IT Security and Communication Policy

'Name of the Company' believes that having an acceptable communication policy decreases conflicts and misunderstandings. It also considers that organizations need to state distinctly the role and extent of electronic equipment's usage and facilities to prevent liabilities and trouble. IT usage and Communication Policy covers the provisions regarding the same.

Purpose

This policy defines the organization's anticipations has and manages the movement of communication both within and outside the organization.

It aims at assisting meaningful and essential communication for employee productivity and morale without constraining communication to prevent employees from feeling intimidated and powerless.

Scope

The policy applies to all employees of the company

Guiding Principles

'Name of the Company' acknowledges that active communication with various stakeholders, and the general public is and constitutional part of its Strategy. The following guidelines must be followed by the employee to achieve its overall goals for communications:

Only authorized persons shall have formal meetings with the external stakeholders through media engagements and press releases.

All the information must be sent through the appropriate and approved communication channels to 'Name of the Company's stakeholders in a punctual manner.

A turnaround of 'Number of days' working days shall apply to all the stakeholders' requests for information.

All the information circulated to the stakeholders shall be accurate, transparent, and open as possible. However, 'Name of the Company's confidentiality must be maintained.

All communication must be clear, compact, and intentional.

Regular feedback is received from all the 'Name of the Company's stakeholders to ensure better service delivery.

Guidelines for External Communication

The support and engagement of ‘Name of the Company’s external stakeholders are critical to its long-term success and are always sought after. All communication with the external stakeholders should support this supposition and aimed make the stakeholders feel caught up and not disoriented.

All external communication must be approved by ‘Formal Title of the Person’, through the ‘Formal Title of the Person’. All the communication with government representatives and transmission of other confidential information requires approval from ‘MD or CEO’.

All the presentations /materials used for external use must be reviewed by the ‘Formal Title of the Person’ before exposing these documents to the stakeholders. It includes presentations at meetings, seminars, conferences, etc. and the information uploaded.

Communication with media is has to be handled with the advanced levels of sensitivity and professionalism and must always be directed by ‘Formal Title of the Person’.

Guidelines for Internal Communications

'Name of the company's internal communication is targeted at all its internal stakeholders towards achieving its overall objectives.

Internal communication shall be handled by the teams responsible for such correspondence.

Communication between and amongst staff members must always be professional.

Staff members should be addressed by their first names (in case of oral communication) or by their initials (in written communication). Official letters must incorporate the full name of the staff member.

The use of nicknames or other names is strictly forbidden in written communication.

Disclosure of Confidential Information

‘Name of the Company’ is committed to providing timely, accurate, and complete disclosure of its necessary company information in an appropriate manner

‘Name of the Company’ strictly prohibits the disclosure of confidential information.

The employees **MUST** sign a Non-Disclosure and Confidentiality Agreement, and violation of the same is a legal offense.

Information Security and Monitoring Policy

Information Security and Monitoring Policy provide a merged set of security measures that must be consistently applied across ‘Name of the Company’ to guarantee a secured operating environment for its business operations.

This policy addresses the information security requirements of Confidentiality, Integrity, and Availability.

Electronic and Wireless Policy

‘Name of the Company’ has developed the electronic policy to maintain of our data and technology infrastructure’s safety.

The employees are advised by us to keep their personal and company issued electronic devices safely protected by passwords and equipped with upgraded anti-virus software.

The employees must only use secure networks to log in.

Cell Phone Policy

The cell phone policy applies to any instrument that can make or receive phone calls, leave messages, send text messages, surf the internet, download information and view, and respond to emails whether the device is owned personally or by the company.

The company owned cellphones need to be kept switched on during working hours, work-related travel, and other times particularly mentioned by the company.

The employees must **NOT** use cellphones in the following situations:

- While driving
- While operating equipment
- During office hours
- For long personal calls during office hours
- During meetings
- For recording the company’s confidential information.

Employees **CAN** use their cellphones for

- Making business-related calls
- Checking important messages
- Scheduling/Checking appointments
- Short personal calls

'Name of the Company' holds the right to supervise the employees for inappropriate and excessive cell phone usage.Disciplinary actions will be taken if the terms are breached by the employee.

Internet Usage Policy

The electronic communication system must be used solely to facilitate the business of the Company.

Employees are warned against using the internet for matters of personal advantage and entertainment.

Employees should further be aware that all the content created by them are not entitled to privacy and can be used by the company without prior notice.

Appropriate internet usage includes using the internet to complete assigned jobs and seek information for the same.

The employee's Internet usage will be considered inappropriate if the employee uses the internet for

- Uploading/ downloading obscene, illegal, or offensive material.
- Exposing company's confidential information to unauthorized entities.
- Invading other employees' privacy.
- Indulging in piracy.
- Visiting unsecured websites that threaten the safety of the computer network
- Hacking.

In case of breaching the terms of this policy, the employee would be eligible for disciplinary actions legal, or otherwise.