copy of nomination in Form 'F' filed by me and duly certified by the employer.

Date :

Signature of the employee: *Mirza Ahad*

Group Personal Accident Insurance Nomination Form

Dear Sir,

I, ...MIRZA.AHAD.BEGH..... an employee of Aegis Customer Support Services Private Limited., hereby nominate the person (s) mentioned below to receive the amount secured by Personal Accident Insurance Policy (Group) and direct that the said amount shall be paid to my nominee (s), as the case may be as per my directions given herein. I agree that payment of the amount secured by the said policy to the nominee (s) in accordance with my directions contained in this letter of nomination, shall constitute a full discharge to Aegis Customer Support Services Private Limited of its liability in respect of the amount secured by the said policy and it shall be binding on me and my heir(s) and representative (s). The nomination shall be in force until revoked by me in writing or varied by subsequent nominations and communicated to you.

Sr. No.	Name and full address of nominee	Relationship with nominee	Proportion in which amount is to be shared
1.	MIRZA AZIB BEG	BROTHER	100%
2.			

I give the below mentioned particulars about myself:

Full Name	MIRZA AHAD BEGH
Religion	ISLAM
Date of birth	31.01.1996
Gender	MALE
Marital status	UNMARRIED
Father's name	MIRZA AYUB BEGH
Husband's name (for married women only)	
Permanent address	ANWAR NAGAR COLONY,RATAPUR RAEBARELI (U.P) Pin :- 229001

Signature: Mirza Ahad

Date:

Acknowledgement Form for Aegis Call Monitoring, Recording & Archiving

In an effort to ensure the quality and consistency of service provided to our clients and their Customers, Aegis Customer Support Services Pvt. Ltd., its clients and its affiliates may from time to time engage in random and/or selected call monitoring, call recording, and/or call archiving of associate phone calls made from Aegis workstations.

The goal of this monitoring and recording activity is of course service-based. To achieve a high level of service quality for our organization and for the clients that we serve, we must have the ability to survey and sample existing calls and conversations and review them against established standards and procedures. In so doing, this allows us the opportunity to document our service levels to our Clients, identify areas needing organizational focus and identify associate who need further training and development in specific areas.

As a typical part of any monitoring, recording, or archiving activity, no advance notice will be provided, thereby ensuring the increased effectiveness of this quality initiative. The results of these efforts, however, will be reviewed on a regular basis with each associate involved and will become a part of the associate's performance and developmental record. As personal phone calls are not permitted from company workstations, Aegis Customer Support Services Pvt. Ltd. Associate assume at their own risk any personal phone calls that may be inadvertently monitored and/or recorded as a result of unauthorized call activity.

As a condition of association with our organization we ask that all associate read and review our policy on monitoring, recording, and archiving associate's calls and that they acknowledge their review and understanding of this policy through their signature below. Should any associate questions regarding this policy or about Aegis's monitoring or recording practices, they should immediately bring these questions to a Leadership Team member or a member of the Human resources Department.

I have read and I understand the above policy on call monitoring, recording, and archiving and all other HR policies applicable to me, I agree to work with my Leadership Team to ensure the highest level of service and quality possible through all my call activities and efforts.

____MIRZA AHAD BEGH____

Mirza Ahad

Employee Name

Signature

Date

Human Resources Representative (Signature)

Date

Confidentiality Agreement

I, MIRZA AHAD BEGH (Name of the employee) _____(Designation) understand that in the course of my employment and performing duties as an employee of Aegis Customer Support Services Private Limited. (Employer) or on behalf of their clients. I may receive and have access to information of a confidential nature, including information and/ or materials disseminated in training programs conducted by my employer or their clients. I acknowledge the necessity of maintaining the strictest confidence with regard to any such information and/ or materials and agree that all such information shall be received and treated by me as confidential and used only for the purpose set forth above, and not disclosed by me to any third-party without the prior express written consent of Employer.

Further, I agree I will not make any copies, facsimiles, record, or the like, of any of the information or materials disclosed by my Employer or their clients. I expressly acknowledge and agree that I will immediately return to my Employer or their Clients any and all information or materials to my Employer upon the earliest to occur of: (a) the request of my Employer; and/ or (b) upon the termination of my employment with my Employer.

This Agreement shall remain in effect at all times I am an employee of my Employer and all times thereafter.

Mirza Ahad

Employee's Signature: Employee's name: MIRZA AHAD BEGH Date

UNDERTAKING

I hereby undertake that I will adhere to the Company Policy of not using mobile Phone on the production floor.

In case, I am found using the mobile phone on the production floor Company has all the right to take disciplinary action against myself in line with the Company Policy.

Employee Name:MIRZA AHAD BEGH.....

SAP Code :

Temp Id :

Date :

Mirza Ahad
Employee Signature

Employee Declaration (PAN Number)

I hereby confirm that the PAN No./Receipt Number for PAN Application/Acknowledgment Number, as mentioned below, provided by me is correct to the best of my knowledge. Any changes in the details furnished will be intimated to you immediately.

I, also confirm that I will submit a copy of my PAN Card with Human Resource Department, within 20 Days of my Date of joining.

PAN Card No. / CSPPB3052G

Receipt Number/

Acknowledgment No. :

Employee Name :MIRZA AHAD BEGH.....

SAP Code :

Temp ID :

Date of Joining :

Mirza Ahad
(Employee Signature)

Place: RAEBARELI

Date:

Aegis Ethics Agreement

The Customer promise

As the voice of Aegis, I promise to conduct myself with integrity at all times, provide excellence in service, and ensure a world-class customer experience on every call or interaction. In addition, I must abide by the rules of conduct specific to customer interactions.

By signing below I agree to the following terms and conditions:

1. I will comply with directives regarding the Zero Tolerance Policy.
2. I understand that I am to only access an account when there is a valid business reason. I will uphold Aegis's standards of quality and compliance.
3. I have received Zero Tolerance Policy training and fully understand the guidelines and will comply with its expectations.
4. I fully understand that any transgression I am found guilty under the ZTP may lead to a termination of my services if found guilty.

If I do not share Aegis's commitment to ethical behavior, or if at any time I find I am having difficulty complying or cannot, or do not wish to comply with the terms of this Agreement, I will consult with my Manager or a Human Resource representative prior to taking any action which might violate the terms of this Agreement.

Hereby agreed to by:

Employee Name: MIRZA AHAD BEGH

Supervisor Name:

Mirza Ahad

Employee Signature:

Supervisor Signature:

Date:

Location:

Behaviors that lead to Termination under ZIP:

- ▶ Call Disconnection/Forceful Closure – Customer Avoidance.
- ▶ toggling between Auto – in and modes very frequently to avoid taking calls work avoidance.
- ▶ Abusing/using profanity on the call.
- ▶ Rude/Impolite/unprofessional languages/shouting on call.
- ▶ Intentionally not understanding the customer's query.
- ▶ Call Avoidance – Putting a customer on hold for such a long time (more than 2 mins without coming back) that the customer has to disconnect the call.
- ▶ Logging in into Auto in w/o being present – To increase log in hours.
- ▶ Threatening a colleague or supervisor or an officer of the company.
- ▶ Not escalating the call to a supervisor when requested.
- ▶ Taking steps with the intention to violate the integrity of a business metric.
This includes the following but is not limited to:
 1. Avoiding documentation
 2. Wrong/Incorrect Documentation
 3. Using Family and Friends to influence a metric
 4. Incorrect Waivers

Reporting ZTP:

The Zero Tolerance Violation report will be published at 2 levels:

1. Weekly report to Sr. Leadership at Aegis and President to highlight the compliance to the policy.
2. All Zero Tolerance Violations must be reported to the respective HOPE team immediately The same will be added to the tracker and published to operations team for appropriate actions.

Mirza Akhad
Employee Signature:

Date:

Acknowledgement Form

I Hereby confirm that I have been communicated and explained all the below mentioned policies/processes/guidelines in detail.

I have understood the same and agree to abide by them.

Sr. No.	Name of Policy/Guideline
1.	Code of Conduct
2.	Working Hours Policy
3.	Leave and Holiday Policy
4.	Login Hours Adherence Guidelines & Salary deduction Methodology in case of shortfall
5.	Internal Job Posting
6.	Corrective Action Plan
7.	Full Timer – part Timer Conversion Policy
8.	Open door Policy/Grievance Handling Process
9.	Prevention of Gender Harassment Policy
10.	Whistle Blower Policy
11.	Policy on Health, Safety & Environment
12.	Group personal Accident Insurance Policy
13.	Probation & Confirmation
14.	Agent Career Path
15.	Salary Disbursement
16.	Policy on Equal Employment Opportunity
17.	Policy on Prohibition of child Labor
18.	Policy on Human Rights
19.	Separation Process

I shall myself updated with any changes that may take place by reading updates in the notice board/Communication mails

Mirza Ahad

Signature of Employee

Name of Employee MIRZA AHAD BEGH:

Employee No. :

Date :

1. Objective

To ensure authorized access of mobile phone devices on operational floor.

2. Scope

This policy shall cover all users who have access to Operation floor area.

3. Mobile Phone Policy Guidelines

- a) Only Employees provides with a unique identification mark on their ID cards shall be allowed to carry mobile phones in to the policy, provided the phone is a non – camera phone or camera is cover/closed properly and will be referred to as Authorized users as approved by business heads.
- b) All other employees shall place their call phones in dedicated lockers before entry into the production floor.
- c) Voicemail and Emails on phones should be protected with password.
- d) All exception to be approved by center Head, Physical security Head and information security.
- e) Authorized users shall abstained from using these devices for information gathering, communicating or storage purposes.

4. Enforcement

This is the responsibility of each supervisor/TL/Manager to communicate this policy to their respective teams and ensure everyone adhere to this policy.

There will be random audits on the floors be admin for all employees at all levels (authorized and unauthorized) and if found not adhering to the guidelines, the phone will be confiscated and handover to site HR and penalties will be applicable as per table indicated below:

Employee Type	First Violation	Second Violation	Third Violation
Un-Authorized users	Warning Letter	One day salary Deduct & Final warning Letter	Termination of Services
Authorized Users (Camera not Cover)	Warning Letter	One day salary Deduct & Final warning Letter	Termination of Services

Remote Work Policy

1. Objective

The purpose of this policy is to set guidelines for employees while working from home.

2. Scope

This policy applies to employees who are permitted to work in a home office. The consideration for remote work requires a written recommendation from the direct supervisor and shall be finalized by the Head of Department and HR.

3. Policy Guidelines

- **Compliance with Policies and Procedures:** Employees remain obligated to comply with all company rules, practices and instructions as outlined in the HR Policy manual.
- **Workspace Expectations**
 - ✓ Remote work shall only be performed from the employee's primary residence and
 - ✓ employees are required to:
 - ✓ Designate a workspace that is quiet and distraction free.
 - ✓ Workspace that is dedicated for placement and installation of equipment to be used while teleworking.
 - ✓ Maintain this workspace in a safe condition, free from hazards and other dangers to the employee and equipment.
 - ✓ The company shall not be responsible for costs associated with the setup of the employee's home office, such as remodeling, furniture or lighting, nor for repairs or modifications to the home office space.
 - ✓ Employee is expected to submit three photos of the home workspace to management prior to implementation wherever feasible.
- **Schedule:** A general schedule must be communicated to the employee and agreed to by the direct supervisor. Deviations from that schedule if any, should be immediately communicated to the supervisor.
- **Attendance:** The employee must adhere to attendance and break schedules as agreed upon with their manager and in compliance with the company policy.
- **Performance objectives:** The Supervisor is encouraged to submit a formal work plan for the employee working remotely. The plan will identify and outline areas of responsibilities, daily tasks and measurable long term objectives and short terms goals. For agent staff, the performance reports must be published on a daily basis.
- **Availability and Communication:** Employees undertaking remote work must be logged into the company's communication platform each day to ensure that they are accessible and can easily participate with their team members. Employees must be available by phone, email, Microsoft Teams or any other login id (if client specified) during scheduled shift hours including web cam viewing (if mandated only) and also be present for staff meetings, if required. Any exceptions shall require prior permission from the direct supervisor.
- **Role of Supervisor:** The Supervisor shall ensure that the employee is working in accordance with the Remote Work Policy, review and sign-off on records of hours worked (timesheets) as and when required, monitor and review the Remote Work Policy agreement on a regular basis and schedule communication meetings including methods of disseminating information to employees who are working from home.

- Company materials taken home, if any, should be kept in the designated work area at home and not be made accessible to others.
- The company reserves the right to make on-site visits to the remote work location (only if need be) for purposes of determining that the site complies with the rules set forth herein and to maintain, or retrieve company-owned equipment, software, data or supplies.
- Employee may use only the computer accounts and workspace authorized by the company. Use of another person's account, identity, security devices/tokens, or presentation of false or misleading information or credentials, or unauthorized use of information systems/services is prohibited.
- Employees are responsible for all use of information systems conducted under their user ID(s) and are expected to take all precautions including password security and file protection measures to prevent use of their accounts and files by unauthorized persons/entities. Sharing of passwords or other access tokens with others is prohibited.
- To protect access to information systems against unauthorized or improper use, and to protect authorized users from the effects of unauthorized or improper usage, the company has the right with or without notice, to monitor, record, limit or restrict any user account, access and/or usage of account. The company may also monitor, record, inspect, copy, remove or otherwise alter any data, file, or system resources in its sole discretion. The company further has the right to periodically inspect systems and take any other actions necessary to protect its information systems including monitoring employee keystrokes. The company also has access rights to all files and electronic mail on its terminal systems. Anyone using these systems expressly consents to such oversight.
- Equipment supplied by the employee, if deemed appropriate by the organization, will be maintained by the employee. However the company accepts no responsibility for damage or repairs to employee-owned equipment.
- The company reserves the right to reject from the network or block electronic communications and content deemed not to be in compliance with this or other policies governing use of company's information systems.

- **Equipment to be provided by Employee**

- Computer System (if not provided for by the company)
- Internet Bandwidth
- Web Camera (not a mandatory requirement unless specified)
- USB or 3.5mm Headset with Microphone

- **Employer Provided Equipment and Maintenance / Usage Expectations**

- Employees will be provided equipment that is essential to their job duties and the list of such equipment shall be notified.

- **Equipment provided by the company is company property and employees must keep it safe and avoid any misuse by adhering to the below guidelines:**

- Keep equipment password protected.
- Store equipment in a safe and clean space when not in use.
- Follow all data encryption, protection standards and settings.
- Refrain from downloading suspicious, unauthorized or illegal software.
- Make sure to always lock the system when taking a break.
- Comply with the terms of computer software license and copyright agreements, computer virus and protection requirements and procedures.

- **Right to seize/inspect company-owned Computing Devices:** The company reserves the right at any time, with or without prior notice or permission from the user or users of a computer or other company-owned computing device, to seize such device and/or copy, any and all information from the data storage mechanisms of such device as may be required in the sole discretion of the company in connection with investigations of possible wrongdoing or legal action. In addition to the foregoing, privately owned devices connected to the company network are also subject to inspection by authorized company personnel.

- **Home Safety:** It is expected that the employee's workspace at home must meet the following standards:

- Temperature, ventilation, lighting, and noise levels are adequate for maintaining a home office.
- Electrical equipment is free of recognized hazards that would cause physical harm (frayed, exposed, or loose wires; loose fixtures, bare conductors, etc.).

- Electrical system allows for grounding of electrical equipment (three-prong receptacles).
 - The home workspace (including doorways) is free of obstructions to permit visibility and movement.
 - Phones lines, electrical cords, and surge protectors are secured under a desk or alongside a baseboard.
 - The home workspace should be free of combustibles, floors are in good repair, and carpets are well secured.
4. Employees who leave the company are obligated to return any confidential files and equipment back to the company. The equipment shall be in the same condition as at the time of issuance. The I.T. team shall inspect the equipment and recovery, if any for repairmen, shall be charged to the employee at the time of clearance and full and final settlement.

5. Consequences of Policy Violation

Any unauthorized, inappropriate, illegal or other use of company's information systems or failure to comply with this policy shall subject the violator to disciplinary action by the company, including, but not limited to, termination of employment and criminal prosecution.

6. The company reserves the right to revise all or any portion of this policy at any time and from time to time in its sole discretion, subject to applicable laws, rules and regulations.
7. Any deviation in the policy shall need approval of the Global CPO.

I have read and been informed about the content, requirements, and expectations of the Remote Work Policy. I have received a copy of the policy and agree to abide the policy guidelines as a condition of my employment.

Employee Name MIRZA AHAD BEGH

Employee Signature Mirza Ahad

Date _____

CONFLICT OF INTEREST DISCLOSURE FORM

Employee Name	MIRZA AHAD BEGH	Employee Code	
Designation/Department	CSE	Band/Location	RAEBARELI
Statement/Question	Y/N	Description (As Applicable)	

SECTION 1: RELATIONSHIPS		
1. Have you initiated or participated directly or indirectly in decisions that provided a direct benefit (e.g., hiring, merit increase, work assignments, Performance appraisals, etc.) to persons related to you by blood, marriage, or civil union, or members of the same household, including domestic partners or persons with whom you have a personal relationship? If yes, please give a description of the nature of Relationship and the consequent Conflict of Interest, whether Actual, Potential, Specific or perceived.		
2. Do you have any direct or indirect, family relationship with the Directors of Aegis Customer Support Services Private Limited or any other Group Company.		
SECTION 2: CONSULTING OUTSIDE EMPLOYEMENT AND EXTERNAL ACTIVITIES		
2. Have you worked as an employee, independent contractor, or consultant (Paid or unpaid) for any organization other than the Company (You are not required to disclose work that is not connected to and does not interfere with your responsibilities at the company and takes place after normal working hours). If yes, then please list all the activities below and nature of your relationship to your at the company and tenure.		
3. Have you either directly or indirectly, engaged in any business or activity which is competitive with the business of the Company either as owner, partner, agent, representative or as an employee of any person, firm, corporation or other entity? If yes, then please list all the activities below and nature of work and relationship to your work at the company and tenure.		
4. Do you have a management or other fiduciary role in any organization other than the Company? This includes but is not limited to service as an officer, board of director, or supervisor or manager at an organization other than the Company. It also includes any type of scientific, technical, advisory, or other board appointment for Which you might or might not have received remuneration or reimbursement for related travel or other expenses? If yes, then please list all the activities below and nature of your relationship with that entity i.e. name of the organization and your position, nature of work and relationship to your work at the company and tenure.		
5. In light of the Company's Conflict of Interest Policy and your responses above, do you perceive any risk of conflict of interest or commitment, in performing your Company's job duties? If yes, please describe the nature of the relationship, including a description of the real or potential conflict of interest or commitment.		
SECTION 3: PURCHASING AND CONTRACTS		
6. Have you made any decision or do you have the authority to make a decision as an employee of the Company with respect to any organization in which you (or persons related by blood, marriage or civil union, members of the same household, including domestic partners or persons with whom you have a personal relationship) have greater than one percent (1%) of such organization's stock or ownership interest? If yes, then please provide a brief analysis and description below of the real or potential conflict of interest or commitment with regards to company, nature of work & relationship and percentage of ownership.		
7. Have you made any decision or do you have the authority to make a decision as an employee of the Company with respect to any organization with which you or persons		

related by blood, marriage, or civil union, or members of the same household, including domestic partners or persons with whom you have a personal relationship, have current or pending employment, consulting, management, fiduciary or similar affiliation? If yes, then please provide a brief analysis and description below of the real or potential conflict of interest or commitment with regards to company, nature of work & relationship and amount and percentage of ownership.		
8. Have you made any decision or do you have the authority to make a decision as an employee of the Company with respect to any organization from which you have solicited or accepted gifts, gratuities, favors, or anything of monetary value, including and not limited to current or potential vendors or contractors or their agents? Exceptions include ordinary business courtesies, such as payment for a meal or event, or acceptance of gifts that are promotional items without significant value and that are distributed routinely. If yes, then please provide a brief analysis and description below of the real or potential conflict of interest or commitment with regards to company, nature of work & relationship and the value of the gifts/ favours received.		
SECTION4: GIFTS SOLICITATION AND USE OF COMPANY RESOURCES		
9. Have you solicited gifts from vendors, contractors, local businesses, Company departments, or others with whom there is a potential or on-going professional relationship? If yes, then please provide a brief description of the real or potential conflict of interest or commitment.		
10. Have you engaged in fundraising events with co- workers on behalf of charitable organizations? Exceptions are passive fundraising events and Company sponsored activities. If yes, then please provide a brief analysis and description of the real or potential conflict of interest or commitment.		
11. Have you accepted gifts or perquisites from local businesses, vendors, contractors, or others with whom there is a potential or on-going business or professional relationship, Including travel expenses, meals hotel accommodations, or their reimbursement, etc.? Exceptions include ordinary business courtesies, such as payment for a meal or event, or gifts which are promotional items without significant value and which are distributed routinely. If yes, then please provide a brief description of the real/ potential conflict of interest or commitment.		
12. Have you used your office, staff (including their own time), specialized office equipment, office supplies, personal computers, and/or telephone for non-Company related activities? While there may be occasional instance when business related correspondence or the like is received at the Company office, employees should not routinely use office facilities (either during or after normal business hours) for the conduct of outside business. Exceptions include: personal use of telephone for local calls (e-mails etc.) that are incidental and kept to a minimum as per Company's policy. If yes, then please provide a brief analysis and description of the real or potential conflict of interest or commitment		
SECTION 5: SIGNATURE AND MANAGEMENT REVIEW		
By signing this form you a) Certify that you have read the Company's Conflict of Interest policy; b) Certify that the information contained in this Disclosure Statement is complete and accurate to the best of your knowledge; c) Acknowledge your continuing obligation to complete and submit a new Conflict of Interest Policy- Disclosure Statement when there is any actual or anticipated significant change in your outside activities or related financial interests.		

SIGNATURE: Mirza Ahad

Date



Violation of this policy, including failure to complete this form considered a serious matter and may result in disciplinary action up to and including employment termination without compensation/ settlement.

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

I have reviewed this disclosure form and determined that:

.....The individual had no material conflict of interest or commitment with regard to his/her responsibilities.

.....The individual had a material conflict and the following descriptions is how he/she will eliminate the conflict.

Suggestion:

Supervisor' Name:

Supervisor's signature:

Date:

INFORMATION SECURITY AWARENESS DECLARATION

Information security (sometimes shortened to InfoSec) is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic or physical). For us here at Startek, that means protecting our customers data with strong security measures, and being aware of our responsibilities, regardless of your role.

General Computer Controls (Strong/Weak Controls)

Controls are the measures we put in place to minimize our exposure to information security risks. The types of controls you can implement in your client area might be:

- A strong password
- Keeping a workstation free of written documentation, customer records or data
- Ensuring your access to client data is only accessible by you. No sharing of passwords!
- Disposing of confidential records
- Storing information securely. Following ID and verification processes on every call or email where required.

Security Knowledge

Internet access is an integral component of our business here at Startek. However, such access does introduce the possibility of malicious attacks on our data and networks from anywhere on the planet.

To safeguard from such threats, Startek staff are required to have **adequate security awareness to ensure they understand the potential risks to the company** and its customers, and that poor security knowledge and practice can result in:

- Identity theft
- Monetary theft
- Legal ramifications (for yourself, Startek or its clients)
- Termination if company policies are not followed

Confidential information

Confidential information is any information considered to be private and sensitive. Some examples you might encounter in your client area are:

- Protected personal information about a client or customer
- Banking information
- Credit card information
- Financial records
- Passwords, PIN numbers, or other security codes
- Internal communications between Startek and a customer
- Various customer records related to their business dealings with us

Confidential information can be stored in many forms. It can be information printed on paper; data files stored on a computer or a hand-held device such as a laptop or smartphone; or recorded spoken words such as in a voice mail.

“Regardless of the form it takes, you are responsible to protect it from unauthorized disclosure or modification.”

How to Protect Confidential Information

- Use only approved procedures when handling confidential information, especially when using the internet, email, or even voice communications.
- Your supervisor or the IT department can provide specific guidance on how to properly handle confidential information.
- If you are unsure of any procedures, ask your manager to guide you or see our policies on **SAFI**

User Ids

- Your user ID uniquely identifies you. You are responsible for all actions associated with your user ID; therefore, it is important to ensure that your user ID is used only by you and no one else.
- You will be held responsible for the actions of another individual if you allow them to obtain and use your user ID and password, or allow them access to any information in a client application while you are logged in with your ID.

Password Protection

Protecting your password is a critical factor in protecting confidential information; therefore passwords should be:

- Memorized and never written down in such a way that others can see or use them
- Kept a secret from others
- Be aware of scams to trick you into disclosing your password through anonymous phone or email
- Under no circumstances should anyone ever ask you for your password, or should you voluntarily give it out if asked
- Likewise, you must not attempt to learn another person's password and/or access another person's account using their password.
- Care should be taken when selecting a password. A poorly chosen password compromises security.
Create a "strong" password by following these simple rules:
 - It must be at least eight characters in length, and in some areas of the business it must be at least ten characters in length (*Tip: The longer your password is, the harder it is to break*)
 - Use at least one upper case and one lower case letter
 - Use at least one number
 - Use at least one special character such as *? # @ & \$
 - Avoid using common words that can be easily guessed
 - Avoid using personal information such as your child's name, favorite sports team or pets.
 - Our systems at Startek will require you to change your login in password regularly to ensure we maintain information security.

Your Computer Workstation

- It is your responsibility to **log off or lock your computer** workstation whenever **leaving it unattended**, so that any confidential information on screen **cannot be seen by others**.
- It is recommended to log off your workstation when you are leaving your work area at the end of your shift.
- Leaving a workstation logged on and unattended could **lead to an unauthorized access of confidential information**.

Personal Usage

- Startek computer systems are intended to be used for **business purposes only**.
- Limited personal may be permissible with **approval by your supervisor** and is on **your own personal time**.
- Startek provides a limited number of computers that can be used for personal internet browsing outside of your work area i.e. in the breakout areas on each floor.

EMAIL

- Organizational email is limited to authorized users and is for conducting official Startek communications. Personal use of company email is not allowed.
- You are responsible for all activity on your assigned email account. **Don't share your password with anyone.**
- Keep communications with Startek customers formal and friendly.

INTERNET

- Internet access is provided to Startek staff based on **legitimate business needs**.
- All internet access from all company workstations is logged and monitored by IT.
- Restrictions to access to non-work related, objectionable or malicious sites is enforced by IT.
- **The ability to connect with a specific website does not in itself imply that access is allowed.** If you discover that you have inadvertently connected to an inappropriate website please disconnect from that site and notify the IT Service Desk.

Inappropriate Activity

- Under no circumstances should organization-owned systems be used for gambling, personal profit, or to download, distribute materials, comments, pictures, or other forms of communication of a sexual nature or which are otherwise obscene, intimidating, offensive, or create a hostile work environment.
- **The violation of above mentioned rules may lead to disciplinary action not only including termination, but also subject to applicable laws involving civil and/or criminal penalties for violations with regard to inappropriate access or disclosure of private or confidential data or information.**

Social Engineering

- Social engineering is the practice of obtaining confidential information by manipulation of legitimate practices. A social engineer will commonly use the telephone or internet to trick people into revealing sensitive information or getting them to do something that is against typical policies.
- Social engineers exploit the natural tendency of a person to trust another's word, rather than exploiting Computer security holes.
- Social engineers might attempt to:
 - ✓ Try to persuade you to **disclose personal information** about someone they have no right to i.e. they may claim to be related to, the spouse of or have some other emergency reason for obtaining the data.
 - ✓ Pose as members of an organization that claims rights to data
 - ✓ Offer bribes or coerce

Avoid Being a Social Engineer Victim

- If an unknown individual claims to be from a legitimate organization, **try to verify his or her identity directly with the company before beginning dealings with them.**
- Do not provide personal information or information about your client area unless you are **certain of a person's authority to have the information.** If in doubt, **escalate the call to your supervisor.**
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a link or web site connected to the request.

Phishing

- Phishing is a form of social engineering. Phishing attacks use email or malicious websites to obtain personal information by posing as a trustworthy organization.
- For example, a caller may seemingly be from a reputable credit card company or financial institution that requests account information on one of your customers, often suggesting that there is a problem or it is an emergency. They may even advise the customer has already authorized them.
- Always follow your ID checks as required by your business on every call.

How Can I Safeguard Against Phishing?

- Don't reply to email or pop-up messages that ask for personal, financial or organizational information on our systems here at Startek.
- Look out for a sender's email address that is similar to, but not the same as, a company's official email address.
- **Don't share your Startek / Client email address with an organization you can't verify.**
- Fraudsters often send thousands of phishing emails at one time. They may have your email address, but they occasionally have your name. Be doubtful of an email sent with a generic greeting such as "Dear Customer" or "Dear Member".
- Never submit confidential information via forms embedded within email messages.
- Don't click on links in email or instant messaging, and never use links in an email to connect to an external web site unless you are **sure the address is safe.**

IT SECURITY DO's & DON'Ts DO's:

- ✓ Store all data and files on a network shared drive so that it can be backed up if necessary, and cannot be lost if your computer breaks or is stolen
- ✓ Password should be changed at least **once in every 45 days**
- ✓ Be extra careful when required to enter your password on a stranger's computer
- ✓ **Lock your computer while you are not working** (by pressing ALT+CTRL+DEL)
- ✓ Be cautious when opening attachments from strangers
- ✓ **Maintain a clear desktop / Follow all processes to ensure compliance** with PCI where relevant
- ✓ Deposit unwanted papers containing personal/customer information into shredding or recycling bins provided
- ✓ Be cautious while discussing, receiving or forwarding proprietary information
- ✓ Printing, photo copying or faxing is used and limited for legitimate business needs only
- ✓ Internet should be used for **business purposes only** i.e. responding to inbound customer emails for your client area
- ✓ At the end of your shift, ensure any papers or documents are disposed of or stored securely.
- ✓ Sensitive or classified information, when printed, should be cleared from printers and/or fax machines immediately
- ✓ Leave devices capable of recording or capturing customer data away from the operations floor.

DON'Ts :

- ✓ Never share your passwords with anyone
- ✓ Never leave your computer unlocked when you are away from your desk
- ✓ Do not keep computers online when not in use (Lock it while going on breaks & Logoff when the shift ends)
- ✓ Never send personal information about yourself or a customer (including names, account numbers, addresses, phone numbers or passwords) to strangers
- ✓ Do not write your password down anywhere
- ✓ Do not share your access with anyone
- ✓ Do not save your password on your system
- ✓ Do not gossip or share with others, sensitive information that you have access to
- ✓ Do not throw confidential reports in to the rubbish bin without shredding them

- ✓ Do not save files on the local desktop or hard drive of your computer
- ✓ Do not install unauthorized software or attach unauthorized hardware devices
- ✓ Do not access or download content not required or related to Startek
- ✓ Call center staff are not to carry any mobile phones on the Operations floor
- ✓ Use of any portable storage device or media (e.g. USB sticks CD/DVD ROMs, compact cameras) is prohibited in production area.
- ✓ Do not send any chain emails or jokes, and do not subscribe to any non-work related (e.g. humor, pornography, news) mailing lists
- ✓ Do not send greetings to large distribution lists. Attaching multimedia files with greetings is prohibited
- ✓ Do not upload Startek data to the internet (including sending such documents by email without the prior approval of your manager)
- ✓ No attachments can be viewed or downloaded from the personal email sites
- ✓ Do not send credit card, ATM or electronic funds transfer information over the internet
- ✓ Playing songs, video, software, games or viewing images, files not meant for official purpose are prohibited. Also running any non-standard and unapproved software even for official purposes is prohibited.
- ✓ Do not enter company facilities without ID cards displayed at all times, or refuse to show them to security personnel whenever asked
- ✓ Photographic equipment is prohibited in Startek premises (without prior approval)
- ✓ All personnel are guided not to repair, change or relocate their computer by themselves. The IT Service Desk must be consulted for any assistance.

Reporting Security Incidents

Notify IT and your supervisor if you become aware of or suspect the following:

- ✓ Theft of or damage to IT equipment
- ✓ Unauthorized use of a user's password
- ✓ Policy violations
- ✓ Usage of gadgets, mobile phones and/or cameras, USB hard drives or other media storage devices in the production environment
- ✓ Any other problems or questions with information security or privacy.

You can also call the IT Service desk on (03) 9256 5034 or send an email to servicedesk@au.aegisglobal.com or information.security@aegisglobal.com to register any security concern or incident.

**The internet security policy can be found on Safi!
HELP -> Human Resource -> HR policies**

Employee Declaration

Name : MIRZA AHAD BEGH

Emp. Code : _____

Department : CSE

I understand that as an employee of Startek Services Australia, my actions and behavior are governed by range of legislation and policies as amended from time to time

I hereby confirm that I have read and understood my rights and responsibilities related to Startek' policies on Information Security. I am aware that breaching this policy could result in any one of the following ramifications: informal chat, informal warning, final warning or dismissal.

I am committed to perform my duties and drive a culture of security in our organization at all times. This also extends to any Startek sponsored or employment related situation such as training courses, promotional events, Christmas parties, whether outside working hours or at another site.

Employees Signature: *Mirza Ahad*

Date :

Declaration and Acknowledgement – Work From Home (Equipment owned by the Employee)

I hereby agree and give my consent to use the following in adherence to the remote work policy:

- My own personal space for home office and equipment set up.
- Personally owned devices to connect to company network and services and meet business needs of the organization. These devices may include Computer/ Laptop System, Internet Bandwidth, Web Camera (only if specified), USB or 3.5mm Headset with Microphone or any other device as specified by the organization.
- The type of device, the operating system, firmware and configurations for connectivity to the organization network from the personally owned device shall be approved by IT.
- I shall refrain from uploading any personal data / information through own device on the company network/ server storage.
- Privately owned devices connected to the company network can be subject to inspection by authorized company personnel in connection with investigations of possible wrongdoing or legal action.
- In the event of my separation from the company, connectivity shall be de-activated on the close of my last working day.
- I shall comply with the 'Acceptable Use Policy' outlined and available with IT and the 'Remote Work Policy' in the HR policy manual at all times during my work from home tenure.

By signing below, I understand and agree that, I shall be responsible for ensuring safety and security of my own device, even when not in use. The organization shall not be responsible for technical support or loss due to theft or damage of the personally owned device. Lost or stolen device shall be reported immediately to my supervisor and IT team so that organizational information, if any that resides on the device can be wiped out remotely.

I further understand and agree that nothing herein constitutes a guarantee of ongoing employment and my employment with the Company remains at-will, meaning that it is subject to termination by me or the Company, with or without cause, with or without notice, at any time, unless I have a separate employment agreement with the Company that states otherwise.

Employee's Signature: *Mirza Ahad*

Employee's Name: MIRZA AHAD BEGH

Date:

Code of Conduct

The Company maintains high standards of integrity, ethics and professional conduct for employees as our work brings us into frequent contact with clients, prospective clients, vendors etc. Employees are the Company's representatives to the outside world and their professional conduct reflects the value system of the Company. The code of conduct aims at creating and building employees' core values, determining best-in-class practices and establishing centers of excellence in the Company. It emphasizes the Company's goal of striving to attain the highest ethical standards when resolving potential or actual conflicts of interest.

The following clauses are by no means inclusive of the circumstances an employee may encounter during the course of his/her employment with the Company. An employee who is unsure of how to proceed when faced with a particular situation must discuss the matter with Human Resources prior to taking any action. Management expects all employees to exercise the highest degree of professional business ethics in all actions they undertake on behalf of the Company. All employees are expected to adhere to the code of conduct. Any contravention of the clauses mentioned herein could result to disciplinary action up to and including termination/ dismissal.

This policy should be provided to and followed by the Company's agents, Board of Directors and representatives, including consultants and contract employees. If a law conflicts with a clause in this policy, employees must comply with the law. The company retains the right to revise all or any portion of this policy at any time and from time to time in its sole discretion, subject to applicable laws, rules and regulations.

1. Non-Disclosure

During the tenure of employment, all employees will be acquainted with:

- Information pertaining to the clients (whether now existing or developed during period of employment either by employee or the Company) and business methodology of the Company.
- Confidential and privileged information relating to clients, special client information, development and production methods and techniques, promotional materials technical information and confidential processes (including software tools and software development processes), design ideas, machinery, plans, devices or materials and other similar matters treated by the Company as confidential.

The said information is a valuable, special and unique asset of the Company and was acquired or will be acquired at a considerable expense to the Company and it is also confidential and a trade and business secret. Employees have an ethical duty not to disclose any information gleaned from business transactions and to protect confidential relationships between the Company and its customers / suppliers and shareholders. Business information that has not been made public (e.g., insider information) must not be released to private individuals, organizations or government bodies unless demanded by legal process such as a subpoena or court order. Employees shall not use confidential information obtained in the course of their employment for the purpose of advancing any private interest or for personal gain. The use/ disclosure of such confidential information

/data by persons or entities other than the Company may pose a threat to the business. To protect the confidential information, employees are expected to:

- Classify and label all employee information
- Safeguard confidential and restricted information in secure locations with limited access
- Comply with all record retention guidelines
- Share confidential or restricted information with employees or outside entities only as required to meet Company's business objectives and with prior authorization from the Management.

2. Proprietary Information / Data

Any and all discoveries and/or inventions (which shall include but not be limited to improvements and modifications) relating to work performed by the employees, or relating to matters disclosed to employees in connection with work to be performed, or suggested by such matter, whether or not patentable, discoveries and/or inventions made or conceived by the employee, solely or jointly with others during the term of his/her employment (regardless of whether conceived or developed during working hours) or during a period of one year thereafter, shall be a property of the Company or its nominee and such discoveries and/or inventions shall be promptly disclosed to the Management.

The Company or its nominee will have the right to file and prosecute, at its own expense, all patent applications, whether local or foreign, on said discoveries and/or inventions. The employee shall, during his/her employment, or at any time or times thereafter, provide to the

3. Confidentiality of information

All records and information relating to the organization or its customers / clients are confidential and employees must, therefore, treat all such matters accordingly. No Company or Company-related information, including without limitation, documents (including electronic documents), notes, files, records, computer files or similar materials may be removed from the Company's premises except in the course of performing duties on behalf of the Company and with the permission of the respective Department head / Business HR head. Additionally, the contents of the Company's records or information otherwise obtained in regard to business may not be disclosed to anyone, except where required for a business purpose.

Employees (during the term of employment and

thereafter) must not disclose, furnish, or make accessible, any confidential information, purposefully or inadvertently (through casual conversation), to any unauthorized person inside or outside of the Company.

Privacy and confidentiality of employee information should be maintained. Nothing in this code is designed to interfere with the employee's rights to engage in concerted activity in accordance with the law of the land. On-line access to employee information will be limited to authorized users. Level and type of access will be based on information needed by user to perform work-related duties.

Company or its nominee all documents, information and assistance requested for the filing, prosecution or defense of any legal action or application pertaining to such discoveries and/or inventions and for the assignment or conveyance to Company or its nominee, of all right, title, and interest in and to such discoveries and/or inventions, patent applications and letters issued thereon.

Employees will, in addition to the above, upon request of the Company or the Company's client, to whose work he/she is assigned, execute and deliver such agreements pertaining to discoveries and/or inventions made during the period of his/her employment. Upon termination or expiry of employment with the Company, employees will deliver to the Company all items including, but not limited to, drawings, blueprints, descriptions or other papers or documents that contain any such confidential information. The foregoing provision in this paragraph shall be for the benefit of the Company and/or its clients to whose work the employee is assigned, and either or both shall have the rights and remedies to enforce such provision.

4. Competition and Fair Dealing

We seek to outperform our competition fairly and honestly. Stealing proprietary information, possessing trade secret information that was obtained without owner's consent or inducing such disclosures by past or present employees of other companies is prohibited. Each employee should endeavor to respect the rights of and deal fairly with the Company's customers, suppliers, competitors and employees. No employee should take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other intentional unfair-dealing practice.

5. Non-Solicitation

To protect employees from unnecessary distractions, distribution of literature, or merchandise on Company premises during working hours is prohibited. This includes soliciting employees for membership, subscription to any organization or entity or the circulation of petitions, notices or other printed materials for any public or private enterprise or for gifts of any nature.

6. Conflict of Interest, Accepting/ Giving gifts

All employees must avoid incurring even the appearance of impropriety, either financial or personal, which might affect or appear to affect their judgment in dealing on the Company's behalf with clients, suppliers or individuals. Where there is a possible conflict, the situation should be mentioned in writing to the HR department. Employees shall not use knowingly or unknowingly organization property, funds, position or power for personal or political gain. Employees must not allow any situation or personal interests to interfere with the exercise of their independent judgment or ability to act in the best interests of the Company. A conflict of interest may arise in the following areas:

- Holding a direct or indirect financial interest as owner, officer, stock-holder, partner joint venture, guarantor or director in a firm which provides services or supplies materials or equipment to the Company or which is in competition with the Company or to which the Company makes sales, provides services or makes loans or where the individual engages in direction or operation of such firm.
- Speculating or dealing in equipment supplies, materials or property purchased by the Company or dealing for his/own account in products sold by the Company.
- Borrowing money from suppliers or clients or from individuals or firms with whom the Company does business.
- Acquiring by purchase or lease an interest in real estate in which it is known that the Company has interest or which may improve in value because of Company interest in adjoining property.
- Misusing information to which the employee has access by reason of his/her position, such as disclosing confidential information to competitors or others outside the business, or using such information for personal use (e.g. trading in securities)
- Serving as an employee or consultant to another similar business organization without Company's consent. Permission to provide services to other similar businesses must be authorized by the Management.
- Accepting gifts or favours, being entertained or accepting other personal obligations, which are substantial for him/herself or a family member from clients and/or suppliers, whether local or foreign. Any gift so received, either in cash, stocks, bonds, options or similar items or in kind, should be shared among employees.

Detailed policy is outlined in the 'Conflict of Interest Policy' and employees are expected to adhere to it.

7. Non-disparagement

No employee during the term of employment or after the cessation of employment shall disparage or criticize the Company or its present or past directors, employees, shareholders, advisors, or issue any communication, written or otherwise, that reflects adversely on or encourages any adverse action against the Company or its present or past directors, employees, shareholders and advisors, except if testifying truthfully under oath pursuant to any lawful court order or subpoena or otherwise responding to or providing disclosures required by law. In case, where an ex-employee was dismissed or asked to leave for reasons pertaining to misconduct, indiscipline or non-performance, and if any reference is sought by an external organization or person, the matter would be referred to concerned HR, who will confirm the employment dates and refrain from disparaging or passing any negative comments about the ex-employee.

8. Investments and Insider Trading

Employees are prohibited from investing in any of the organization's clients, suppliers or competitors unless the securities are publicly traded; the investments are on the same terms available to the general public and not based on any inside information and the investment is not significant to the individual's net worth. This prohibition applies to all forms of investments and to all employees, directors, officers and agents of the Company and their immediate families. In general, employees should not have any financial interest in a client, supplier or competitor that could cause divided loyalty or give the appearance of divided loyalty.

Employees who have access to confidential information are not permitted to use or share that information for stock trading purposes or for any other purpose except the conduct of our business. All non-public information about the Company, which the Company maintains as confidential, should be considered confidential information. To use non-public information for personal financial benefit or to "tip" others who might make an investment decision on the basis of this information is not only unethical but also illegal. In order to assist with compliance with laws against insider trading, the Company has adopted a specific policy governing employees' trading in securities of the Company. This policy has been distributed to every employee and questions should be referred to the Company's Chief Financial Officer.

A detailed policy on Insider Trading is available with the Human Resource Department.

9. Anti-Money Laundering (AML)

Any form of money laundering, whether indirect or direct is prohibited to be carried out by employees, agents, subsidiaries, business partners or other intermediaries or third parties associated with the company. The process of money laundering attempts to disguise the true origin of the proceeds of criminal activities so that after a series of transactions, the money, its ownership and the income earned from it appears to be legitimate. The company is committed to preventing, detecting, investigating, monitoring and reporting all forms of money laundering activity.

Employees shall abide by the policies and procedures outlined for customer due diligence, vendor documentation, records and policy prior to a deal and ensure that every vendor is known to us and satisfies the company's AML checks by completing, recording and storing all necessary details. Employees managing the vendors and vendor management shall ensure that proper documentation is made to be compliant with the procedure and process of the company so that every potential purchaser is known to the company and satisfies the due diligence checks including completion of Purchaser Information Form, process of verification and retention of records.

Employees should ensure that while identifying customers, partnerships, trusts, charities and sole traders, identity information should be obtained that is relevant to that entity. This includes the full name of the company, registration number, registered address, country of incorporation, its memorandum or other constitutional documents and any other documents of relevance. Employees handling sales and customer acquisition shall carry out basic functions of know your customer forms that must include matters pertaining to customer name, registration, registered office address, business license, memorandum or constitution copy etc., and shall keep a 'check and confirm' process on customers of particular concern (OFAC listed or Govt black listed), customers resident abroad, how the customer comes to the business, for example non face-to-face customers, occasional transactions, the pattern of behaviour and any changes to it and corporate customers, partnerships, or trusts.

In case employees observe any suspicious activity, those must be reported. Some of the examples of suspicious activity include customer's reluctance to provide details of its identity, providing fake documents, customer's using intermediaries to protect their identity or hide their involvement, use of cash in a quick sale, or cash exchanges directly between the parties including cash deposit etc.

Employees are expected to read, understand and implement the anti-money laundering policy and they shall also be provided with regular training on the same. Any violation of this policy will lead to strict disciplinary action.

10. Engaging in private trade or alternate/ outside employment

All full-time employees, shall not engage directly or indirectly in any trade/business or undertake any other employment or consultancy or undertake such trade/business/consultancy on behalf of anyone else, either with/without remuneration, during the course of his/her employment with the Company, except with the written permission of the management. Also, such private trade and/or alternative employment should not adversely affect performance and conflict with the business interest of the Company (this would include working for a competitor). In cases of conflict with any outside employment activity, the employee's obligations to the Company must be given priority. In general, private trade and/or alternative employment is not allowed when:

- It prevents an employee from fully performing work for which he/ she is employed with the Company.
- It prevents an employee for engaging in overtime assignments (if applicable).
- It involves companies that are doing or seeking to do business with the Company, including actual or potential vendors or customers.
- It violates provisions of law or the Company's policies and procedures.

11. Antitrust and Competition

Employees should ensure that they abide with the antitrust laws which are designed to protect the competitive process and generally prohibit:

- formal or informal agreements with competitors that harm competition or customers, including price fixing and allocations of customers, territories or contracts
- formal or informal agreements that establish or fix the price at which a customer may resell a product
- sharing of certain kinds of information, such as pricing, production and inventory, which should never be exchanged with competitors, regardless of how innocent or casual the exchange may be and regardless of the setting, whether business or social
- abuses of a dominant position, which might need to be applicable if there are any markets in which the company has substantial market power (as evidenced, for example, by a market share of 40% or more). Activities which risk breaching competition law will be subject to strict disciplinary action.

12. Maintenance of Corporate Books and Records; Financial Integrity and Reporting

Employees shall ensure that all transactions and holdings relating to the company, be recorded in proper detail and according to the accounting standards applicable from time to time. Such records shall be available for audit at any time and no such records may be held elsewhere than at company premises and/or on company's systems, and all such records should be accessible to authorised staff at all times. Funds or property belonging to the company should not be hidden or disguised from audit or other scrutiny for any reason whatsoever. Supporting documentation such as invoices or receipts should not be forged or post-dated. The integrity of company records and public disclosure depends on the validity, accuracy and completeness of the information supporting the entries to the books of account. Employees are strictly prohibited from making of false or misleading entries, whether they relate to financial results or test results. It is important that the books, records and accounts accurately and fairly reflect, in reasonable detail, the assets, liabilities, revenues, costs and expenses, as well as all transactions and changes in assets and liabilities.

13. Authorization to sign contracts/ agreements during service of notice period

After submitting resignation and during the service of notice period, an employee is not authorized to sign any agreements/ contracts on behalf of the organization without written consent of his immediate supervisor. Any contract signed by the employee while serving notice period, after resignation without written consent of his immediate supervisor, will not be binding on the organization and employee will be solely responsible for the consequences arising out of the same.

14. Ethical standards

The Management expects all employees to exercise the highest degree of professional business ethics in all actions they undertake on behalf of the Company. Employees should observe all laws and regulations governing business transactions and engage in fair competitive actions. Employees are prohibited from using, directly or indirectly, corporate funds and assets for any unlawful purpose or to accomplish any unlawful goal. The Company also prohibits the establishment or maintenance of undisclosed or unrecorded funds and assets. All reporting of information should be timely and accurate. Employees should not make any false or misleading entries in any book or record. Employees should use Company funds only for legitimate and ethical purposes.

15. Family Relationships

If an employee wishes to do business on behalf of the Company with a member of his or her immediate family, other relative, or with a Company of which a relative is an officer, director or principal, he or she must disclose the relationship and obtain the prior written approval of the CFO and CPO.

16. Inappropriate/ Illegal Behavior

The Company is committed to providing its employees and visitors a safe, healthy and productive work environment. Violent behavior or threat of violent behavior in the workplace or Company premises will not be tolerated. Employees are prohibited from bringing weapons on Company/client premises, including parking lots, leased buildings and recreation areas. Any employee, who threatens violence, by word or deed, shall be asked to leave the Company/ client premises until a review can occur.

Employees must avoid improper acts and the violation of any government law or regulations in the course of performing his/her duties. When in doubt about any law or regulation, the employee should consult the HR department. The following guidelines have to be adhered to:

- No corporate or subsidiary funds, assets or corporate participation in any nature should be used for personal benefits, directly or indirectly.
- No corporate or subsidiary funds or assets will be used for any improper or unlawful purpose such as paying bribes or kickbacks to obtain privileges, concessions or special benefits.
- No employee will accept payment or anything of value whether characterized as a bribe or a kickback, or otherwise; whether intended for Company or personal use, if the payment and/or receipt is illegal or is designed to cause the employee to grant a privilege, benefit or concession to the payer.
- No undisclosed or unrecorded funds or assets of the Company will be established for any purpose.
- No false or artificial entries or documents will be made or entered into the books or records of the Company or its subsidiaries for any reasons, and no employee will participate in an arrangement that results in such a prohibited act.
- No payment on behalf of the Company will be approved or made with the intention, understanding or agreement that any part of such payment is to be used for any purpose other than what is described by the documents supporting the payments.
- No employee will use the Company's resources unless properly authorized.
- Any employee having knowledge on any prohibited act, past or present, should report it to the HR department.

17. Workplace Relationships (Fraternization and Nepotism) & Employment

The purpose of this policy is to provide guidelines for employment of spouses, relatives, and other persons involved in personal relationships with current employees. Employment of spouses, relatives, and persons involved in other personal relationships in the same area of an organization can cause serious conflicts of interest, problems with favoritism, and can affect employee morale. Spouses, relatives, and persons involved in personal relationships with current employees will be considered for employment on the same basis as all other applicants, except under certain conditions as described in this policy. For the purpose of this policy, relatives include, but are not limited to; spouse, common-law spouse; child, stepchild, legal dependent; parent, step-parent, parent-in-law; sister, step-sister, sister-in-law; brother, step-brother, brother-in-law; aunt, uncle, grandparent, grandchild, niece, nephew, cousin. Personal relationships include, but are not limited to, those involved in dating relationships, casual sexual involvement where the parties have no intention of carrying on a long-term relationship, co-habitation, and any other kind of behavior associated with romantic or sexual relationships. Because it may be difficult to disclose all personal relationships, the company reserves the right to determine whether a familial or personal relationship exists between individuals and whether this relationship proves problematic for company in implementing this policy. Hiring and all other employment decisions concerning family members and persons involved in personal relationships are at the discretion of the Human Resources department.

Employment of Spouses

Employees who are married or involved in a common law relationship may continue employment as long as the following situations do not exist:

- One spouse would supervise the other or be in a position to exercise authority to appoint, dismiss, or discipline the other spouse or to influence a term or condition of the spouse's employment.
- One spouse would audit, verify, receive, or be entrusted with money handled by the other spouse.
- One spouse has access to confidential information including but not limited to payroll and personnel records.
- The relationship creates an appearance of an actual or potential conflict of interest.

Employment of Other Relatives or Parties Involved in Personal Relationships Relatives or parties involved in a personal relationship may not be work in a position where one of the following conditions exist:

- One individual would be involved in the processing of the other's work.
- One individual would audit, verify, receive, or be entrusted with money handled by the other person.
- One individual has access to confidential information including, but not limited to, payroll and personnel records.
- One individual would supervise the other or be in a position to exercise authority to appoint, dismiss, or discipline the other individual influence a term or condition of the other individual's employment.
- Either an actual or a potential conflict of interest would be created.
- In other cases where a conflict or the potential for a conflict arises, even if there is no supervisory relation- ship involved, the parties may be separated by reassignment or termination from employment.

The restrictions of romantic relationships apply regardless of the sexual orientation of the employees involved. This applies equally to opposite sex and same sex relationships.

Employment of Human Resources

Members of human resources are prohibited from engaging in personal relationships with any employee throughout the organization.

Fraternization

All employees in a Leadership role or any role where an employee may supervise the other or be in a position to exercise authority to appoint, dismiss, discipline, audit, verify, or access personal information on another employee should use discretion when attending social gatherings outside of the workplace where other Employees may be present, particularly where alcohol is served. Behavior, discussions, and Interaction in such circumstances must not interfere with the integrity of employees, the integrity of the workplace relationships, and must not violate any other company Policy including the Code of Ethics, Confidentiality, or the Harassment Policy.

The resolution procedure for Conflict of Interest is outlined in detail in the Conflict of Interest Policy.

18. Maintaining a positive work attitude & environment/ Floor rules

The Company is committed to providing a positive and learning environment to all employees where all employees are treated fairly, with respect, regardless of their status/designation. Employees also are expected to follow the same principle when dealing with colleagues. No employee should engage in acts of intimidation and harassment. No employee should pass derogatory/insulting remarks about any colleague. No employee should make negative comments about any policy/ system/ process/ methodology of the Company, which will lead to unrest and disturb the work environment. Employees are required to follow the grievance handling procedure to vent their frustrations/ complaints etc.

Employees are expected to adhere to the following guidelines while at their work desks:

- No eatables and drinks shall be carried to the floor/ workstation/ desk apart from a water bottle.
- All employees are expected to maintain neatness and orderliness of their desk and the place of work.
- No confidential documents must be kept lying unattended in the open.
- Employees are expected to maintain personal hygiene.

19. Participation in politics/ Membership of political parties

Employees shall take prior permission for becoming members of any political party. No employee shall participate in any demonstration, which would incite an offence under the law of land.

20. Use of Company's property and equipment

All the employees should endeavor to protect the Company's assets and ensure their efficient use. Theft, carelessness, and waste have a direct impact on the Company's profitability. Any suspected incident or fraud or theft should be immediately reported for investigation. All employees are required to handle the Company's property/equipment with due diligence and care. They shall return all such property/equipment to the Company in good condition at the time of separation from the Company or as and when directed by the Management.

The protection of information, property and all other Company assets are vital to the interest and success of the organization. Accordingly, no related information or property, including without limitation, documents, electronic documents, files, records, computer files, equipment, office supplies or similar materials may be removed from the Company's premises except in the course of performing duties on behalf of the organization and with the permission(s) of the appropriate Department Head and Country Head.

In case of employees working from home, the company has stringent IT and data protection policies and procedures in place and expects employees to be cognizant of the fact that all policies and processes are adhered to as is done in the physical contact center or the client's environment. Employees should adhere to the IT Security and Protocol guidelines specified in 'Remote Work Policy'. In addition, employees shall follow the Acceptable Use Policy (AUP) available with IT department for all IT assets (whether owned by company or individual).

21. Telephone courtesy

Much of our business is conducted via telephone and for the same, each employee is expected to place special emphasis on telephone courtesy. The following guidelines should be adhered to when speaking on the telephone:

- Use a tone of voice that conveys interest, enthusiasm and a willingness to help.
- Answer calls promptly.
- Ask callers if you may put them on hold, and do so only for one minute or less; call them back promptly if you are unable to talk right away.
- When transferring a call, identify by name and extension number, the person to whom you are transferring; inform the person receiving the transfer who the caller is and the nature of the call.
- Make your calls as brief as possible.
- Personal calls should be avoided unless emergencies arise.

22. Computer, Email, Intranet & Internet usage and Official Instant Messaging Service Computer

- The Company purchases and licenses the use of various computer software/ hardware for business purposes.

Employees may only use software according to the business requirement. The Company prohibits the illegal duplication of software and its related documentation.

- Equipment must not be attached to or removed from, the Company network, or removed from its normal location, without the approval of the IT in-charge/ the person authorized by him. This includes any equipment brought into the Company, for any reason, by third parties.
- Modems must not be connected directly or indirectly to the Company network without the approval of the IT in-charge / the person authorized by him/her.
- Illegally acquired software must not be loaded on Company owned equipment to avoid risks from viruses or other malicious devices and to prevent exposure to legal proceedings.
- Password to network access should not be shared or disclosed. If a workstation is shared by more than one person, then the each user should use his own user ID while accessing the network. There should not be any written record of passwords.
- The Company has installed a variety of firewalls, proxies, internet address screening programs and other security systems to ensure the integrity, safety and security of Company's network and to limit access to certain sites. Any attempt by users to disable, defeat or circumvent these systems may result in disciplinary action and suspension of access to Intranet/Internet.

Email

- The Company's e-mail system is designed exclusively for business purposes. Personal use of the e-mail system is not permitted. Employees provided with access to e-mail should use discretion and professionalism when writing e-mail messages.
- Each e-mail user has a unique access login and password. The login allows access to messages sent for the user. Use of passwords or other security measures does not in any way diminish the Company's rights to access materials on its system, or create any privacy rights of employees in the messages and files on the computer/laptop. Any password used by employees must be revealed to the Management, as emails may need to be accessed by the Company in an employee's absence.
- Login facility will be issued by the e-mail administrator upon receipt of a request from the user duly approved by HR department.
- Legally, e-mail messages are the same as written messages and, like written documents, can be subpoenaed and used in a court of law as evidence. Accordingly, confidential matters should be marked appropriately and / or sent only via hard copy, where appropriate.
- E-mail is a Company asset and any misuse such as carrying/receiving pornography or any undesirable communication etc. may result in disciplinary action.
- The Company, in its discretion as owner of the email system, reserves and may exercise the right to monitor, access, retrieve and delete any matter stored in, created, received or sent over the email system, for any reason and without the permission of employees.
- Employees should be aware that deletion of any e-mail messages or files would not truly eliminate the messages from the system. All email messages are stored on a central back- up system in the normal course of data management.
- The Company's policies against sexual or other harassment apply fully to the e-mail system, and no e-mail messages should be created, sent, or received if they contain intimidating, hostile, or offensive material concerning race, colour, religion, gender, sexual orientation, age, national origin, disability or any other classification protected by law. In addition, the Company's e-mail system may not be used for religious or political causes, commercial enterprises, or on behalf of outside organizations.
- The Company's e-mail system will not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information or similar materials without prior authorization from the Company management. Employees, if uncertain about whether certain information is copyrighted, proprietary, or otherwise inappropriate for transfer, should resolve all doubts in favor of not transferring the information and consult any member of the Company's Information Technology staff.
- **Derogatory Statements:** Because e-mail records and computer files may be subject to discovery in litigation, employees are expected to avoid making statements in e-mail or computer files that would not reflect favorably on the Company or any employee if disclosed in litigation or any other legal matter.
- **System Maintenance:** Employees should routinely delete outdated or otherwise unnecessary e-mails and computer files. These deletions will help keep the system running smoothly and effectively, as well as minimize maintenance costs.
- **Courtesy:** Employees are reminded to be courteous to other users of the system and always conduct themselves in a professional manner. E-mails are sometimes misdirected or forwarded and may be viewed by persons other than the intended recipient. Employees should write e-mail communications with no less care, judgment and responsibility than they would use for letters or internal memoranda written on Company letterhead.

Intranet/ Internet

- The Company provides access to the information available on the Intranet/Internet to its employees specifically for business related and other permitted purposes only.
- Employees should not use the facility of Intranet/Internet in violation of the laws and regulations of the land.
- The Company is not responsible for material viewed or downloaded by Internet users. The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content and having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Users accessing the Internet do so at their own risk.
- The downloading, possession, distribution or copying of a copyright work (e.g. a computer program, document, photograph, music, video etc.) is an infringement of copy right unless properly authorized to do so by the copyright owner. None of these should be downloaded or stored until one is satisfied that such authorization has been obtained. Any files or software properly downloaded into the Company network in compliance with copyright authorizations or licenses become the property of the Company.
- Images, audio or videos may not be downloaded from the Internet using Company facilities except for explicit business-related use. Permitted file transfers or video downloads etc. which are communications-intensive should be scheduled for off-peak times.
- Transfer or uploading of any software or data licensed to or owned by the Company is not permitted.
- Normally transfer of any confidential / sensitive data pertaining to the Company through Internet is not permitted. However, with explicit authorization from the appropriate authority in the Company, confidential / sensitive data pertaining to the Company may be transferred across the Internet after encrypting using encryption software approved by the Management.
- Users must not possess, access, display, archive, store, edit, record, send or use any kind of sexually explicit, indecent or obscene images or text on the Company's systems. Employees must disconnect immediately if by accident connected to an Internet site that contains such material and should advise the HR/IT department immediately if they receive any such unsolicited material.
- Users must remain polite and respectful of the feelings and beliefs of others in all dealings on the Internet/Intranet and must not knowingly make any statements which may defame, slander or intend to lower the reputation of any person or entity or their goods or services.

Official Instant Messaging Service

- The company provides official instant messaging service to selected employees along with guidance on its usage to keep information safe and actions that may be taken to monitor the effectiveness of this service.
- These employees shall be provided with a unique official instant messaging service account by the company for transacting official information.
- Official instant messaging service shall be used only for the business purpose and the confidential information shall not be shared with any unauthorized recipient and external official instant messaging service account/ IDs.
- Sharing of jokes, rumors, gossips, vulnerable & glossy offensive materials, forging information and other unsubstantial claims through official instant messaging service platform is strictly prohibited.
- The official instant messaging service platform shall not be used to transmit confidential, proprietary, personal, or potentially embarrassing information about the State, its employees, citizens, business associates, the media, or other third parties.
- The employees shall not view, damage or delete files or communications that belong to others and shall not open messages or attached files from any unauthorized source with permission.
- The company owns any/ all communication sent via its official instant messaging service system that is stored on company equipment. It reserves the right to investigate /monitor messages of any user for verifying any non-violation of its policies.
- Transmission of messages to multiple users/ group must be controlled to maintain the effectiveness of official instant messaging service. Employees are also prohibited from copying or storing of messages into any form of local message archives including, but not limited to, PST files, public folders, personal folders and local file folders.
- The employees are expected to adhere to the official instant messaging service guidelines and any infringement of the clauses mentioned herein could result to disciplinary action.

23. Participating and Engaging on Social Platforms

Online social platforms such as blogs (e.g. Twitter), content communities (e.g. YouTube) and social networking sites (e.g. Facebook, LinkedIn etc.) are being increasingly adopted by people to engage and exchange their views and opinions with each other about their interests, opinions, hobbies and work. These individual interactions will be an important arena for organizational and individual development and the company is committed to advocate responsible involvement in this rapidly growing environment of relationship, learning and collaboration. Therefore, employees are expected to be aware of the following guidelines while participating in this sphere of information, interaction and idea exchange on social media and other online mediums:

- The company has well established means of communicating publicly to the marketplace or to the general public; hence only officially designated employees have the authorization to speak on behalf of the company.
- Employees should refrain from discussing topics relevant to the organization, however in case they would like to share their views in capacity of 'Subject Matter Experts', employees should use their real name, be clear who they are, and identify that they work for the organization. If there is a vested interest in the discussion, then employees should be judicious in disclosing personal details.
- While identifying as an employee in a social network, employees should ensure that the content associated with them is consistent with their work at the company. New joiners should update their social profiles to reflect the company's guidelines. The organization's logos or trademarks should not be used as a part of any postings, including identity on a site, unless approved to do so.
- Employees should speak in the first person, use their own voice and bring their own personality to the forefront while communicating in blogs and social media sites.
- While publishing content to any form of digital media, employees should make it clear that what they say is representative of their views and opinions and not necessarily the views and opinions of the company. The following standard disclaimer should be prominently displayed in one's blog: "The postings on this site are my own and don't necessarily represent the company's positions, strategies or opinions." If a site does not afford enough space to include the full disclaimer, then employees should be judicious in positioning their comments appropriately.
- Managers and executives should note that the standard disclaimer mentioned above does not exempt them from a special responsibility when participating in online environments. By virtue of their position, they must consider whether personal thoughts they publish may be misunderstood as expressing the organization's positions. Public forums are not the place to communicate company policies to employees.
- Proper respect should be shown for the laws governing copyright and fair use of copyrighted material owned by others, including the company's own copyrights and brands. Employees should not quote more than short excerpts of someone else's work and it is a good general blogging practice to link to others' work.
- Employees should be thoughtful of what they publish particularly on external platforms. Confidential or proprietary information related to the company, any other person or company should not be disclosed or used in any online social medium platform. For example, permission has to be sought before posting someone's picture in a social network or publishing in a blog any conversation that was meant to be private.
- Employees should refrain from discussing sensitive topics related to the company even if a disclaimer is being used. For example, comments and speculations on the organization's future business performance (including upcoming quarters or future periods), business plans, unannounced strategies or prospects (including information about alliances), potential acquisitions or divestitures, similar matters involving company's competitors, legal or regulatory matters and other similar subjects could negatively affect the company.
- Clients, partners or suppliers should not be cited or referenced in any social media platform without their prior permission. It is acceptable to discuss general details about kinds of projects and to use non-identifying pseudonyms for a client (e.g., Client ABC) so long as the information provided does not make it easy for someone to identify the client or violate any non-disclosure or intellectual property agreements that may be in place with the client. Information such as travel plans, publishing details about current location or place of work on a particular day may inadvertently lead others to deduce information about clients, partners and suppliers. Employees should not publish anything that might allow inferences to be drawn that could embarrass or damage a client.
- Employees are expected to respect the audience and their co-workers while communicating in their personal blogs. Ethnic slurs, personal insults, obscenity, inflammatory topics such as politics and religion, etc. should be avoided. If the blog is hosted on a company owned property, proper prior approvals should be taken from the reporting manager. If the blog is self-hosted, best judgment should be used to make it clear that the views and opinions expressed are of self and do not represent the official views of the company. While it is fine to disagree, employees are expected not to use their external blog or other online social media to air the differences in an inappropriate manner.

- Company owned domains should be used in a way that adds value to business, helps employees and co-workers, clients and partners to do their jobs and solve problems, helps improve knowledge or skills, contributes directly or indirectly to the improvement of the organization's products, processes and policies, builds a sense of community and helps to promote the company's values. Though not directly business-related, background information about self, family or personal interests may be useful in helping establish a relationship; however it is at the sole discretion of the employee to share this information.
- Employees should be upfront in correcting any error they make while interacting in a social platform as this will help to restore trust. In case any content that was previously posted has been modified, such as editing a blog post, then such modification should be made clear.
- Employees are expected to use a warm, open and approachable tone while communicating in an online platform and also project a positive image of the company's brand.
- Since there are always consequences to what is being published, employees should review the content and discuss it with their Managers to avoid any discomfort. Employees are personally responsible for the content they publish online, whether in a blog, social media site or any other form of user-generated media and the consequences thereof. Hence care must be taken for protection of privacy and understanding a site's terms of service. It is being made explicitly clear that the organization will not be held responsible in any way for the consequences arising out of the content published online by the employees and it will be the sole responsibility of the employee only.

24. Gender Harassment

Gender harassment refers to behaviour of a sexual nature that is not welcome and which interferes with an employee's status of performance by creating an intimidating, hostile or offensive working environment. It is a form of assault, which can manifest itself in terms of physical and psychological acts. This behaviour may involve either the same gender or the opposite gender. This conduct may include, but is not limited to, the following:

- Making unwelcome sexual advances and/or requests for sexual favours or other verbal/physical conduct of a sexual nature as a condition of employment.
- Submission to or rejection of the behaviour becomes (implicitly or explicitly) a basis for decisions that affect the individual's employment or a condition of the individual's employment.
- The behaviour has the purpose or effect of unreasonably interfering with an individual's work performance or creates an intimidating, hostile or offensive work environment.
- Repeated, offensive and unwanted flirtations or advances.
- Demanding sexual favours.
- Verbalizing sexual innuendoes, suggestive comments, lewd/sexual jokes or references, sexual propositions or threats.
- Displaying sexually suggestive objects, graphic commentaries, making suggestive or insulting sounds, whistling and obscene gestures.
- Sexual harassment may be subtle or obvious. Whatever form it takes, it can be insulting and demanding and will not be tolerated.

The Company discourages such behaviour and has a comprehensive framework to deal with such cases.

25. Substance abuse/ Intoxication

The Company expects the employees to report in a state of mind and physical condition that will allow them to perform their assigned duties in a competent and safe manner. For this reason, no employees should possess/consume/use/be under the influence of alcohol, illegal drugs or controlled substances in the Company premises. Selling, possessing, using, delivering or receiving alcohol/illegal drugs/controlled substances at any time during the workday or anywhere on the Company premises is strictly prohibited. Violators will be subject disciplinary action, up to and including termination.

Any employee who must use a prescription drug that causes adverse side effects like drowsiness, impaired reflexes or reaction time shall not be allowed to work during such period.

26. Smoking

The Company is committed to promoting a safe and healthy work environment free from hazards associated with smoking. Smoking entails risk to personal health and secondary smoking to the health of others in the Company. Therefore all office premises of the Company are 'No Smoking' areas and smoking is prohibited within the confines of all buildings and facilities owned or leased by the Company. Employees who wish to smoke may do so during regular breaks and meal periods, but must do so only outside the office premises. Smoking materials must not be kept lying around in the open in the work place or discarded on the grounds within the office premises.

27. Dress code

Employees are required to be appropriately dressed when reporting for work. Employees should remember that potential clients and business partners are often invited to visit Company's offices. Consequently, the Management places a high value on the effect employees' professional appearance can have on the positive image of the Company. In general, employees should dress conservatively, attractively and in good taste. Good personal hygiene is a must.

The following examples represent acceptable standards of dress: skirts or dresses no shorter than 2" above the knee, dress or khaki pants, jeans (without holes, fraying), jackets, blazers, sweaters, vests, dress shirts, golf/ knit shirts/ collared T-shirts, shirts with ties, appropriate undergarments, well-groomed hair worn in an appropriate style, jewelry worn in moderation, dress shoes, athletic/walking shoes, tennis shoes, flats and boots.

The following examples represent unacceptable standards of dress: skirts or dresses that are more than 2" above the knee or that have slits or openings that are more than 2" above the knee, sweat suits, football jerseys, gym clothes, shorts, cutoffs, sagging pants/shorts, tank tops, tube tops, jackets/vests worn without shirts, transparent clothing, backless clothing, visible undergarments, no exposed midriffs, buttocks, breasts or other sexual body parts, clothing on which sexually explicit or profane language is printed, clothing covered with sequins/beads, exotic or extreme hair colors or styles, wearing bandanas or du-rags (head wraps) / caps indoors.

For safety purposes, the following types of footwear are unacceptable: platforms, spike heels (over 2"), flip-flops, open sandals and slippers. Please note that guidelines for acceptable footwear can change at any time without notice.

The guidelines set forth above represent the minimum acceptable standards and may vary at individual locations only to the extent that a location has more stringent standards. In addition, deviations from this policy may be permitted on certain days such as last day of the week or Theme days as approved by the Business HR Head.

On the first violation, the employee will be sent home to change and return to work, dressed appropriately. Repeated violations of the Company's personal appearance standards will result in progressive disciplinary action. Work time missed because of failure to comply with this policy will be without compensation.

28. Access to Employment Records

The Company maintains confidential employment files and records on all employees. Access to the records is restricted to members of the Human Resources department. Limited access may be granted to certain other management personnel if authorized by the Corporate Human Resources department.

- Individual employees may review their own personnel file (not to include any documents secured pre-employment and not to include confidential files) by adhering to the following procedures.
- Requests must be made in writing to Human Resources on "Request to Review Employment Records" form. The Human Resources representative will establish an appointment date and time during normal business hours. This appointment will be set within seven (7) working days of receipt of request.
- All reviews must be conducted in the presence of a Human Resources representative.
- The employee reviewing his/her file can make notes, but may not copy, remove, alter or change any document unless specifically allowed by applicable state law.
- Reviews of employment files will be limited to one review per calendar quarter unless additional review is allowed under applicable state law.

29. Emergency Closing Policy

Emergency conditions such as severe weather, fire, flood, or earthquake, can disrupt company operations and interfere with work schedules, as well as endanger employees' well-being. These extreme circumstances may require the closing of the work facility. In the event that such an emergency occurs during non-working hours, employees will be notified of a closure as per site specific guidelines. In the event that operations are required to be shut down as a direct result of any of the above conditions, time off from scheduled work will not be paid. Employees may opt to use PTO to cover the time off, if available.

30. Visitors

Visitors are welcome in the site and as an organization and may present security, safety and liability issues, employee and the company; therefore visitors should adhere to the following procedure:

- Visitors entering the facility should use the site's main entrance and should never be allowed to access the building through designated employee entrances.
- Visitors must sign the register or visitor log in the main entrance or reception area.
- Visitors will be issued a visitor identification badge that is to be worn in a visible spot at all times and should be returned to the Receptionist or security staff or other designated representative at the conclusion of the visit.
- Visitors must be accompanied by an employee at all times.
- Visitors must exit through established security checkpoint or main entrance or reception area if security checkpoint does not exist.
- Visitors in the building outside the normal business hours should follow the procedure above to the extent possible. Employee must receive approval from their manager prior to allowing a visitor in the facility during non-business hours.

Business Visitors

Business Visitors will be required to follow the general guidelines of this policy and should have a scheduled appointment.

- Business visitors must remain in the main lobby or receptionist area until the employee is able to greet them and escort them to the meeting location.
- Length of visit should be limited to the time necessary to conduct established business.

Personal Visitors

Personal Visitors will be required to follow the general guidelines of this policy and may or may not have a scheduled appointment.

- Personal visitors should remain in the main lobby or receptionist area until the employee is able to greet them and escort them to a meeting location in a non-production area.
- Employee will be required to sign a waiver for children in the workplace if the child is under 18 years of age.
- Building access will be limited to non-production areas.
- Employee must receive approval from their manager before a personal visitor can access or tour the production area.
- Length of visit should be limited to the time the employee is allotted for lunch or break or time needed to tour the facility.

Other Visitors

Other Visitors must sign the register or visitor log in the main lobby or receptionist area and generally will not have a scheduled appointment.

- Other visitors should be encouraged to schedule an appointment if they do not have one. Building access will be limited to the main lobby or reception area.
- Length of visit should be limited to the time necessary to schedule an appointment or notify visitor of company's no solicitation/distribution policy.

Applicants

Applicants will be required to enter and exit the building through the main entrance reception area or established security checkpoint and may or may not have a scheduled appointment.

- Applicants should remain in the main lobby or reception area until the designated human resources representative is able to greet them and escort them to the testing or interviewing area.
- Building access will be limited to the main lobby or receptionist area and testing or interviewing area.
- Length of visit should be limited to the time necessary to complete application, testing, and interviewing procedures.

Contractors and Temporary Employees

Contractors and Temporary Employees must enter and exit through established security checkpoint or employee entrance if security checkpoint does not exist.

- Contractors will be required to follow the policies and procedures outlined by the company.
- Contractors should be issued a temporary employee identification badge and should return it upon completion of the project or assignment for which they were hired.

31. Record-Keeping

The Company requires honest, complete and accurate recording and reporting of information in order to make responsible business decisions. For example, only the true and actual number of hours worked should be reported and approved. Many employees regularly use business expense accounts, which must be documented and recorded accurately and approved. If an employee is not sure whether a certain expense is legitimate, inquiries should be made to supervisors or the controller.

All of the Company's books, records, accounts and financial statements must be maintained, must appropriately reflect the Company's transactions and must conform both to applicable legal requirements and to the Company's system of internal controls. Unrecorded or "off the books" funds or assets should not be maintained unless permitted by applicable law or regulation.

As a public company, it is of critical importance that the Company's filings with the Securities and Exchange Commission be accurate and timely. Depending on the employee's position, he/ she may be called upon to provide necessary information to assure that the Company's public records are complete, fair, and understandable. The Company expects the employee to take this responsibility seriously and provide prompt and accurate answers to inquiries related to the Company's public disclosure requirements.

Business records and communications often become public, and we should avoid exaggeration, derogatory remarks, guesswork, or inappropriate characterizations of people and companies that can be misunderstood. This applies equally to e-mail, internal memos, and formal reports. Records should always be retained or destroyed according to the Company's record retention policies. In accordance with those policies, in the event of litigation or governmental investigation please consult the Company's Chief Financial Officer. Employees are required to cooperate with any and all internal and external audits that are sanctioned by the Company. From time to time, the Company may be involved in lawsuits or other government audits. Only approved employees are authorized to participate in legal proceedings and in government investigations and audits as instructed by the Chief Financial Officer or Legal Department. Any employee who becomes aware of any legal matter, such as receiving a copy of a lawsuit or request for information from a government agency, should immediately notify the Legal Department. If the Company or the government issues a document retention notice in connection with any lawsuit or investigation, all employees are expected to fully comply with any document retention notice. Nothing in this code should be construed to limit employees' rights to respond accurately and fully to any question or inquiry when required by legal process or as part of a government investigation.

32. Responsibilities of Senior Financial Management

In addition to the other provisions of the Code, the Company's Chief Executive Officer, Chief Financial Officer, Controller, Principal Accounting Officer and other employees performing similar functions (the "Senior Financial Management") have particular obligations to promote honest and ethical conduct and to deter wrongdoing. All members of the Senior Financial Management shall:

- Act honestly and ethically in the performance of their duties at the Company and lead by example.
- Avoid actual or apparent conflicts of interest between personal and professional relationships.
- Provide full, fair, accurate, timely and understandable disclosure in reports and documents that the Company files with, or submits to, the Securities and Exchange Commission and in other public communications by the Company.
- Comply with rules and regulations of federal, state and local governments and other private and public regulatory agencies that affect the conduct of the Company's business and the Company's financial reporting.
- Act in good faith, responsibly, with due care, competence and diligence, without misrepresenting material facts or allowing the member's independent judgment to be subordinated.
- Respect the confidentiality of information acquired in the course of work, except when authorized or legally obligated to disclose such information.
- Share knowledge and maintain skills relevant to carrying out the person's duties within the Company.
- Proactively promote ethical behavior as a responsible person among peers and colleagues in the work environment and community.
- Achieve responsible use of and control over all assets and resources of the Company entrusted to the person.
- Promptly bring to the attention of the Audit Committee of the Board of Directors any information concerning (a) significant deficiencies in the design or operation of internal controls which could adversely affect the Company's ability to record, process, summarize and report financial data, (b) any fraud, whether or not material, that involves management or other employees who have a significant role in the Company's financial reporting, disclosures or internal controls or (c) any material violation of (i) any law, rule or regulation (including securities laws applicable to the Company or the operation of its businesses) or (ii) this Code.

33. Complaint Procedures

Hotline. Although complaints should first be reported to supervisors, managers, Human Resources, and other appropriate personnel, the Company also has a toll-free confidential hotline id i.e. ethicscommittee@startek.com for its employees to report any violations of law, this Code or other Company policies by Company officers, directors or employees. Complaints submitted on the hotline will be managed as follows:

The Company will not tolerate harassment, retaliation, or any kind of discrimination or adverse action against an employee (whistleblower) who:

- Makes a good-faith complaint about suspected Company or employee violations of the law or of this Code;
- Provides information or assists in the investigation; or
- Testifies or participates in the proceeding related to violations of the law or this Code.

The Company encourages employees to report suspected retaliation and also requires supervisory employees to report suspected retaliation. Employees can report alleged retaliation in the same manner discussed above. Additionally, employees may take any violations of this Code or retaliation for reporting violation of this Code to the Audit Committee. Employee complaints of alleged retaliation will be promptly investigated and addressed.

- Complaints of a human resource nature will be referred to and handled by Human Resources.
- Complaints relating to financial and accounting matters will be referred to and handled by the Audit Committee of the Board of Directors.
- All other complaints will be referred to and handled by, or under the direction of, designated executive officers of the Company.

Reporting Violations, Investigation and Response. In order to facilitate a complete investigation, employees should be prepared to provide as many details as possible, including a description of the questionable practice or behavior, the names of any persons involved, the names of possible witnesses, dates, times, places, and any other available details. The Company encourages all employees with complaints or concerns to come forward with information and prohibits retaliation against employees for raising concerns or participating in investigations. Nonetheless, if an employee feels more comfortable doing so, reports may be made confidentially and/or anonymously in the manner described above.

Supervisors and managers who become aware of any questionable accounting or auditing matters, or who receive complaints or concerns about such matters from other employees, must immediately report them through the Hotline as referenced above. Supervisors and managers who receive complaints of questionable accounting or auditing matters must consult with the Audit Committee before undertaking an investigation or other action. The Audit Committee has final responsibility and authority for the investigation and handling of any concerns or complaints relating to accounting and auditing practices. Any supervisor or manager who fails to report allegations of questionable accounting or auditing practices in accordance with this Code or who otherwise fails to deal properly with such allegations may be subject to discipline.

Financial, Accounting and Audit Matters. Any person who has complaints or concerns about the Company's accounting, internal accounting controls or auditing matters, or who becomes aware of questionable accounting or auditing matters, is strongly encouraged to report such matters through the hotline as described above or directly to the Audit Committee. The Audit Committee will oversee the receipt and handling of allegations of questionable accounting or auditing matters, including directing an appropriate investigation and response. Based on its investigation, the Audit Committee will direct the Company to take prompt and appropriate corrective action in response to the complaint or concern if necessary to ensure compliance with legal and ethical requirements relating to financial, accounting and audit matters of the Company.

Confidentiality and Non-retaliation. Complaints will be kept confidential to the extent possible consistent with the Company's obligation to investigate and correct unlawful or unethical accounting or audit practices or other violations of this Code. In order to ensure confidentiality, an employee may elect to make a complaint anonymously. Anonymous reports will be investigated if sufficient information is provided. In conducting an investigation, the Company will respect the privacy of all concerned; however, complete confidentiality may not always be possible because of the need to conduct an investigation and take appropriate steps. Employees are expected to cooperate in internal investigations of misconduct and other violations of this Code.

The Company will not retaliate or take any form of reprisal against any person who makes a report pursuant to this Code or who participates in an investigation regarding a violation of applicable securities laws, rules or regulations, or any provision of other laws regarding fraud against stockholders. Any employee who retaliates against another employee or a witness as described above will be subject to discipline, up to and including termination of employment. Employees who believe they are subject to retaliation because they have made a report or participated in an investigation should report such suspected retaliation to the Audit Committee in the same manner as described above for the reporting of questionable practices. Knowingly or recklessly providing false information to the Company regarding any complaint may result in disciplinary action, including termination without notice (subject to applicable laws, rules and regulations and any employment agreement which governs an employee's employment).

34. Compliance with Laws, Rules and Regulations

Obeying the law, both in letter and in spirit, is the foundation on which this Company's ethical standards are built. All employees must respect and obey the laws of the cities, states and countries in which we do business as well as respect local cultures and customs.

I have read and been informed about the content, requirements, and expectations of the code of conduct Policy, and agree to abide the policy guidelines as a condition of my employment.

Employee Name MIRZA AHAD BEGH

Employee Signature *Mirza Ahad*

Date

Orientation Program Quality Monitoring Questionnaire

Questions

Feedback

(Excellent/ Good/ Average/ Not Applicable)

Arrival (not applicable for virtual/ remote joining):

1	How well were you guided by the Security?	
2	How well were you welcomed by the receptionist?	
3	How did you find the office ambience?	
4	How quickly were you guided by the right person?	

Joining Formalities:

5	How user friendly was the joining kit?	Excellent
6	How did you find the procedure?	Excellent

Query Handling:

7	How sensitive were the people to your needs?	Excellent
8	How quickly were you queries / anxieties, if any, handled?	Excellent
9	How clearly did you get resolution for your queries?	Excellent
10	How satisfied were you the way your queries were handled?	Excellent
11	How complete was the information provided to you?	Excellent

Departmental Induction:

12	How would you rate the Department Induction?	Excellent
----	--	-----------

Orientation Process :		
13	Were you explained about?	(Yes/ No/ Not applicable)
	Policies and Procedures	YES
	Performance Management System	YES
	Operating Guidelines	YES
	Buddy	YES
	Job Expectations	YES
	Logistics	YES
14	How relevant did you find the contents?	Excellent
15	How did you find the method of orientation?	Excellent
16	How has your orientation expectation been met?	Excellent
17	How do you rate the overall quality of orientation program?	Excellent
Overall:		
18	How well did your HR facilitator hand hold you?	Excellent
Any other comments / suggestions:		
Excellent		
Do you have any suggestions to improve the process?		
Excellent		

Your views on the duration of the Orientation Process?

Your overall joining experience at Startek

5	Excellent
4	Very Good
3	Good
2	Average
1	Poor

***We thank you for your valuable time that you have invested in answering our questionnaire.
Thanks,***

TEAM HR