CloudExtel

EMPLOYEE HANDBOOK

CloudExtel (Excel Telesonic India Pvt. Ltd.)
The Ruby, 11th Floor, AWFIS, Dadar (West),
Mumbai, Maharashtra - 400028
Official No: +91 98671 51303

CIN No: U74999MH2010PTC207323

10x LEVEL UP

WELCOME TO

CloudExtel

EMPLOYEE HANDBOOK

- Excel Telesonic India Pvt. Ltd.
- Netfra Solutions Pvt. Ltd.
- Bombay Gas Company (Proprietary) Pvt. Ltd.
- Orange Waves Networks Pvt. Ltd.

Index

Introduction

Awesome! Welcome to CloudExtel, an innovative and rapidly growing startup at the forefront of technology in the telecom space. We are thrilled to have you on board and we extend a warm welcome as you embark on this exciting journey with us. We are poised for remarkable growth and your contribution will be instrumental in propelling our organization forward.

At CloudExtel, we firmly believe that each team member plays a pivotal role in shaping the success of our company. Your skills and expertise are highly valued, and we are eager to witness how your unique talents will contribute to our collective achievements. We are committed to fostering a work environment that not only encourages peak performance but also provides opportunities for skill development and career advancement. Recognizing that the initial days in a new work environment can be challenging, especially in a dynamic and fast-paced organization like ours, we have designed a comprehensive induction program. This program is tailored to equip you with the necessary information, introduce you to key team members, and clarify any queries you may have about our business operations. We encourage you to make the most of this onboarding period to seamlessly integrate into the vibrant culture of CloudExtel.

CloudExtel will be both professionally rewarding and enjoyable. Your success is our success, and we look forward to achieving great milestones together.

Once again, welcome to CloudExtel. We're certain that you will have a fulfilling and enriching experience with us.

What Is The Purpose Of CloudExtel

There are many companies doing amazing work. We have picked something that solves a real problem. A problem that is not only significant but also has wide applicability. We provide NaaS (Network as a Service) solutions to telecom operators, internet service providers, data centers, enterprises, and large content providers for addressing the challenges emerging from the hyper growth of data consumption in India.

We own & operate networks that address critical points of network stress, leverage sharing and adopt emerging heterogeneous network technologies.

We have built a strong foundation basis the scaling of our Infrastructure as a Service business currently focused on Passive Infrastructure.

The principles that guide our business include:

- Enabling our customers to deliver services to their end users at the most critical points of network stress.
- Deploying networks in the most scalable, differentiated and economically efficient way, yielding substantial cost reduction and investment optimization.
- Scaling as a specialist adopting ever evolving principles & technologies from software and cloud platforms.

About The Employee Handbook

This Employee Handbook is effective from 1st April 2024 and applies to the employees engaged with the following companies in the group:

Excel Telesonic India Private Limited (ETIPL)

Netfra Solutions Private Limited (NSPL

Bombay Gas Company (Proprietary) Private Limited (BGCPPL)

Orange Waves Networks Private Limited (OWNPL)

Excel Telesonic India Private Limited is the parent entity and NSPL, BGCPPL and OWNPL are its wholly owned subsidiaries. All these four companies are collectively referred in this Handbook as “CloudExtel”, our brand name. In this Handbook, we will refer to CloudExtel as "We", "Us", "Our", or the "Company”.

This Handbook has been created to guide employees with the employment policies and practices of the Company. It serves as a resource to help you understand your rights, responsibilities, and the standards expected of you. Our objective is to ensure a productive, respectful, and inclusive work environment. This Handbook also aims to provide clarity on procedures, benefits, and company culture, ensuring that all employees are well-informed and supported throughout their employment journey. By familiarizing yourself with this Handbook, you will be better equipped to contribute to the success and growth of our Company. Any Query or suggestion, please email it to hr@cloudextel.com with subject line: “Queries on Employee Handbook / Suggestions for Improvement in the Employee Handbook”. We shall consider the suggestion, and if considered valid we will consolidate the suggestion and during the revision of the handbook in the next version they will form part of the Employee Handbook.

We are glad to have you as a member of CloudExtel. As a team member of the Company, you are an essential part of the team effort. We hope that you will find your position with the Company rewarding, challenging, and productive.

Surprise yourself everyday!

1. Code Of Conduct

OBJECTIVE

Code of Conduct outlines the expectations and guidelines for behavior within our organization, fostering a culture of respect, collaboration, and professionalism.

This policy is designed to ensure that all individuals, including employees, contractors, volunteers, clients, and visitors, feel safe and supported in their interactions with others. We believe that everyone has a role to play in creating a welcoming and inclusive atmosphere that promotes the success and well-being of our organization.

APPLICABILITY

All individuals associated with our organization, including but not limited to:

- Employees, whether full-time, part-time, or temporary.
- Contractors, consultants, and other third-party collaborators.
- Clients and customers engaging with our products or services.
- Visitors participating in events, conferences, or other activities organized by our organization.

This policy covers all interactions within our organization, including those conducted via online platforms, social media, email, and any other communication channels associated with our organization.

Violations of this policy may result in disciplinary action, including but not limited to warnings, probation, suspension, or termination, depending on the severity and recurrence of the violation.

CODE OF CONDUCT GUIDELINES

Ethical Business Practices

Adherence to all applicable laws and regulations. Avoidance of bribery, corruption, and any form of unethical conduct. Ensuring fair and transparent dealings with customers, partners, and competitors.

Customer Privacy and Data Protection

Commitment to safeguarding customer privacy and protecting their personal information. Compliance with data protection laws and regulations in all customer interactions and data management processes.

Diversity and Inclusion

Promotion of diversity and inclusion in the workplace, ensuring equal opportunities for all employees regardless of gender, race, ethnicity, or other characteristics. Creating an inclusive work culture that values and respects differences.

Health and Safety

Commitment to providing a safe and healthy work environment for all employees. Compliance with occupational health and safety regulations and the implementation of safety measures in all operations.

Fair Employment Practices

Non-discrimination in hiring, promotion, and compensation practices. Fair treatment of all employees, including providing opportunities for professional growth and development.

Intellectual Property Protection

Respect for intellectual property rights, including patents, copyrights, and trademarks. Avoidance of infringement on the intellectual property of others.

Ethical Conduct and Fair Dealing

Conduct all business activities with the highest standards of ethics and integrity. Engage in fair and honest dealings with customers, suppliers, partners, and competitors, fostering an atmosphere of trust in all business relationships. Avoid deceptive practices, conflicts of interest, and any actions that may compromise the company's commitment to ethical conduct.

Manager-Subordinate Relationship

Cultivate open communication, mutual respect, and fairness. Prohibit harassment and discrimination, ensuring performance evaluations are merit-based.

2. Corporate Policies & Directives

2.1 EMPLOYMENT

This section provides further details on employment. It should be read in conjunction with the Appointment Letter.

Induction and Training

To help an employee settle smoothly into the organization, detailed HR Induction and Process Training will be provided. HR Induction will assist in understanding the policies, guidelines, and procedures of the company.

While joining employee must sign and submit the following documents as a condition of their employment:

- Aadhar card copy
- Pan Card
- Address Proof (Present & Permanent)
- Relieving letter of previous organization
- Signed copy of the offer letter
- Declaration related to any other document proof not submitted while joining.
- EPF Passbook / details of EPF (Previous UAN, EPF, EPS member, etc. details)
- Declaration of Pan linked to Aadhar via email to be sent to Savita Thakur at s.thakur1@cloudextel.com
- Joining Form
- Gratuity Nomination Form F
- PF Declaration form 11
- Appointment Letter (Employment letter)

Probation and Confirmation

The performance of the employee will be reviewed during the probation period which is 60 days. If an extension is not granted, employment status will be automatically confirmed.

In cases where performance is not satisfactory, the probation period may be extended. While extending the probation, the concerned manager shall also indicate the new date of appraisal for confirmation. The probation can be extended for a maximum of three months.

Work Hours

While CloudExtel maintains flexible working hours, it is expected that everyone will be present in the office on time, i.e. latest by 10:00 am, unless with prior written approval for an exception or due to work commitments outside the office.

Excessive absenteeism or tardiness will not be tolerated and will be cause for disciplinary action.

Additionally, if an employee arrives in the office any day post 1:30 pm, that will be considered as a Half Day. For this kind of scenario, employees are expected to apply half day leave on HRMS.

In the event of emergencies, employees may opt for remote work (WFH) if they possess their official laptop. The decision to approve WFH rests with the Reporting Manager, allowing a maximum of two occurrences per month. If additional instances of WFH are necessary, the approval of the Head of Department (HOD) is required.

WFH Protocols:

- Attendance at all scheduled meetings is a crucial expectation from employees.
- Employees are urged to meet the specified work hours, ensuring completion of their tasks efficiently.
- Employees are expected to promptly respond to incoming emails and phone calls.

Working hours can be extended due to any work-related activity, if required. Emphasis is placed on completing the required work within the agreed timelines and priority should be given to this, independent of working hours. Any work outside normal working hours or working days will not bestow a right to the employee to be compensated with additional compensatory leaves.

All employees are required to mark their attendance, apply for leave, submit their investment declaration and proof via. HRMS only.

Dress Code

- Customer Facing: Business formals on weekdays and business semi-formals on Friday.
- Non-Customer Facing: Business semi-formals all week. Men must always wear shoes.

2.2 COMPENSATION

Employees' compensation is detailed in their employment agreement and paid monthly after standard deductions; increases are at the Company's discretion based on performance and other factors.

Salary Deposit

Salaries are directly deposited into employee accounts and are paid by the last day of the month or the next working day if it's a holiday.

Advances

Salary advances are only given in special cases, like medical emergencies. The advance can be up to 50% of your monthly gross.

Employees should send their advance request email to HR at least two weeks in advance, and it must be approved by their manager, HOD, and Head HR.

For other advances (like buying supplies or client entertainment), get approval from your Reporting Manager and HOD first.

You won't get a new advance until the previous one is settled, unless you have special permission from your department head and HR Head. If the advance isn't settled within a month, it will be deducted from your next month's salary automatically, without any extra notice.

Deductions

The Company reserves the right at any time during their employment, or on termination of employment to deduct from salary any overpayment made and/or money owed to the Company by an employee. Including and not limiting to sum of money for any excess holiday / leaves, outstanding loans, advances, relocation cost, missing assets, etc.

2.3 REIMBURSEMENT POLICY

Employees' compensation is detailed in their employment agreement and paid monthly after standard deductions; increases are at the Company's discretion based on performance and other factors.

Objective

Reimbursement policy is a structured framework that outlines the procedures, guidelines, and rules for employees seeking reimbursement for legitimate business expenses they incur on behalf of the company. This policy serves as a crucial document that delineates the expectations, processes, and boundaries of employee-initiated expenses.

Applicability

The policy is applicable to all On-roll employees in following ways:

Eligibility (On Roll Employee)	Applicable Reimbursement	
GM & Above	✦ Car Reimbursement ✦ Meal Coupons (WIP) ✦ Uniform Reimbursement	✦ Books & Periodicals Allowance ✦ Internet Reimbursement ✦ Annual Gift Card Reimbursement
Below GM	✦ Meal Coupons (WIP) ✦ Uniform Reimbursement ✦ Books & Periodicals Allowance	✦ Internet Reimbursement ✦ Annual Gift Card Reimbursement

Car Reimbursement

Employees with designation GM & above only are eligible for car reimbursements as a part of their CTC. For details kindly refer the Reimbursement Policy.

Internet Reimbursement

For reimbursement eligibility, the internet connection must be registered in the employee's name or that of a family member. When claiming reimbursements, employees are required to submit their internet bills as supporting documents. Reimbursement is applicable on the actual bill amount, adhering to the company's policy, with a maximum cap set at INR 30,000 per annum.

Uniform Reimbursement

The reimbursement is granted based on the bills submitted by employees, covering the actual expenses incurred. As per Section 10(14)(ii) of the Income Tax Act, the total expenditure on purchasing uniforms for official purposes is eligible for deduction, with a maximum cap as per the company's policy set at INR 15,000 per annum.

Books & Periodicals Allowances

This allowance covers the reimbursement of expenses incurred by employees for newspaper and magazine subscriptions. The company's policy sets a maximum cap of INR 15,000 per annum for this allowance.
Tax exemption: As per law, same is exempted up to actual bill amount.

Meal Coupons

For Meal Benefit, the load value will be 2,200/- per month (26,400/- in an annual year). By incorporating 'Meal Allowance' as a designated component in the compensation structure for registered employees, the Company not only streamlines access to free food and beverages but also provides a tax-free benefit to enhance the overall compensation package (Work in progress).

Gift Card

If an employee selects a gift card, the Company extends an annual gift card valued at INR 5,000, completely exempt from tax implications. These gift cards are treated as cash equivalents, irrespective of their specific nature.

Mobile Bill Reimbursement

For all employees, flat 50% of their total mobile bill will be reimbursed monthly. For senior management i.e., AVP and above a flat 80% of their total mobile bill will be reimbursed monthly. (Claim Form attached in Annexure). Note that claims for family plans will not be accepted; only one connection per employee is eligible for reimbursement. Additionally, OTT-related charges are not covered.

Process

- Share Claim form via email to Reporting Manager and HOD and take approval on the same.
- Share this approval mail along with supporting documents to the Finance department for getting the amount reimbursed as per eligibility.

2.4 PROVIDENT FUND

- Employees eligible for EPF and EPS are recommended to join the schemes as per the Employee Provident Funds Act, 1952.
- Both the employee and the Company contribute to EPF, and employees receive a lump sum with interest upon retirement.
- Employees must provide details to join EPF & EPS and nominate a beneficiary for the funds in case of death.
- Employees transferring from another company should move their past PF balance to the new account using their Universal Account Number (UAN).
- UAN, given by EPFO, consolidates employee IDs from various jobs into one platform.

2.5 STATUTORY DEDUCTIONS

- All required deductions (like Provident Fund, Professional Tax, TDS, ESIC) will be made from employee payments according to current government rules.
- Employees must provide valid proof of any tax-saving investments or schemes. If they don't submit this proof on time, the Company will deduct taxes as required by law without prior notice.
- Employees will get a statement showing details of their gross pay, deductions, and net pay.

2.6 GRATUITY / EX-GRATIA

Gratuity will be provided in accordance with the Payment of Gratuity Act, 1972.

Additionally, as a special benefit, the company will offer an ex-gratia payment on a pro-rata basis even if you before completing the mandatory gratuity period. This is part of the generous compensation package outlined in your offer letter.

2.7 LEAVE POLICY

Employees are entitled to 12 days of paid holidays annually, as outlined in the ETIPL/NSPL Holiday List, which is provided at the beginning of each calendar year.

In addition, employees accrue a total of 30 days of leave per year, at a rate of 2.5 days per month. Leave is credited on a pro-rata basis at the end of each month.

Employees are eligible to encash 10 unused leave days and carry forward a maximum of 10 days to the following year. Any remaining leave days beyond this will be forfeited. And the same rule will be taken into consideration for calculation of FNF i.e. 10 days leave are eligible to be encashed on a pro-rata basis of that Fiscal Year.

Leave requests must be submitted through Pulse HRM and are subject to approval by the reporting manager. During the notice period, employees are not permitted to take any leave (except exceptional circumstances).

Adoption Leave

Female employees on the adoption of a child may be granted leave up to 30 days subject to age of the adopted child. During adoption leave, leave salary equal to last pay drawn is admissible. The C reporting manager must approve all such leave.

Maternity Leave

The Company will provide maternity leave to eligible female employees in accordance with the Maternity Benefits Act, 1961. Female employees are entitled to up to 26 weeks of maternity leave for their first two children.

Maternity Leave is a separate leave taken over and above the other leaves permissible to the female employee. During maternity leave, leave salary equal to last drawn pay is admissible. PLI for the period of maternity leave will be paid at 100%, and performance rating applied to the balance months of the FY for purposes of evaluation of final PLI payment amount.

If less than 26 weeks of leave is taken, the remaining leave can be used within one year of returning to full-time work. Additionally, maternity leave may be extended by up to 4 weeks at half pay if there is a documented medical reason for the extension.

Female employees are also entitled to 30 days of leave in the event of a miscarriage.

Paternity Leave

Male employees are eligible for 10 days paid paternity leave on below mentioned scenarios:

- Has a childbirth
- Legally adopts a child and becomes an adoptive father.
- Commissioning father

Birthday Leave

Birthday Leave allows employees to take one day off each financial year to celebrate their birthday, emphasizing work-life balance and recognizing special moments.

Eligibility: Available to both on-roll and off-roll employees.

- Employees are entitled to one Birthday Leave per financial year, which must be taken during the month of their birthday.
- This leave is an extra benefit beyond the standard leave policy.
- Birthday **Leave** cannot be carried forward or encashed.

Unscheduled Leaves

If there is no available leave balance, any additional leave taken beyond the entitled leave will be categorized as Leave Without Pay (LWP).

Bereavement Leave

Employees are eligible for 10 working days of bereavement leave. This leave is available immediately upon the death of a close family member or a loved one.

For the purposes of this policy, close family includes only parents, parents-in-law, immediate sibling, spouse, or children.

Employees are required to submit a death certificate upon resuming work.

2.8 MEDICAL INSURANCE POLICY

As part of our commitment to employee well-being, all employees are covered by our comprehensive Medical & Accidental Insurance plan from the day they join the organization. This insurance ensures that our employees and their families have access to quality healthcare, promoting a secure and healthy work environment.

Under the Group Medical Coverage (GMC), on-roll employees receive coverage up to INR 5 Lakhs for self, spouse, and two children. For off-roll employees, the coverage is INR 2 Lakhs for self only.

Under Group Personal Accidental (GPA) policy provides varying coverage based on job roles.

2.9 RELOCATION POLICY

Our Relocation Policy outlines allowances for travel, household goods transportation, and accommodation based on employee grades. For detailed information, please refer to the separate policy document.

This policy applies to existing staff. For new hires, relocation benefits will be determined based on the offer letter and relocation approval from management.

2.10 TRAVEL EXPENSES

Outstation Travel Expenses

Employees will be reimbursed for outstation travel related expenses incurred while on business meetings.

The following applies to all outstation travel within India that involves an overnight stay. Employees are required to submit bills for reimbursement, which will be processed based on actual expenses. Only GST-compliant invoices will be accepted. This policy covers hotel stays, meals, and local transportation.

City Type	Travel Expenses Off Roll	Travel Expenses ON Roll (upto DGM Level)
Metro	4000	6000
Capital	2500	5000
Others	2500	4000

Metro Cities Mumbai, Delhi, NCR, Bengaluru, Chennai, Hyderabad & Kolkata

Capital Cities Capital Cities of States

Other Cities Towns other than Capital cities of states

Travel Expenses for GM & above is based on actual expenses incurred

Note :

- The limits specified represent the maximum permissible expenses. Reimbursements will be based on actual expenses and the bills submitted.
- All outstation travel costs, including hotels, tickets, visas, and client-related expenses, must be approved by the employee's reporting manager prior to incurring the costs. Hotel invoices should be issued in the Company's name, including the appropriate GST number/code.

Process

- When an employee travels for business purposes, he/she needs to take a formal approval of their travel over mail from their reporting manager.
- For reimbursement, employees need to share Claim form (OPE Claim Form attached in Annexure) via email to Reporting Manager and HOD and take approval on the same.
- Share this approval mail along with supporting documents to the Finance department for getting the amount reimbursed.

Local Conveyance

Use of Personal Vehicle for Local Conveyance: -The Company has a policy of allowing employees to use personal vehicle for local duty in their 'Duty Station.' The entitlements are given below. These entitlements are for local duties only in their 'Home station' and should not be mixed with tour entitlement.

The reimbursement rates for use of own vehicle are mentioned here 👉

Mode of transport	Entitlements
2 Wheeler	Rs 5/km
4 Wheeler	Rs 8/km

For expenses in taxi/auto services, any expense above Rs 250 requires a receipt or photo of the meter at the completion of the journey in case a bill is not available.

The above claims must be made along with log of origin, destination, and purpose, duly approved by the Reporting Manager before being submitted to the Finance department. The rates shall be revised from time to time, based on fuel prices prevalent.

All Expense Claim Forms with the relevant supporting documents attached need to be approved by the reporting manager and then should be submitted to the Finance department not later than the 25th of the month.

All Expense Claims need to be submitted within One months of the expenses incurred. Claims submitted later than one months will not be accepted or processed.

Employees need to coordinate with the Finance department and maintain a record of their reimbursements at their end. Expense Claims submitted to the Finance Dept. will be checked & processed, and will be paid within 10 days, post satisfactorily solving any queries.

Abroad Travel

Employees travelling out of India shall be eligible for reimbursement expenses of:

- Stay
- Meal
- Hotel
- Local Travel

Reimbursement for the aforementioned expenses will be processed upon submission of valid receipts, subject to approval from the respective Heads of Departments (HODs) and the Chief Executive Officer (CEO).

2.11 EMPLOYEE REFERRAL PROGRAM

To encourage and reward employees for referring qualified candidates for open positions, we offer the following incentives.

If a referred candidate is hired and completes the specified tenure, the referring employee will receive the following referral bonus:

Position	On-roll/ Off-roll	Grade	Candidate Tenure completion period	Referral Bonus
SVP	On-roll	Band 1A	90 Days	70,000
AVP, VP	On-roll	Band 1B	90 Days	70,000
Senior GM, GM	On-roll	Band 2A	90 Days	70,000
AGM, DGM	On-roll	Band 2B	90 Days	50,000
Senior Manager	On-roll	Band 3A	90 Days	25,000
Asst Manager, Manager	On-roll	Band 3B	90 Days	15,000
Senior Executive, Sr Officer	On-roll	Band 4A	90 Days	12,000
Assistant, Executive, Officer	On-roll	Band 4B	90 Days	10,000

The payment will be processed once the referred candidate has completed the specified tenure period from their date of joining.

Please note that Senior Management (i.e., GM and above), HR and Hiring managers directly involved in the selection process are not eligible for the Employee Referral Program.

2.12 PERFORMANCE REVIEWS

Employees are expected to have a Goal setting exercise with their reporting manager and identify their Key Result Areas (KRAs). Based on the set KRAs annually, their performance will undergo a comprehensive review.

Ratings will be assigned in accordance with these KRAs. The final decision on their performance review will be a collaborative effort between their immediate manager and the Head of the Department (HOD).

Performance Linked Incentive (PLI)

Upon completion of the Probation Period and confirmation, the Employee will be eligible for an annual performance linked incentives (“PLI”) which is payable for a financial year.

The Employee shall be eligible for PLI only upon completion of at least 6 (six) months in a financial year. For example, an employee who joins on or before September 30 will be eligible for PLI in that financial year. Any employee joining after September 30, will not be eligible for PLI in that financial year but will be eligible for PLI in the next financial year. To be eligible for receiving the PLI, the Employee must be actively employed by the Company and not have resigned or be serving notice at the time of disbursal.

PLI is based on individual and Company’s performance, The disbursal of PLI is subject to management discretion.

Performance Improvement Plan (PIP)

Employees may be placed on a Performance Improvement Plan (PIP) if performance issues arise. At the end of the PIP period, performance will be reviewed.

- Satisfactory Performance: PIP ends, and the employee continues as usual.
- Unsatisfactory Performance: PIP may be extended, or employment may be terminated.

2.13 RESIGNATION

If an employee wishes to resign, they must formally notify their reporting manager, and the resignation should also be submitted through the Pulse HRMS Portal.

The employee is expected to serve the full notice period as specified in their appointment letter.

If the employee fails to serve the complete notice period as outlined in their contract, a pro-rata amount will be recovered based on the total monthly gross salary.

Exit Process

Prior to the employees last working day with CloudExtel, HR connects with the employee for exit interview. On the last day, employee is expected to do the following:

- To get sign off on the handover from the reporting manager.
- Submit all Claim forms with necessary approvals for reimbursement.
- Return company provided assets like ID card, visiting card, laptop or any other company related property which employee has to handover to their manager or to the HR.

Note Full and final settlement will be made within 45 working days.

2.14 RE-HIRE POLICY

Former employees who voluntarily resign and reapply within one year may be considered for rehire at their previous level and compensation, provided their qualifications and competencies align with the role.

For those reapplying after one year, rehiring decisions will be based on the Company's current policies. Compensation in these cases will be determined based on the position and the Company's established guidelines.

2.15 ANTI-BRIBERY AND ANTI CORRUPTION POLICY

Purpose

Our company is committed to conducting business with honesty, ethics, and professional integrity, maintaining a zero-tolerance stance towards bribery and corruption. The Company adopted the following policies in this regard:

Scope and Applicability

Covers various forms of bribery and corruption, including unauthorized gifts, discounts, political donations, and facilitation payments.
Complies with global anti-bribery laws such as the Indian PCA, U.S FCPA, and the UKBA.

Applicable to employees, with strict adherence required, subject to disciplinary actions and potential termination for violations.

Prohibited Activities

Our Company prohibits, directly or indirectly, engaging in Bribery and Corrupt Practices. Along with offering of Bribes by Company's Employees and / or Third Parties, this Policy also prohibits the receipt of a Bribe by, or for the benefit of, the Company's Employees and / or Third Parties. Personal funds may not be used to accomplish what is otherwise prohibited by this ABAC Policy.

The following are examples of Corrupt Practices which are prohibited under this Policy:

- Payments (other than those expressly required to be made under applicable laws) to secure licenses, permits, renewals, and any other required approvals or clearances in order to operate in an area, state, country or other jurisdiction.
- Payments to influence any act or decision of a Governmental Official or individual in the private sector in their official capacity; and
- Payments inducing a Government Official to use their influence with a Government Entity to affect or influence any act or decision of a Government Entity.

A payment that would otherwise be prohibited under this policy may be allowed where there is an imminent physical threat to their personal safety or where employees are coerced to make the payment. Any such payment must immediately be reported by them to the Company's Compliance Officer.

Common practices that could imply Bribery and Corruption

- Receiving and offering gifts and entertainment of value exceeding INR 2000.

  To assess if a gift or entertainment is acceptable, consider the following criteria:

  - It must not give rise to any actual, perceived or potential conflict of interest.
  - It must not improperly influence or encumber the independence of the recipient.
  - It must not be excessive, repetitive, or inappropriate.
  - It should be reasonable and consistent with customary business practices.
  - All gifts and entertainment offered and received must adhere to the Company's Supplier Code of Conduct (COC) and ABAC policy.

- Facilitation Payments or Kickbacks: Facilitation payments typically involve securing non-discretionary permits, licenses, customs clearances, entry or exit visas, or police protection, whether related to new or existing business operations.

- Use of Third Parties: All dealings with Third Parties shall be conducted with the highest standards of integrity and in compliance with all relevant laws and the ABAC Policy. Act of bribery by employees and/or through third parties, or tolerating such actions, jeopardizes the Company's interests and may lead to disciplinary action, termination of relationship, or imposition of liability.

- Contribution to political, charitable, and religious institutions:

  - Political contributions must always be for legitimate purposes and comply with local laws. Approval from the Board of Directors is required before making any political contributions.
  - Charitable or religious donations must be legal, ethical, and free of any expectation or inducement, to avoid violating anti-corruption laws. Background checks on charitable or religious organizations should be conducted to ensure they are not involved in illegal activities, such as money laundering or terrorism.

- Sponsorships: Any sponsorship must be for genuine business or charitable / religious objectives without any element of quid pro quo. Any such sponsorship must be transparent, duly approved by the CEO, properly documented, and duly reported.

- Conflict of Interest where employee has a relationship with a vendor or vice versa: Examples of conflicts of interest which are to be avoided include holding financial interest through shares or loans, directly or indirectly, including through relatives in:

  - A company to which business is given.
  - A company in which the Employee is involved in making a buy-out decision.
  - Directing business to a supplier managed by a relative or close friend.
  - Soliciting subcontractors and vendors for donation / advertisements to a charity, in which the Employee is involved.
  - Using Company facilities for personal purposes or for relative's business.
  - Taking a part-time job requiring the Employee to spend time, during normal working hours or using Company equipment in meeting personal responsibilities.
  - Employing or making a promotion decision about a relative.

Trainings

In order to combat ABAC risks and threats, regular training will be provided to all business units, which must be completed within the specified timeframe. Employees must not consider these programs as one-time events and should stay up to date by repeatedly undergoing training at regular intervals. Failure to comply without justification may lead to disciplinary action, including suspension or termination.

Reporting of Violations / Complaints

- Employees and/or Third Parties who are or become aware of or suspect any violation of this Policy and/ or anti-corruption laws are under an obligation to report their concerns to the Chairperson of our Audit Committee as soon as it comes to their knowledge. Such reporting can be done in accordance with the Whistleblower Policy of our Company.
- If he/she is unsure whether a particular act constitutes Bribery or Corruption or if he/she has any other queries, these should be raised with the respective reporting manager and the Compliance Officer at the following email address grievance@cloudextel.com
- No Employee and/or Third Party who in good faith, reports a violation of the ABAC Policy shall suffer harassment, retaliation, or adverse employment consequences.

Responsibilities and Penalties

Any violation of the ABAC Policy will be treated as a serious offense, leading to disciplinary action, including suspension / termination of employment / contractual terms, consistent with applicable laws.

Bribery is a criminal act, and individuals found guilty, whether directly or by assisting others, will face personal liability. Punishments can include imprisonment (3 to 7 years under the Prevention of Corruption Act, 1988) and significant fines, which the Company will not cover.

2.16 ANTI CHILD LABOUR POLICY

Objective

At CloudExtel, we are dedicated to promoting the well-being and empowerment of minors. Our policy reflects our commitment to ensuring that our Company, including its subsidiaries and all associated vendors, strictly adheres to legal standards and prioritizes the welfare of children.

Child Labour refers to the work that deprives children of their childhood, their potential and their dignity, and that is harmful to physical and mental development. Child labour is a violation of fundamental human rights and has been shown to hinder children's development, potentially leading to lifelong physical or psychological damage.

Violations of this policy will result in appropriate disciplinary action, which may include termination of employment, contract termination, or legal action as deemed necessary.

Principles

- **Compliance with Laws:** Our organization will comply with all applicable laws and regulations including prohibition of child labour, human slavery, and trafficking, including minimum age requirements for employment.
- **Applicable laws:** Minimum Age Convention, 1973 (No. 138) and Worst Forms of Child Labour Convention, 1999 (No. 182) and Child and Adolescent Labour (Prohibition & Regulation) Act, 1986
- **Verification and Documentation:** The company will implement procedures to verify the age of all employees and maintain accurate and up-to-date employment records.
- **No Exploitation:** Company will not engage in or support any form of forced or compulsory labour, and employees will not be subject to exploitative working conditions.

- **Supplier Due Diligence:** The Company will conduct due diligence on suppliers to ensure they adhere to similar child labour policies. CloudExtel shall ask for undertaking on non-involvement in child labour from our suppliers / contractors. If in doubt / as required, the Company will monitor their employment practices through surveys, site visits, and audits.
- **Education and Awareness:** We are committed to raising awareness among employees and suppliers about the importance of preventing child labour and providing information on relevant laws and regulations.
- **Remediation:** In the event of any identified violation of this policy, the Company will take immediate corrective action, working with suppliers to implement remediation plans. However, if there is no positive impact observed in the employment practices of contractors / suppliers and others; the Company must terminate the business dealings with such offending suppliers / contractors.
- **Reporting Mechanism:** Employees are encouraged to report any concerns related to child labour through the established reporting mechanisms within the Company without fear of retaliation.

2.17 ANTI FORCED LABOUR POLICY

CloudExtel will uphold the elimination of all forms of forced and compulsory labour.

Definition

As per the ILO Forced Labour Convention, 1930 (No. 29), forced or compulsory labour is any work or service that is exacted from any person under the menace of any penalty, and for which that person has not offered himself or herself voluntarily. Providing wages or other compensation to a worker does not necessarily indicate that the labour is not forced or compulsory. By right, labour should be freely given, and employees should be free to leave in accordance with established rules. The ILO Forced Labour Protocol (Article 1(3)) explicitly reaffirms this definition.

This definition consists of three elements:

- Work or service refers to all types of work occurring in any activity, industry, or sector including in the informal economy.
- Menace of any penalty refers to a wide range of penalties used to compel someone to work.
- Involuntariness: The terms “offered voluntarily” refer to the free and informed consent of a worker to take a job and his or her freedom to leave at any time. This is not the case for example when an employer or recruiter makes false promises so that a worker takes a job he or she would not otherwise have accepted.

Actions and Implementation

- The Company will not make use of slave, forced, or compulsory labour in any form.
- The Company will ensure that employees are free to resign.
- The Company will ensure that working hours for workers do not exceed the maximum number as per the national law or withhold wages.
- The Company will ensure that the employees will not be subjected to work more overtime than is allowed under national law.
- The Company will ensure the contractors, suppliers, and others with whom the Company have a substantial involvement are strongly aware of the standards, which the Company expect from them.
- The Company shall ask for undertaking on non-involvement in forced labour from our suppliers / contractors. If in doubt / as required, the Company will monitor their employment practices through surveys, site visits and audits.

- The Company may opt for a strategy of constructive engagement with offending suppliers, rather than simply terminating contracts with them. However, if there is no positive impact observed in the employment practices of contractors / suppliers and others; Company must terminate the business dealings with such offending suppliers / contractors.

2.18 PREVENTION OF SEXUAL HARASSMENT (POSH) POLICY

Policy Statement

Our organization is committed to providing a workplace free from sexual harassment. We believe in fostering an environment where all employees, irrespective of their gender, feel respected, valued, and safe. This Prevention of Sexual Harassment (POSH) Policy outlines our commitment to preventing and addressing incidents of sexual harassment.

Applicability

This policy applies to all employees, contractors, vendors, clients, and any other individuals associated with the organization. It covers all locations and situations where work-related activities take place, including but not limited to offices, meetings, business trips, and company-sponsored events.

Definition of Sexual Harassment

Sexual harassment includes, but is not limited to, unwelcome sexual advances, requests for sexual favours, and other verbal or physical conduct of a sexual nature that creates an intimidating, hostile, or offensive work environment.

Prohibited Conduct

Unwelcome sexual advances or propositions:

- Requests for sexual favours in exchange for employment benefits.
- Display of offensive materials of a sexual nature.
- Any form of verbal or physical conduct of a sexual nature.
- Retaliation against those reporting incidents of sexual harassment.

Internal Complaints Committee (ICC)

The Internal Complaints Committee (ICC) at our organization is a dedicated internal body responsible for receiving and addressing complaints related to sexual harassment in the workplace. As mandated by law, the ICC comprises a minimum of four members who play a crucial role in ensuring a safe and respectful work environment.

Reporting Mechanism

Employees are encouraged to report incidents of sexual harassment to the ICC by sending an email to **icc@cloudextel.com** or may reach below ICC members: -

Presiding office	**Shubha S. Karra**	VP - General Counsel
Member	**Richa Gaur**	Senior General Manager – CEO's Office
Member	**Shashank Goenka**	Vice President – BD & Sales
Member	**Rahul Nair**	Vice President – HR & Admin
External Member	**Kanisha Vora**	

Confidentiality

The organization is committed to maintaining confidentiality to the extent permitted by law during the investigation process. Every effort will be made to protect the privacy of all parties involved.

Prevention and Awareness

Our organization is committed to preventing sexual harassment through training programs, awareness campaigns, and regular communication on appropriate workplace behavior. Employees are encouraged to participate in training sessions to understand their rights and responsibilities.

2.19 WORKPLACE HEALTH, SAFETY, AND ENVIRONMENT POLICY (WHSE)

- **Introduction:** Our organization, as a responsible and environment-conscious company, is committed to upholding the highest standards of Workplace Health, Safety, and Environment (WHSE) in our business activities. This policy serves as a foundation for creating a safe, sustainable, and environment friendly workplace.
- **Core Values:** WHSE is a core value at our organization. We strive to contribute to the preservation of nature and maintain responsible behaviour toward the environment. Safety and Health are paramount, reflecting our commitment to the well-being of our employees, associates, and partners.
- **Environmental Commitment:** Our organization is dedicated to preserving the environment. We will integrate environment friendly practices into our business activities and contribute positively to the communities where we operate.
- **Safety and Health Commitment:** The safety and health of our employees, associates, and partners are of utmost importance. Our organization is committed to creating and maintaining a safe and healthy workplace.
- **Adherence to Standards:** All employees are expected to follow the WHSE framework and always demonstrate safe behaviour. This includes maintaining a clean and organized workspace, complying with safety and health requirements, and adhering to policies and instructions communicated from time to time.
- **Competence and Training:** Employees should only undertake work for which they are trained and competent. Our organization will ensure to provide necessary training required to perform specific risky tasks like work at height, electrical work, excavation etc. as identified during the Hazard Identification and Risk Assessment (HIRA). Risk assessments and hazard identification will be conducted systematically to identify, reduce, and eliminate hazards in our operations.

- **Emergency Preparedness:** Employees must be aware of emergency procedures and know how to respond in case of workplace emergencies. Our organization is committed to providing appropriate health and safety information and training to all employees and partners. (refer SOP for Emergency preparedness and response plan).
- **Compliance:** Our organization expects all employees and business partners to comply with the WHSE policies and procedures of the company. This includes ensuring that partners are aligned with our commitment to safety and environmental responsibility.
- **Incident Reporting:** All incidents must be reported immediately. Employees are encouraged to act persistently to prevent unsafe acts or conditions. This reporting is crucial for continuous improvement in our safety and health practices with the learnings incorporated from all reported incidents, near miss (refer Incident investigation and reporting SOP).
- **Review and Improvement:** This policy, subsequent Standard Operating Procedures (SOPs) and relevant checklists will be periodically reviewed and updated to ensure its effectiveness and relevance. Continuous improvement will be pursued through feedback, incident analysis, and emerging best practices in WHSE across the organization and industry.
- **Communication:** We will communicate WHSE policies, procedures, and updates to all employees regularly. Open lines of communication will be maintained to address concerns and suggestions from the workforce and partners.
- **Responsibilities:** All levels of management are responsible for implementing and enforcing this policy. Each employee has a responsibility to contribute to a safe, healthy, and environmentally conscious workplace for everyone associated with the company directly or indirectly.

2.20 WHISTLE BLOWER POLICY

Objective

To encourage all the employees as well as stakeholders of the Company to disclose and freely communicate their concerns or complaints regarding any kind of misuse of our Company's properties, wrongful conduct including unlawful or unethical behaviour, actual or suspected fraud, misuse or abuse of authority or violation of our Company's code of conduct, without fear of retaliation of any kind with a view to build and strengthen a culture of transparency and good corporate governance in the organization.

Applicability

This Policy is applicable to our Company's Stakeholders which include:

- Employees (including permanent, off-roll, temporary and contract employees, key managerial personnel, trainees and interns)
- Directors
- Channel partners, suppliers, vendors, consultants, customers and any other third- party representatives of the Company.
- This Policy is also applicable to the Company's branch offices across India.

Incidents that may be reported

- A Whistleblower may report any unethical behaviour, wrongful conduct or illegitimate acts at the workplace. Given below is an illustrative list for reference:
- Any breach of law, rules, regulations, circulars, directives, notifications, guidelines, or policies as notified by the Government of India from time to time, or
- Any non-compliance with the Company's policies, rules, procedures, code of conduct by whatever name called, or
- Any grave / gross misconduct including misappropriation, financial fraud of any nature, inaccurate financial reporting, dishonest or unethical behaviour including soliciting, accepting or offering a bribe, facilitation payments or other such benefits, corruption, pilferage or leaking of confidential / propriety information, conflict of interest, criminal breach of trust, misuse of authority, concurrent employment, criminal conduct, customer data – substantiated incidents of serious loss of customer data, misconduct by any vendor / supplier, human rights breaches including modern slavery or human trafficking, manipulation of data / key performance indicators, money laundering, negligence, cheating, forgery, engaging in any trade or business outside the scope of employment without the consent of the appropriate authority, drunkenness or riotous or disorderly behaviour or indulgence in betting or gambling or speculation, wilful damage or attempt to cause damage to the property of our Company or any of its customers which will affect the reputation of our Company.

Procedure

- All the Protected Disclosures should be addressed to the Chairperson of the Audit Committee of ETIPL. A Whistleblower can raise a concern in one of the manners prescribed below:
  - Sending an email addressed to grievance report id (grievance@cloudextel.com) or
  - Sending a letter in a sealed envelope marked "Confidential" to the below mentioned address. The letter can be typed or written in legible handwriting, preferably in English. A Whistleblower may use the template given below in annexure section for reporting a concern.
  - General Counsel & Compliance Officer, Excel Telesonic India Private Limited the Ruby, 11th Floor, AWFIS, 29 Senapati Bapat Marg, Dadar (West), Mumbai – 400028.
- Protected Disclosures should be factual and not speculative or in the nature of a conclusion and should contain as much specific information as possible to allow for proper assessment of the nature and extent of the concern. To the extent possible, following information should be covered in the Protected Disclosure:
  - Name of the employees and/or third-party Stakeholders, if any, allegedly involved in the matter.
  - The nature of improper conduct and when it occurred or is likely to occur.
  - Factual background concerning the matter in detail including allegations of wrongdoing by the Subject and any material to support the matters raised in the Protected Disclosure such as documents, emails, chats from messaging apps, recordings (audio or video) or the names of potential witnesses.

Anonymous Complaints

Whistleblower can choose to remain anonymous while making a Protected Disclosure, over the course of the investigation and after the investigation is finalized. No attempts will be made to ascertain Whistleblower's identity if they have requested to remain anonymous. An anonymous disclosure will be reviewed and assessed in the same way as if the Whistleblower had revealed their identity. However, in some cases not knowing Whistleblower's identity can have an adverse impact on the investigation, and it may also be difficult to offer the same level of practical support. Accordingly, it is encouraged to disclose the identity when making a Protected Disclosure but there is no obligation to do so.

3. INFORMATION TECHNOLOGY, SYSTEMS AND SECURITY

INFORMATION SECURITY POLICY OVERVIEW

As a company, we are committed to safeguarding the confidentiality, integrity, and availability of our information assets. Information security is not just the responsibility of our IT department but a shared duty across all employees and departments. The purpose of this policy is to ensure that we protect our data, systems, and networks from unauthorized access, breaches, and other security threats.

Key Objectives

- **Confidentiality:** Ensure that sensitive information is accessible only to those authorized to have access.
- **Integrity:** Protect information from being modified or tampered with by unauthorized individuals.
- **Availability:** Ensure that information and critical resources are available to authorized users when needed.

Employee Responsibilities

- **Adherence to Policies:** All employees must comply with the company's security policies and procedures.
- **Data Protection:** Employees must handle all company data with care, particularly sensitive information, and follow encryption and secure communication practices.
- **Access Control:** Employees should only access data and systems for which they have explicit authorization. Sharing of credentials is strictly prohibited.
- **Incident Reporting:** Any security breaches, suspicious activities, or violations must be reported immediately to the IT or security department.

Security Measures

- **Password Management:** Employees must follow best practices for password creation and management, including regular updates and the use of complex passwords.
- **Device Security:** All company-provided devices must be secured with passwords or biometrics. Personal devices used for work purposes must adhere to the same security standards.

- **Regular Training:** Employees will receive regular training on information security best practices, including recognizing phishing attempts, secure handling of data, and understanding the implications of social engineering attacks.

Continuous Improvement

Our Information Security Policy is regularly reviewed and updated to address emerging threats and incorporate new security technologies. We encourage all employees to stay informed about these updates and participate in ongoing training.

By following this policy, each employee plays a crucial role in protecting our company's information assets and ensuring our continued success.

3.1 EMPLOYEE DATA PRIVACY

The Company is committed to protecting the privacy and security of all personal information and complying with the privacy legislation within each jurisdiction in which we operate.

- In order to meet the regulatory and other obligations, we collect certain Personal Data of employees and process it to protect the interests of both the Company and its Employees including the following:

- Personal information like date of birth, age, marital status, birthplace, nationality, mother tongue.
- Contact information (e.g., name, address, telephone, and email address).
- Gender of the Employee.
- Caste and religion.
- Beneficiary information.
- Recruitment and selection information including skills and experience, qualifications, references, CV, and interview and assessment data.
- Previous employment records.
- Aadhar or other government-issued identity numbers.
- Photographs and signature copies.
- Emergency contact details.
- Access card entry details.
- Regulatory information including records of Employee registration with any applicable regulatory authority, regulated status including any criminal record or credit background checks which may be necessary, and any regulatory certificate and references.
- Remuneration information including Employee salary/hourly plan/contract pay/fees information as applicable, allowances, overtime, bonus, and commission plans. Other benefits include payment for leave, bank account details, grade, tax information, expense claims, and payment information.
- Leave and management information including attendance records, absence records, holiday dates, requests and approvals, and information related to annual leave or other special or statutory leave, details of incapacity, details of work impact and adjustments, manager, and Human Resources (HR) communications, Performance Improvement Plans (PIP) and return to work interviews.
- Monitoring information (to the extent authorized by applicable laws) including Closed Circuit Television (CCTV) footage, system and building login and access records, and download and print records.
- Call or meeting records, information captured by IT security programs and filters.

- The work output of Company's Employees, whether in paper record, computer files, or in any other storage format belongs to us, and that work output, and the tools used to generate work output, are always subject to review and monitoring by the Company.
- Health information including information about short - or long-term disabilities or illnesses that the Employee may share with the Company, particularly in relation to any leave of absence the Employee may need to take.
- The Company may collect the aforementioned information from the Employee directly, from Employee references, and other data sources. We may also collect information from third parties subject to the requirements of applicable law.
- When required by the law and otherwise reasonable, the Company gives Employees notification of the specific purpose for which it collects their personal information at or before the time of collection.
- Company uses the Employee personal information for internal business purposes, including establishing or managing the employment relationship with the Company. Examples include:
    - **To authenticate the Employee identity.**
    - **To determine eligibility for initial employment, including verifying references and qualifications.**
    - **To administer pay and benefits.**
    - **To process Employee work-related claims including worker compensation and insurance claims.**
    - **To establish training and development requirements.**
    - **To conduct performance reviews and determine performance requirements.**
    - **To assess qualifications for a particular job or task.**
    - **To gather evidence for disciplinary action or termination.**
    - **To identify a contact point in the event of an emergency.**
    - **To comply with applicable labour or other applicable laws.**
    - **To ensure Employee safety and confidential information of the Company.**
    - **For any other purposes that are required by the Company in connection with the employment with the Company.**
- Company uses appropriate technical and organizational security measures to protect the security of the Personal Data both online and offline including implementation of access controls, implementation of firewalls, network intrusion detection and use of anti-virus software.
- Despite our best effort it is pertinent to note that no system involving the transmission of information via the internet or electronic storage of data is completely secure and we cannot be held responsible for data breaches that occur outside of our reasonable control. We will, however, follow all applicable laws in the event a data breach occurs, including taking reasonable measures to mitigate any harm as well as notifying them of such breaches as soon as possible.
- The Employee will have the right to access the Personal Data and to correct, amend, or delete it if is inaccurate or has been processed in violation with our internal Privacy Policy, except when the burden or expense of providing access, correction, amendment, or deletion would be disproportionate to the risks to the privacy, or where the rights of other people would be violated. To exercise any of these rights, the Employee can contact the Company at the below at the information provided at the end of this handbook.

✦ If the Personal Data we collect, covered by our internal Privacy Policy, is to be used for any purpose materially different from the purpose described here or disclosed to a third party not acting as our agent, in a manner other than as disclosed here, we will always give the Employee an opportunity to opt-out of this materially different use or disclosure.

- We will keep the Employee Personal Data for as long as is needed to carry out the aforementioned purposes, or as otherwise required by law. This means we will keep the Personal Data until the end of employment with us, thereafter a reasonable period necessary to respond to any employment inquiries, deal with legal, tax, accounting, or administrative matters, or provide the Employee with ongoing pensions or other benefits.
- Where we have no continuing legitimate business need to process the Personal Data, we will either delete or anonymize it or, if this is not possible (for example the Personal Data has been stored in backup archives), then we will securely store their Personal Data and isolate it from any further processing until deletion is possible.

3.2 INTERNET USAGE & CYBERSECURITY

Our electronic communication systems are vital to the successful operation of the Company. Employees are expected to use these systems exclusively for business-related activities. The use of the internet for personal gain, entertainment, or any non-business-related purposes is strongly discouraged.

Personal Device Usage

Logging into Company accounts from personal devices (e.g., mobile phones, tablets, laptops) poses significant security risks. It is advised that employees refrain from accessing Company data on personal devices. If such access is unavoidable, employees must ensure their devices are secured with appropriate security measures.

Recommended Security Practices

Password Security: Employees must keep all electronic devices secure with strong, regularly updated passwords and the latest security features.

- **Safe Network Usage:** Always access Company accounts using secure, trusted networks.
- **Antivirus Software:** Regularly update antivirus software on all devices to protect against potential threats.
- **Device Protection:** Do not leave devices unprotected or exposed, particularly in public or unsecured environments.

Email and Communication Security

Emails are common vectors for scams and malware. If you are unsure whether an email or attachment is safe, contact the IT department for guidance.

Safe Email Practices

- Refrain from opening or clicking links or attachments in emails from unknown or untrusted sources.
- Verify that emails are from legitimate Company email addresses or reliable sources.
- Be vigilant for suspicious content, such as offers, unsolicited advice, or unexpected messages that could be phishing attempts.
- Use complex passwords incorporating upper- and lower-case letters, numbers, and symbols. Never share your credentials unless explicitly authorized by a supervisor.

Data Protection

Employees must avoid transferring personal data, including customer or employee confidential information, unless it is essential and in compliance with applicable data protection laws. Adherence to these laws is mandatory.

Remote Work Security

These cybersecurity guidelines and procedures must be strictly followed even when working remotely. Intentional or repeated violations, especially those that compromise Company security, may result in serious disciplinary action, including termination of employment.

3.3 LAPTOP POLICY

Policy objective

Our Laptop Policy is designed to ensure the effective management, usage, and security of laptops issued to employees, supporting them in their roles and responsibilities.

Eligibility

Laptops will be allocated based on job responsibilities, demonstrated need, and at the discretion of Management. Details regarding laptop allocation will be provided upon joining.

Terms and Conditions

Employees issued a laptop should adhere to the following terms and conditions:

- **Ownership:** The laptop remains the property of the Company and must be returned upon resignation or termination.
- **Care and Responsibility:** Employees are responsible for taking appropriate precautions to prevent damage, loss, or theft of the laptop.
- **Software Configuration:** Laptops will come with a standard suite of programs based on company software standards. Additional applications may be provided based on professional needs.
- **Long-Term Absences:** During any long-term absences (1 month or more), the laptop should be submitted to the systems administrator, unless approved otherwise by the Head of the Department.
- **Appropriate Use:** Personal games, entertainment software, inappropriate content, and personal finance software should not be downloaded onto company laptops.
- **Data Backup:** Employees should maintain monthly backups of their laptop data with assistance from the IT department to prevent data loss.
- **Security Updates:** Regular security updates and virus protection must be maintained on the laptop.
- **Device Management:** Laptops will be secured with device management software to protect the Company's intellectual property.
- **Loss or Damage:** Employees are responsible for the laptop's loss or damage if company policies for safeguarding are not followed. The cost of the laptop may be recovered if lost or damaged due to negligence.

3.4 PROTECTION & PROPER USE OF COMPANY'S ASSETS

- **Asset Management:** Employees may be entrusted with valuable assets to support their work. It is their responsibility to manage, use, maintain, and dispose of these assets properly.

- **Care and Compliance:** Assets should be treated with care and used in accordance with company policies. Employees will be liable for costs related to damage or loss due to negligence.
- **Personal Use:** Company assets should not be used for personal gain or purposes outside of company policies.
- **Laptop Damage:** If damage occurs due to employee negligence or misuse, repair costs will be recovered from the employee. In cases of irreparable damage, the full cost of the laptop may be recovered.
- **Eligibility Review:** The Company reserves the right to revoke laptop eligibility without prior notice.
- **Return Procedure:** Upon returning the laptop, employees must power it on in front of the System Administrator to confirm it is in working order.

Note The IT department will determine the market value of the laptop. HR will use this information to apply (if any) necessary salary deductions or process final settlements.

3.5 EMAIL USAGE POLICY

Email facilities are provided for formal business communication. This policy outlines the proper use of email and the maintenance of confidentiality.

Guidelines for Email Use:

- **Confidentiality:** Maintain the confidentiality of sensitive information in all email correspondence.
- **Backup:** Emails that need to be preserved should be backed up and stored offsite.
- **Personal Use:** Avoid using your official email for personal matters or external notifications from banks, credit card companies, mobile operators, etc.
- **Configuration:** Do not configure your official email on personal devices without IT department's approval.

Instructions for Safe and Professional Email Use:

- **Appropriate Content:** Do not send defamatory material, breach copyright or confidentiality, or share content that could harm the company's reputation.
- **Respect and Professionalism:** Avoid sending emails with gossip, offensive content, harassment, or personal relationships.
- **Access and Confidentiality:** Do not access the email records of others without management authorization.
- **Confidential Information:** Do not share company confidential information outside of the organization without proper authorization.

4. REVISIONS TO THE POLICY

As our business evolves, so do our processes and systems. Consequently, we reserve the right to interpret, amend, suspend, or cancel any part of our policies, procedures, and benefits, with or without prior notice.

We will keep all employees informed of these changes on a regular basis. Updates will be effective from the dates specified by the Company and may be applied retroactively if necessary. Once revised, these policies will supersede and replace all previous versions, including manuals and guidelines. Any amendments will be communicated via email and updated on the HRMS portal.

Please review the policies carefully. If you have any questions or suggestions, please email us at **hr@cloudextel.com** with the subject line: "Queries on Employee Handbook / Suggestions for Improvement." We value your input and will consider all valid suggestions for inclusion in the next edition of the Employee Handbook.

Directory

DISPLAY NAME	EMAIL ADDRESS
CloudExtel Accounts	ap@cloudextel.com
CloudExtel Auditors	auditors1@cloudextel.com
CloudExtel Careers	careers@cloudextel.com
CloudExtel Event Committee	eventcommittee@cloudextel.com
CloudExtel Grievance Redressal Team	grievance@cloudextel.com
CloudExtel HR	hr@cloudextel.com
CloudExtel IT Security	itsecurity@cloudextel.com
CloudExtel Legal	legal@cloudextel.com
CloudExtel Support Desk	itsupport@cloudextel.com
CloudExtel TeamSafety	TeamSafety@cloudextel.com

CloudExtel

+91 98671 51303

accounts@cloudextel.com

www.cloudextel.com

CloudExtel (Excel Telesonic India Pvt. Ltd.)
The Ruby, 11th Floor, AWFIS, Dadar (West), Mumbai,
Maharashtra - 400028