



Business
Services

ORANGE BUSINESS SERVICES INDIA TECHNOLOGY PRIVATE LIMITED
Employment and Personal Data Form

Please complete all sections in your hand writing. If a section is not relevant, please indicate accordingly.

Joined as: Technical Consultant Blood group: O+ Ve
Location: BSP Bhilai Height (Ft.): 6.1"
Date: 28/01/2018 Wright (Wg.): 67 Kg.



Staff name: Bhanu Pratap Deshmukh
Father's / Husband's full name: Lahurman Singh Deshmukh
Gender: Male Date of birth: (DD-MMM-YYYY) 14-12-1993
Marital status: Single Place of birth: Kurg

Permanent address: Vill- Neoji , Post - Kachandwri
Teh- Gunderdehi Balod 491223
Telephone no: 07587185580 , 09098566196

Emergency address: Purani Basti Gandhi chowk
Supela Bhilai 490023.
Telephone no: 08 09179525647

Nationality: Indian Religion: Hindu Mother tongue: Hindi
Physically defects (if any): NA Any major illness: NA



**Business
Services**

ORANGE BUSINESS SERVICES INDIA TECHNOLOGY PRIVATE LIMITED
Employment and Personal Data Form

Nominations	Name of the nominee	Address	Relation	DOB	Percentage
Provident Fund	LAHURMAN SINGH DESHMUKH	Vill- Deosri Post - Kachandw Teh - Gunderdehi Balod - 491223	Father	10/02/63	100 %
Gratuity	LAHURMAN SINGH DESHMUKH	Vill- Deosri Post - Kachandw Teh - Gunderdehi Balod - 491223	Father	10/02/63	100 %
Any dues					

Family Information:

Please give details of your family members (spouse, children, parents, brothers and sisters)

Name	Relation	DOB	Qualification	Occupation	Location if not staying with you
LAHURMAN SINGH DESHMUKH	FATHER	10/02/63	I.T.I	Service	Gunderdehi
MEENA DESHMUKH	MOTHER	04/04/67	Matric	Service	Gunderdehi
Bhupendra Deshmukh	Brother	03/02/89	BE	Service	Bhavneshwar
Ragini /	Sister, In, Law	21/09/90	M.Tech	H/W	Bhavneshwar



Business
Services

ORANGE BUSINESS SERVICES INDIA TECHNOLOGY PRIVATE LIMITED
Employment and Personal Data Form

Previous Experience:

Name of the employer	From	To	Designation	Reporting to (Name & Designation)	CTC on Separation	Reason for Leaving
Centum workskill priv. Ltd.	01/09 2016	20/01 2018	Vocational Trainer	Idrish M. Ansari State Coordinator	2040LPA	Better opportunity

Job Responsibilities at your previous
employer:

Vocational Training on basic telecommunication
to Govt. High school students

Your specific Achievements in the said job:



Business
Services

ORANGE BUSINESS SERVICES INDIA TECHNOLOGY PRIVATE LIMITED
Employment and Personal Data Form

Language known	Read	Write	Speak
Hindi	✓	✓	✓
English	✓	✓	✓

Your Strengths:

Willingness to Learn, Problem solving skill

Your Weaknesses:



ORANGE BUSINESS SERVICES INDIA TECHNOLOGY PRIVATE LIMITED
Employment and Personal Data Form

Education details:

Degree	Month & Year of Passing	Board/University	Major Subjects	% of Marks
SSC or equivalent	March 2009	CGBSE Raipur		73.33%
HSC or equivalent	March 2011	CGBSE Raipur		70.60%
Diploma				
Graduation	BE (EC)	CSVTU Bhilai		72.05%
Post-Graduation				
Professional				
Technical Certification				
Others				

Professional Training attended:



Business
Services

ORANGE BUSINESS SERVICES INDIA TECHNOLOGY PRIVATE LIMITED
Employment and Personal Data Form

Passport details:

Passport Number	Start Date	End Date	Issued at	Visas (if any)

Preferences:

Please provide two references. One from your ex-Employer.

Name	Occupation/Designation	Employed with	Email ID	Contact Number	Mailing address
Gulshan Deshmukh	Service/ Vocational Trainer	Centum work skill indit. Ltd	gulshan. desh@ gmail.com	9630519751	
Bhupendra Deshmukh	Service/ Administrative officer	National Insurance Co. Ltd.	B bhupendra. deshmukh03 @gmail.com	9179525647	

I hereby confirm that the above information is true & correct is the best of my knowledge.

Signature

28/01/2018

Date

Place



Business
Services

To

Human Resources
Orange Business Services India Technology Private Limited
Navi Mumbai

Date: 28/01/2018

Subject: Joining report

Respected Sir/Madam,

Further to your offer letter dated 18/01/2018 this is to inform you that, I have joined duties at BSP, Bhilai (location) with effect from 25/01/2018 (date).

I am enclosing the company standard application form in all its details including two passport size photographs for your records.

I look forward a fruitful association and a successful career with Orange Business Services India Technology Private Limited.

Name: Bhanu Pratap Cheshmalki Name: _____

Signature: [Signature] Signature: _____
(of employee) (of HR representative)



Code of Ethics

Attire Code

It is essential that everybody follows the highest level of professionalism at work, both internally at office site and externally with customers.

Appearances contribute a great deal to the business image that the Company presents to the customers, visitors and colleagues.

Monday to Thursday: "Business Formals"

Business Formals for Men	Business Formals for Women
Business suit, Blazers (optional)	Business suit (optional)
Formal collared shirts and trousers	Formal collared shirts and trousers, skirts (at least knee length)
Formal shoes (black or brown) and socks	Traditional Indian formal churidars and salwar kameez (kameez should be at least knee length) / sarees
Formal ties complimenting the shirt (optional)	Formal shoes, sandals (no floral and lacy chappals/sandals)

Friday, Saturday and Sunday "Smart / Business Casuals":

Smart / Business Casuals for Men	Smart / Business Casuals for Women
Normal jeans (no fancy jeans), shirts, round neck / collared T-shirts, sports shoes.	Normal jeans (no fancy jeans), shirts, round neck / collared T-shirts, sports shoes/sandals.

Everybody is strictly required to avoid inappropriate dress code that is defined below.

Example of inappropriate dressing:

- Dirty, rippled, patched or faded clothing or shoes
- Trousers with embroidery / tattoos
- Sweat shirts / jerkins, or athletic shirts with offensive slogans
- Excessive accessories like too many bangles, heavy jewellery
- Loud make up, bright hair color like red / green etc
- Shirts with other Company's corporate (Competitor) logos or with offensive or political slogans
- Clothing which is too tight, short or revealing
- Visible body piercing is also inappropriate (on eye brows/tongue etc. unless for medical reasons)



Employees and managers are expected to use good business judgment in determining whether specific attire is appropriate. Anything that may not appear to be appreciable dress code is not allowed on any of the working / week end dress code.

CODE OF ETHICS

Ethics goes beyond what law of the land expects. It means a set of moral principles which are maintained and practiced voluntarily by institutions and persons in everyday life.

In order to ensure that all the actions and decisions taken on behalf of the Company are in consonance with highest and world class standard of integrity, it is desirable to lay down code of Ethics for the Company; its Board including Managing Director and employees.

CORE VALUES

Company has set for itself the Vision, Mission and Core Values. Our cardinal 'Core Value' stipulates that; 'we shall treat everyone with personal attention, openness, honesty and respect they deserve.'

The Code of Ethics laid down below follows from this core value, particularly the aspect of openness and honesty.

1. CODE OF ETHICS FOR BOARD, INCLUSIVE OF MANAGING DIRECTOR

- a. they shall keep the interests of the Shareholders always on the top
- b. be transparent and give true picture of the happenings to the investors, depositors, lenders etc.
- c. refrain from adverse or negative publicity/comments about fellow industrialist/business community instead exchange value-based knowledge with business community in mutual interest
- d. endeavor to get the Company recognized as a good corporate citizen discharging all its social obligations
- e. disclose promptly, on their own, any clash of interest of whatsoever nature as soon as such interest becomes apparent (this clause of disclosure of "clash of interest" is applicable also to all Employees)

2. CODE OF ETHICS FOR ACCOUNTS and FINANCE DEPARTMENT

- a. not to disclose the Company financial matters to anyone who, according to the Management, does not come under "need to know" category
- b. stay clear of any behavior leading suspicion of "insider trading"
- c. make payment promises to creditors on conservative estimates after keeping time margin up the sleeves
- d. honour all the commitments in time
- e. not to accept any favors in cash or kind, from any person receiving payment from the Company
- f. Employees shall report to Managing Director / Joint Managing Director / Chief Financial Officer any bonafide concern they may have if fellow employees are engaged in fraudulent practices. It is unethical to remain silent under such circumstances. Also it is breach of trust, Management has in the Employee



3. CODE OF ETHICS FOR SALES & MARKETING

- a. not to give false promises about quality of goods or execution dates
- b. not to indulge in running down competitors or their products but market the Company products by highlighting their merits
- c. honor all the guarantees and/or warranties given for the products and services thereof, in spirit and not by letter
- d. be transparent while granting discounts to different dealers and observe fair trade practices. There should be no discrimination / favoritism amongst dealers. The Discount terms can be different only on the grounds of turnover, payment terms, Quality of Service, infrastructure facilities available and such other factors, but not on any extraneous factors

4. CODE OF ETHICS FOR OPERATIONS & TECHNOLOGY DEPARTMENTS

- a. help the society to keep the planet pollution free and ecofriendly. To avoid all types of pollution viz. air, water, noise, electro-magnetic, thermal
- b. ensure that appropriate actions are taken to check the electromagnetic or radio frequency pollution, if any, caused due to Company Operations and that the Company products are free from viruses, radio frequency interference and other nuisances
- c. respect intellectual property rights; and not to use pirated software nor to infringe any patent rights
- d. to protect the Company from corporate technical espionage and not to involve in such activities

5. CODE OF ETHICS FOR HUMAN RESOURCES DIVISION

- a. extend courtesy to all candidates aspiring to become company Employees and protect their privacy and confidentiality
- b. not to take unfair advantages of weakness and ignorance of these candidates, particularly regarding compensation which should be offered as per company established norms
- c. endeavor not to under-employ, even if the candidate is willing to do so due to compelling circumstances. In such cases efforts should be made so that Individual facets are fully utilized and compensated
- d. select the employees solely on the basis of merits and not being influenced by recommendations of friends, high level Government Officials, relatives or by ethnic, religious, linguistic considerations
- e. not to disclose any personal details of the Employees to any outsider person/agency, unless it is required by law
- f. ensure that Office Premises are observed as non-smoking zones
- g. ensure that no drugs or intoxicants are consumed by the Employees during the office hours and within the office premises
- h. ensure that no Employee indulges in any act which may lead to sexual harassment.
- i. try to retain good Employees by persuading / counseling them but if these efforts fail and the employee insists on leaving, allow them a smooth passage and not to take steps which may compromise their future career



6. CODE OF ETHICS FOR INDEPENDENT PROFIT CENTRES

- a. not to misuse the assets and facilities provided by the Company
- b. effect procurement only after ensuring that
 - I. the quality of the products is not compromised
 - II. arm's length distance is maintained, while dealing with friends, relatives and associates
 - III. decisions are not influenced by any extraneous considerations of whatsoever nature
- c. disclose promptly, the instances of frauds in the Profit Centers. In no circumstances these incidences of frauds are to be suppressed
- d. the Managers heading the operations of branches or overseas offices to give periodically a certificate that the requirements of Code of Ethics are complied with



Code of Conduct at customer's location

Physical security compliance @ customer location

- photo ID Badges that may be issued by client must be continuously worn and visibly displayed at all times when working at customers location
- in connection with performing work on behalf of Orange, you may be issued with an Electronic Access card for gaining admittance to customer facilities. These cards cannot be loaned to anyone or used to assist another person to enter any customer facility
- lost ID Badges / Access Cards must be immediately reported to the local customer representative
- these cards and badges are the property of customer and must be returned the day your assignment to customer ends, or immediately upon customer's request
- follow customer's physical security policy when @ customer's location
- all parking and local speed limit regulations shall be followed when operating a vehicle on customer facility
- declare any USB data storage devices @ the entrance of the premises if it is mandatory requirement of the customer premises
- lock up Customer or Orange documents, system when not @ desk allotted to you
- do clean /clear your desk / workspace when you leave
- do not Leave Orange computer system unattended @ customer site or at public places without appropriate protection or security e.g. use laptop locks to secure laptops physically

Logical security compliance @ customer location

- access to customer Computer Systems, Data Networks or any Computerized Resources
- in the course of providing your services to customer, if you are provided access to any customer computer systems, you are required to protect that access using the established system of passwords and other security measures
- if you have been given Secure Token Access then passwords and Secure Tokens should not be shared with anyone, and reasonable measures should be used to protect them
- secure Tokens must be returned to the authorized customer Manager upon completion of your assignment
- customers' Computer and Network resources are exclusively for customer business purposes. Non customer business use or personal use is not advisable. (It can be done only after prior permission of the authorized customer manager)
- unauthorized access, loss, damage, theft or misuse of customer computerized or network resources must be reported to authorized customer Manager
- share the information / data with the authorized people only @ customer end
- don't bring / use any unauthorized data storage devices while in customer network
- don't access social networking/ blogs, shares trading, games, restricted sites using customer network
- avoid online chatting while in customer network
- don't post any information about customer / Orange/Customer's customer on social networking/ blogs sites
- don't download any proprietary / cracked software, illicit materials using customer / Orange network
- don't download any songs / movies / games using customer/Orange network



Business Services

- avoid using any free anti-virus scan offers while using customer or Orange computer System
- unauthorized copying of customer copyrighted material and the installation of any copyrighted software for which Orange does not have an active license is strictly prohibited
- introduction of malicious programs into the customer or Orange network or server (e.g., viruses, worms, trojan horses, e-mail bombs, etc.) is strictly prohibited
- do not reveal your Orange/customer account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home
- avoid using an Orange/customer computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or IT act 2008
- avoid Executing any form of customer network monitoring which will intercept data not intended for your host, do not make use of the Customers' telephone, fax, postal, email or other services without the verbal authorization of the Customer.
- avoid Covert information gathering on or of the Orange or customer assets and business activities
- do not Send unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email Spam)
- do not send any form of harassment communication via email, telephone or paging, whether through language, frequency, or size of messages using Orange or customer network
- do not create or forward "chain letters" or E-mail Hoax of any type.
- do not Send "France Telecom Group restricted", "France Telecom Group confidential", "France Telecom Group secret" classified information to third party via any means or media or access
- do not Send customer company's or customer's customer confidential information received for internal consumption/ evaluation to third party's via official mail ID or personal mail ID. You must safeguard customer information regarding business activities, structure, financial situation, performance, and/or any other information deemed confidential
- do not access or send personal confidential information of customer or Orange employees to third party's via official mail ID or personal mail ID
- the confidentiality and integrity of Orange business information shall be maintained while having verbal communication through telephonic network

Personal behavior standard @ customer location

- Conduct which is specifically prohibited:
- Theft, neglect or abuse of customer tools/equipment
- Possession of a firearm (even if unloaded)
- Fighting, gambling, possession of narcotics or illegal substances.
- Consumption or being under the influence of intoxicating beverages or illicit drugs or substances
- Any illegal activity using customer's name, information, property, time or other resources to perform
- Outside activities, which must be kept separate from the activities performed for customer
- Any conduct that creates an intimidating or offensive work environment. This includes, but is not limited to racist, sexist, ethnic, or homophobic comments or



Business Services

jokes; sexual advances, inappropriate physical contact; or sexually oriented gestures, pictures, jokes or statements

- Your use of the Orange's technical resources must not interfere with your productivity, the productivity of any other employee, or the operation of the Orange's technical resources. You are not authorized to play games on the Company's computers and other technical resources
- If you are running late for the meeting, inform the concerned person at customer end and ask for his availability accordingly
- Smoking is not permitted anywhere on Customer's premises outside designated smoking areas
- You must confirm with the site manager if there are designated smoking areas on the Customer's premises and if contractors are allowed to smoke in these designated areas. You will adhere to the smoking rules set up by Customer's site rules and health and safety policy. computers and other technical resources

Property use and removal @ customer location

- No property may be removed from customer owned/managed premises without written authorization from a customer representative. The customer Property Removal Procedure must be followed which provides a record of persons removing property
- "Scrap" or waste materials are customer property and should not be removed without prior permission of the authorized manager of the customer and Orange

Verbal Communication @ customer location

Verbal Communications - THINK TWICE BEFORE YOU SPEAK

- Do not discuss Orange proprietary information in public areas
- Discuss only with employees and others who have a "need-to-know"
- Do not leave Secret or Confidential information on voice mail systems
- Exercise caution when discussing proprietary information over cellular or portable telephones

Meetings

- Verify only those invited are in attendance
- Ensure participants are aware of the sensitivity of information being presented and protection guidelines
- Share information on a "need-to-know" basis only
- At the close of the meeting, check tables, white boards, flip charts, etc., and properly dispose of proprietary information. Leave the room as you found it with no information left behind



Laptop security

Physical Security

- The laptop shall be transported in a sturdy, weatherproof, padded, adequately sized bag
- The laptop shall not be positioned near an exterior window where it would be subject to a smash and grab type theft

Data Security

- Laptops shall be loaded with approved OS with all relevant patches and updates applied as and when available, for ensuring the security of the information residing on the laptop
- Laptops shall have power on passwords
- All-important data shall be backed up and the current copies kept readily available. Back up shall be done on appropriate media. All disks shall be carried separately from the laptop
- The hard disc shall never be reformatted without prior testing of information that is backed up
- Anti-virus software shall be installed and shall be updated on a regular basis (recommended auto update)
- Personal folders to be password protected on the laptop
- Unlicensed software, freeware/shareware, games etc. shall not be installed
- All CDs / DVDs shall be scanned for Viruses/ Trojans before use

When Traveling

- Care shall be taken not to forget / misplace the laptop and thus prevent loss.
- The equipment shall not be kept unattended or out of sight, even during a security check at an airport
- The laptop shall not be checked in as baggage
- When traveling abroad proper documentation shall be carried to ensure

Information Classification Guideline

Asset classification is the responsibility of document owner/ custodian

- **unrestricted:** the information can circulate freely outside the group without harming our interests. e.g.- company prospectus and brochure, sales and marketing material ,etc.
- **France Telecom - Orange restricted:** a breach of confidentiality would cause a limited loss to the company .e.g.- employee hand books, training manuals, etc.
- **France Telecom - Orange confidential:** a breach of confidentiality would cause serious harm and threaten our business in the short to medium term. e.g. – Project details, Business Continuity plans, Network Access passwords etc.
- **France Telecom Group Secret:** a breach in confidentiality would cause unacceptable, very serious and sustained loss, putting the company or one of its business lines at risk. e.g.-Strategic business plans, pre-sales financial information



cell phone etiquettes @ customer location

- Keep the cell phone in silent mode or the ring tone at a low level with a tune that is soft, gentle and not annoying. A obnoxious ring tones must be strictly avoided
- Speak softly on cell phone while at customer location. The goal is to communicate effectively without anybody else noticing or getting disturbed
- Do not take a personal call during a business meeting. This includes meetings with coworkers or subordinates
- Before using a cell phone in a customer/public location to discuss business issues, make sure that there will be enough distance to keep the content private
- Do not use camera phones to capture photographs of people or places or confidential information at customer location

office etiquettes @ customer location

- First impressions are important! You are the ambassador/s of the business
- Be neat, clean and as conservative as the business requires you to be
- Be respectful and courteous at all times and with everybody
- Show appreciation for the slightest courtesies extended to you
- Say, "Please; Thank you; You're welcome", as part of your everyday courtesy
- Take responsibility for your mistakes, apologize and go about correcting the mistakes
- Chewing gum and popping bubble gum in the presence of customer should be avoided
- Don't gossip about anything at customer location
- It is impossible to provide a full set of security measures to be taken in each situation. The intent of this "code of conduct" has been to present the most usual principles guiding the development and maintenance of the protection measures to secure customer data

dress code @ customer location

It is essential that everybody follows the highest level of professionalism externally with customers. Appearances contribute a great deal to the business image that the Company presents to the customers,

Business Formals for Men	Business Formals for Women
Business suit, Blazers (optional)	Business suit (optional)
Formal collared – Light colored shirts and black/brown trousers	Formal collared shirts and trousers, skirts (at least knee length)
Formal shoes (black or brown) and socks	Formal shoes (black or brown) and socks
Formal ties complimenting the shirt (optional)	Formal shoes, sandals (no floral and lacy chappals/ sandals)

Everybody is strictly required to avoid inappropriate dress code that is defined below,

- Dirty, rippled, patched or faded clothing or shoes.
- Trousers with embroidery / tattoos.
- Sweat shirts/ jerkins, or athletic shirts.
- Shirts with other Company's corporate logos or with offensive or political slogans.
- Clothing which is too tight, short or revealing.



Business
Services

- For more detailed information and information security policies, pl. go to Quality Repository:
<http://shp.itn.ftgroup/sites/Quality@GSIndia/default.aspx>
Paste the above URL in the address bar of internet explorer and hit enter
The web page will prompt for login and password, please enter
Login: Your FTID/CUID account
Password: system password
Click on any certification / Framework tab button for further information.

I have read and understood the Code of Ethic and Code of conduct mentioned in this document and will abide by the same.

Name:

Bhanu Pratap Neshmukh

Signature:

Date:

28/01/2018



Sign the Employee Acknowledgment Form!

I acknowledge that I have received a copy of the Orange Business Services India Technology Private Limited 'Employee Handbook' which describes important information about Orange Business Services, and I understand that I should consult my immediate supervisor or a Human Resources representative regarding any questions not answered in the handbook.

I understand that the only exceptions to the above information are express, written agreements between an individual employee and Orange Business Services that are signed by both the employee and an authorized officer of the Company.

Because the information, policies, and benefits described in the handbook are necessarily subject to change, I acknowledge that revisions to the handbook may occur. All such changes will be communicated through official written notices, and I understand that revised information may supersede, modify, or eliminate existing policies. Any other alteration or modification of the policies must be in writing signed by an authorized representative.

I acknowledge that this handbook is not a contract of employment and does not guarantee employment for a particular period nor does it guarantee any specific process prior to termination.

I have received the handbook, and I understand that it is my responsibility to read and comply with the policies contained in this handbook and any revisions made to it from time to time.

Employee's Name:

Bhanu Pratap Aleshmukh

Employee's Signature:

Date:

28/01/2019

P.S. Please sign this page and return to the HR representatives.

The Group Code of Ethics

ACKNOWLEDGEMENT

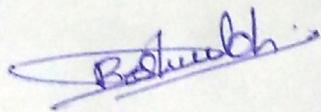
I hereby confirm that you have read, understand and agree to abide by the Group Code of Ethics*.

*should certain provisions of the Group Code of Ethics conflict with local law of a particular country, such regulations would not be applicable in that country.

Employee Name

Bhanu Pratap Seshmulch

Employee Signature



Date

28/01/2018



NON DISCLOSURE AGREEMENT

This Non Disclosure Agreement ("Agreement") made between **Orange Business Services India Technology Pvt. Ltd.**, a Company incorporated under the provisions of the Companies Act, 1956, and having its registered office at **DSO 601-603, 607-608, 6th Floor, DLF South Court, Saket, New Delhi 110017** (hereinafter referred to as the "Company" which expression shall, unless the context requires otherwise, mean and include its successors and permitted assigns).

And

Bhanu Pratap Aeshmuelch

[Name of Employee / outsource resource /

Retainer ship consultant], adult, residing at

Vell-deori, Post-Kachander

Tehsil - Gunderdehi Dist - Balod pin - 491223

(hereinafter referred to as the "Employee / outsource resource / retainer-ship consultant")

WHEREAS

- a. The Company is inter-alia engaged in the business of Network Engineering, Managed Services and other incidental services.
- b. The Employee / outsource resource / retainer-ship consultant is appointed in the Company and in the course of his/her employment, the Employee/outsource resource/ Retainer ship consultant will have access to certain information, which are confidential in nature.
- c. The Company always considers such Confidential information as critical for its business and requires the Employee / outsource resource / retainer-ship consultant to protect the same.
- d. The Employee / outsource resource / retainer-ship consultant acknowledges that his employment with the Company warrants protecting such Confidential information and agrees not to disclose such Confidential information to any third party by any means.

In view of above the Employee / outsource resource / retainer-ship consultant agree as follows :

1. The Employee / outsource resource / retainer-ship consultant shall at all times maintain and keep secret and confidential the Confidential Information (as defined herein below) and shall not disclose or divulge the same or any part thereof to any person.

"Confidential Information" for the purpose means any and all information (oral or written) regardless of whether or not the information is expressly stated as 'confidential' or the same is implied by the context thereof and/or may be recorded in documentary or digitized form, including but not limited to intellectual property, inventions, procedures, technology, techniques, methods, records, documents, proposals, concepts, ideas, data, knowhow, processes, formulae, designs, drawings, specifications, software programs, business plans, prices, pricing formulae and statistics, costs and discount structures, financial data, market



share, product and services development, travel and demonstration schedules and venues, customer lists, trade secrets, business plans, strategies, operational and technical capabilities, and other information and/or any other material so identified or not as confidential by the Company and disclosing such material to the Employee / outsource resource / retainer-ship consultant. All references to Confidential Information in this Agreement shall include any part thereof."

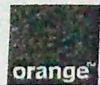
Confidential Information does not include information that:

- a. is in the public domain through no fault of Employee / outsource resource / retainer-ship consultant.
 - b. was properly known without restriction, prior to disclosure by the Company, or
 - c. was properly disclosed by another third person without restriction on its use and disclosure.
 - d. is subsequently independently developed by the Employee / outsource resource / retainer-ship consultant without use of any of the Company's Information, or
 - e. is approved for release or use by written authorization from the Company for the purpose for which it is related, or
 - f. is required to be disclosed under any relevant law or regulation provided the Company is given prompt notice of such requirement and the scope of such disclosure is limited to the extent possible, or
 - g. is required to be disclosed by an order of court, provided that the Company is given prompt notice of such order and (where possible) provided the opportunity to contest it.
2. During the Employees employment with the organization, you will at all times abide by information Security policies implemented in the Company in respect of any technical, trade or business data or any other information asset that might come to Employee's Knowledge or possession which according to the Company are confidential / restricted asset of the Company and not made available to the trade and furthermore, Employee will not disclose them without authority of the Company to anyone other than the Company's officers authorized to receive them and that even after the Employee have ceased to be in the services of the Company, Employee shall not disclose them to anyone. During and after employment period Employment shall adhere and abide by Information Security policies in respect of the above mentioned information.
 3. **Non-Disclosure and Use Restrictions:** The Employee / outsource resource / retainer-ship consultant shall retain in confidence the Confidential Information disclosed pursuant to this Agreement and shall use it only for the Purpose mentioned hereinabove. The Employee / outsource resource / retainer-ship consultant shall use the same degree of care as he/she uses to protect their own confidential information of similar nature, but no less than reasonable care, to prevent the unauthorized use, dissemination or publication of the Confidential Information.
 4. **Ownership of Confidential Information:** All Confidential Information under this Agreement shall remain the exclusive property of the Company and nothing contained herein shall be construed as a grant, express or implied or by estoppel, of a transfer, assignment, license, lease of any



right, title or interest in the Confidential Information. Any discovery, improvement, modification, correction or addition made by you as result of Employee's employment with Company, including computer programs shall remain the sole and exclusively property of Company and/or its affiliates or customers, and that Employee have no proprietary rights thereto.

5. **No Warranty:** No warranty or representation is made by the Company that, any information transmitted by it hereunder is true and correct, patentable or copyrightable, or that any such information involves concepts or embodiments that are free of infringement of other rights.
6. **Return of Confidential Information:** Upon the resignation, termination or the Employee / outsource resource / retainer-ship consultant ceasing to be in the employment of the Company for any other reason, the Employee / outsource resource / retainer-ship consultant shall (i) promptly return to the Company all Confidential Information disclosed in tangible form and copies thereof; or (ii) promptly destroy such Confidential Information (including all copies thereof) with the written approval from his / her superiors and certify their destruction/return to the Company, in writing.
7. **Equitable Relief:** The Employee / outsource resource / retainer-ship consultant acknowledges and agrees that the covenants set forth are reasonable and necessary for the protection of Company's business interests and that irreparable injury may result if they are breached and that in the event of any actual or potential breach of any such covenant that may have no adequate remedy at law and shall be entitled to seek immediate temporary injunctive relief. Nothing herein shall be construed as prohibiting Company from pursuing any other remedies available to it for such breach or threatened breach, including the recovery of damages.
8. **Governing Law:** This Agreement shall be governed and construed in accordance with Indian laws. Any legal action or proceedings relating to this Agreement shall be exclusively instituted in courts at New Delhi, India.
9. **Arbitration:** If any dispute should arise between the Parties, the Parties shall try and resolve the dispute amicably. In the event of failure to resolve such dispute amicably, either Party may refer the same to the Chief operating officer of the Company or any nominee appointed by him who shall be the sole Arbitrator and the award given by the sole arbitrator shall be final and binding on both the parties. The arbitration shall be conducted in English language as per the provisions of The Arbitration and Conciliation Act, 1996 and venue shall be in Gurgaon.
10. **Severability:** If any provision of this Agreement shall be adjudged by any court of competent jurisdiction to be unenforceable or invalid, that provision shall be limited or eliminated to the extent necessary so that this Agreement shall otherwise remain in full force and effect and enforceable.
11. **Waiver:** The failure of Company to act in the event of breach of this Agreement shall not be deemed a waiver of such breach or waiver of future breaches, unless such waiver shall be in writing and signed.



**Business
Services**

12. Entire Agreement / No Amendment: This Agreement constitutes the entire agreement and understanding of the Parties with respect to the subject matter of this Agreement. Any amendment or modification of this Agreement shall be in writing and executed by duly authorized representatives of the Parties.

For and behalf of Orange Business Services

(Signature)

Name:

Designation:

Date:

Place:

For and behalf of Orange Business Services

(Signature)

Name:

Designation:

Date:

Place:

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their duly authorized representatives effective as of the day and year first above written.

Information Security Essentials

ISMS Scope

- Information assets include digital documents and databases, software tools and utilities, network and hardware assets, back-up tapes, software CDs, UPS, A/C, infrastructure, company's brand value.

Information Security Policy

- Information assets and IT assets to be protected against unauthorized access.
- Information is not to be disclosed to unauthorized persons through deliberate or careless actions.
- Information is to be protected from unauthorized modification.
- Information is to be available only to authorized users when needed.
- Applicable regulatory and legislative requirements are to be met.
- Disaster recovery plans for IT assets are to be developed, maintained, and tested as far as practical
- Information security training is to be imparted to all IT users through refresher course.
- All breaches of information security are to be reported and investigated.
- Violations of policies are to be dealt with through a formal disciplinary process.

ISMS Framework

- To establish and manage ISMS
- To implement and operate ISMS
- To monitor and review ISMS
- To maintain and improve ISMS

Ownership of Information Assets

- The person or function creating the document or information is the owner of that document/information.
- Ownership of IT infrastructure and software assets is with the respective environment.
- Ownership of communication facilities such as telephone, facsimile, etc. is with Telecom department.
- Ownership of physical access control systems is with REFM.
- Owners of each information asset are mentioned against each asset.
- REFM shall be the owners of services (utilities such as power supply, water supply, etc.) to the IT infrastructure.

ISMS Security Organization Roles

- Apex Committee
- ISF

- CISO
- Information Security Task Force
- Incident Response Team
- Audit Committee
- System Administrator
 - System Administrator
 - Server Administrator
 - Network Administrator
- Help Desk And Local Administrator
 - ITSD
- Users, Environment Heads
- Human Resource (HR)
- Physical Security

Information Asset Classification

- **unrestricted:** the information can circulate freely outside the group without harming our interests
- **Orange restricted:** a breach of confidentiality would cause a limited loss to the company.
- **Orange confidential:** a breach of confidentiality would cause serious harm and threaten our business in the short to medium term.
- **Orange secret:** a breach in confidentiality would cause unacceptable, very serious and sustained loss, putting the company or one of its business lines at risk.
- Asset classification is the responsibility of document owner/ custodian
- Obsolete documents/records to be handled as per Document and record control procedure.

Human Resource Policy

- Identifies the roles and responsibilities of employees, contractors, and third-party staff
- Imparts training on ISMS policies.
- Defines disciplinary action if breaches are found
- Is applicable even after cessation of employment / contract

Acceptable Use Policy

The following acts are not acceptable as per Acceptable use policy:

- Violating laws such as IT law, copyright act etc
- Disclosing confidential information to unauthorized persons
- Not securing information assets
- Introducing viruses into network
- Affecting network performance
- Not protecting password secrecy
- Violating acceptable usage guidelines

Access Control Policy - Physical

- No entry into restricted / secured areas without authorization
- No media or content enters or leaves the premises without authorization and checking
- Identification badges to be clearly displayed

Access Control Policy - Logical

- Information access based on: business requirements, need-to-know basis, need-to-perform-tasks basis, and asset classification policy
- Lock equipment, media, and assets when not in use
- Promptly remove confidential documents from printers, photocopiers, and fax machines
- Always observe clear-desk-clear-screen policy
- Check your computer daily for latest virus-scan updates

Password Policy

- Don't share passwords
- Change passwords periodically
- Password creation as per guidelines
- Password owner will be responsible for password leakage

Email Policy

- Use emails only for business purposes
- Protect confidential emails from unauthorized access/ display
- Don't transmit offensive material
- Don't attach large files
- Email account will be terminated after 90 days of inactivity
- Report Spam to IT Service Desk

Communication Policy

- Don't engage in loose talk over phone; check your and recipient's environment before discussing confidential information
- Don't let confidential information lie unattended around fax, photocopy machines
- Confirm receiver's identity and destination validity before transmitting confidential information
- Confirm with recipient the receipt of confidential information
- Don't connect mobile phones to networked desktop or laptop
- Promptly destroy scrapped copies of confidential documents

Internet Policy

- Don't view, store and transmit indecent, obscene, offensive, sexually explicit Web content
- Don't indulge in online trading and gambling activity
- Don't upload/download commercial software in violation of its copyright
- Don't attempt to hack into internal or external networks
- Don't crack passwords of other logins
- Don't use external chat applications

Mobile Computing Devices Policy

- Don't attach laptops, PDA, pocket computer, USB/ Zip/ Pen/ Flash drive, I Pods, CD writers, HDD/ Webcam, digital camera, tape, cartridges etc. on to the network without authorization
- For attaching mobile computing devices for work purposes, seek authorization and follow change management procedures
- If access is provided to third-party staff, then ensure information security is maintained

Information Security Incident Management Policy

- Log all security incidents and weaknesses through mail isf.etsipl@orange.com to ISF members, phone, anonymous (drop-box @ canteen)
- Don't discuss security incidents or weaknesses with others
- For serious incidents, try and collect evidences for the incident handling team

Change Management Policy

- Don't add, modify, or delete any pre-installed software, hardware, or network resources
- For alterations, send formal request to using Change Request Form to authorized person

Procurement and Regulation of Software and Hardware

- Don't make or use unauthorized copies of any software or application
- Don't download freeware, shareware, trial ware, beta evaluation versions and games without prior authorization

Acceptable Usage Guidelines

- Ref. Acceptable Usage Guidelines

Password Procedure

- Ref. Password policy and procedure

Refer Quality Repository for ISMS policies @ URL: <http://shp.ltn.ftgroup/sites/Quality@GSIndia/default.aspx>

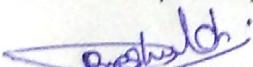


Domicile Declaration Form

1. Name: <u>Bhanu</u>	<u>Bhanu Pratap Deshmukh</u> <First Name> <Last Name>
2. Which is your state of domicile ? (means someone who has been staying or stayed in the said state for a minimum period of 15 years)	<u>Chhattisgarh</u> Name of the State
3. Please mention the document(s) you are furnishing to establish your state of domicile	<ul style="list-style-type: none">1. Domicile Certificate <input checked="" type="checkbox"/>2. School Leaving Certificate3. Property Tax4. please specify if any other (as issued by competent authority)

Employee Self Declaration:

I, Mr. / Ms. Bhanu Pratap Deshmukh do hereby declare that the above information furnished by me is true & correct to best of my knowledge. I undertake to provide the documentary evidence if required by the statutory authorities.


Employee Signature