



# **Code of Conduct For Subexians**



## I N D E X

Subex Code of Ethics and Business Conduct.....	4
Code of Conduct for Prevention of Insider Trading .....	10
Subex Corporate Communications Policy.....	25
Subex Customer Interaction Code of Conduct.....	31
Data Security Policy.....	37
Subex Electronic Mail Policy .....	45
Subex provided Laptop / Desktop and Mobile Facility Usage .....	49

### Overview of our policies

#### **Policies**

- Subex code of ethics and business conduct
- Code of conduct for prevention of insider trading
- Subex Corporate Communications Policy
- Subex Customer interaction code of conduct
- Data protection policy
- Protection of assets policy
- Software compliance policy

#### **Applicability**

**These policies are applicable to Subex and its affiliates all over the world (“Subex”)**

#### **Who must follow Subex Policies?**

Our policies apply to all employees of Subex (“Subexians”) throughout the world. All Subexians should ensure that others representing Subex such as consultants, agents and independent contractors- agree to follow applicable Subex policies.

#### **Responsibility of all Subexians**

1. Have a basic understanding of all applicable policies
2. Seek assistance from your manager, legal counsel or other resources when you have questions about the application of the policies
3. Promptly report any concerns that you or others may have about possible violations of Subex policy

#### **Penalties for violation**

Subexians who violates the spirit or letter of these policies are subject to disciplinary action up to and including discharge. Many Subex polices can also mean violation of law and subjecting yourself and/or Subex to civil sanctions or criminal penalties.

## I. Subex Code of Ethics and Business Conduct

Subex believes that a key ingredient to achieving success in business is the requirement that all Subexians conduct themselves with basic honesty and integrity, in their interactions with the company, colleagues, customers, business partners, vendors and others. Ethical conduct is a core value at Subex. Our customers respect and admire us for the high standards we have set for ourselves in terms of the way we conduct ourselves in every business relationship. We count on Subexians to maintain and enhance that reputation. This Code of Business Conduct provides the guidelines for the essential comprehension and understanding of the responsibilities and obligations to comply with the law and these standards, and to provide feedback to the management of Subex on anything that is not in compliance with the law or these standards.

### Contents

1. Introduction
2. Requisite Obligations
3. Specific Obligations
4. Compliance with Laws, Rules and Regulations
5. Disciplinary Process and Committee
6. Whistle-Blowing Policy and Committee

### 1. Introduction

This Code of Business Conduct has been issued by Subex to deter wrong doing and to promote:

1. Ethical and honest conduct by Subex's Board of Directors and Subexians, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships.
2. Avoidance of conflicts of interest, including disclosure to an appropriate person of any material transaction or relationship that reasonably could be expected to give rise to such a conflict.
3. Full, fair, accurate, timely, and understandable disclosure in reports and documents that Subex files with, or submits to the Regulatory Bodies/ Stock Exchanges, its shareholders and in other public communications made by Subex.
4. Compliance with all other applicable laws, rules, and regulations.
5. Prompt internal reporting of any violations of this Code of Business Conduct.
6. Accountability for adherence to the Code of Business Conduct.

Subex expects all Directors and Subexians worldwide to comply with the following standards of business conduct. Subex is committed to take prompt and impartial action against violations of these policies. Violation of the standards outlined in these guidelines may be grounds for disciplinary action up to and including termination of employment or other business relationship. Subexians and directors who are aware of any misconduct, illegal activities, fraud, abuse of Subex's assets or violations of the standards outlined in these guidelines are responsible for reporting such matters.

### 2. Requisite Obligations

Subex's standards expect from Subexians, the following shared responsibilities. It is your responsibility to;

1. Conduct Subex's business in compliance with, applicable laws, rules and regulations and Subex's policies, including this Code of Business Conduct
2. Treat all Subexians, customers and business partners in an honest and fair manner
3. Avoid situations where your personal interests are in conflict with that of Subex's

4. Proper use of Subex's proprietary and confidential information, assets and resources, as well as those of Subex's customers and business partners.

5. Raise any concern that you or others may have about possible violations of this Code of Business Conduct, laws or the Company's policies. You may,

- a) Raise your concerns with your manager, or
- b) Raise your concerns with company's Compliance Officer, Ramanathan J

All concerns raised will be presented to the Company's Board of Directors on a timely basis pursuant to the procedures established by the Ethics Committee of the Board of Directors.

6. Subexian's are obliged to familiarise themselves with security and business continuity policies, procedures and plans as these relate to Subex's core business and the businesses of the customers that Subex supports.

Individuals have a role to play in compliance to security and business continuity requirements and failure to so do can result in disciplinary action.

### 3. Specific Obligations

#### a) Policy against Retaliation

Subex prohibits any director or Subexian from retaliating or taking adverse action against anyone for raising suspected conduct violations or helping to resolve a conduct concern. Any individual who has been found to have engaged in retaliation against a director or a Subexian for raising, in good faith, a conduct concern or for participating in the investigation of such a concern may be subject to discipline, up to and including termination of employment or other business relationship. If any individual believes he or she has been subjected to such retaliation, that person is encouraged to report the situation as soon as possible to their reporting manager or Subex's Compliance Officer.

#### b) Equal opportunities employer

Subex is committed to equal employment opportunities, a basic goal of free society. By continuing to extend equal opportunity and provide fair treatment to all employees on the basis of merit, we will improve Subex's success while enhancing the progress of individuals and the communities where our businesses are located.

Subex will

- Use merit, qualifications and job related criteria as sole bases for all employment-related decisions affecting employees.
- Recruit, hire, train, compensate, promote and provide other conditions of employment without regard to a person's race, colour, religion, national origin, sex, age disability, veteran status or other characteristic protected by law.
- Provide a work free environment free of harassment of any kind based on diverse human characteristics and cultural back grounds.

#### c) Work Environment

The Subex work environment must be free from discrimination and harassment based on race, caste, creed, religion, gender, sexual orientation, age, national origin, disability, marital status, or other factors that are not related to Subex's business interests. Other activities that are prohibited because they are not conducive to a good work environment include,

- a) Physical harm or threats of physical harm
- b) Violent behavior
- c) Possession of weapons of any type
- d) Use, distribution, sale, or possession on Subex's premises of illegal drugs or any other controlled substance, except medicines for approved medical purposes.



## - Code of Conduct for Subexians

- e) Consumption of alcohol on Subex premises when not at a company sponsored function
- f) Sexual Harassment

Sexual harassment is defined as any form of conduct that a prudent person would find offensive - whether physical (direct or indirect), verbal (express or implied) or environmental. It includes unwelcome sexual advances, requests for sexual favors and other verbal or physical conduct of a sexual nature when one of the following applies.

- Submission to such conduct is made either explicitly or implicitly - term or condition for an individual's career growth or opportunities.
- Submission to or rejection of such conduct by an individual is used as the basis for decisions affecting that individual's career and feelings.
- Such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or of creating an intimidating, hostile or offensive working environment.

The concept of sexual harassment is extremely broad, covering anything that a person who is not hypersensitive finds it offensive – words, magazine pictures, messages, conduct, touching or looking.

There are two forms of sexual harassment viz., quid pro quo (one thing in return for another) and hostile environment. Quid pro quo harassment is the exchange of sexual favors for career benefits. The following three elements must exist for the complainant to be successful.

- Complainant was subjected to unwelcome sexual harassment in the form of sexual advances or requests for sexual favors.
- Harassment complained of was based on sex.
- Submission to the unwelcome advances was an express or implied condition for receiving some form of career benefits, or refusal to submit to sexual demands resulted in a tangible job detriment.

Hostile environment is the creation of an offensive working environment. The fact that the victim voluntarily submitted to the harassment is not a defense and the issue is whether the conduct was welcome or unwelcome.

### **d) Conflicts of Interest**

Subexians may take part in legitimate financial, business and other activities outside their jobs. Those activities, however, must be free of conflicts with their duties and responsibilities at Subex. A "conflict of interest" may occur when an individual's private interest interferes/ appears to interfere, in any way with the interests of the company as a whole. A conflict situation may arise when a Subexian takes action or has interests that may make it difficult to perform his or her company work objectively and effectively, or that interfere with that person's judgment in the course of his or her job at Subex. Conflicts of interest may also arise when an employee, or a member of his or her family, receives improper personal benefits as a result of his or her position in the company.

### **e) Confidentiality**

You are permitted to use and disclose proprietary and/or confidential information only as authorized and in accordance of Subex's business. In addition, you are responsible for making use of adequate safeguards to prevent the disclosure or loss of proprietary and/ or confidential information. Such confidential information should be stored only on computers or storage media owned or maintained by Subex. Such confidential information should not be downloaded to or stored on an employee's personal computer or removable media.

Confidential information includes all non-public information that might be of use to competitors, or harmful to the company or its customers, if disclosed. A Subexian must also maintain the confidentiality of third party information that Subex has agreed to maintain confidential to the extent of any such confidentiality or nondisclosure agreement. A Subexian's obligation to protect Subex proprietary and confidential information



## - Code of Conduct for Subexians

exists whether or not the information is explicitly labeled or otherwise designated as being proprietary or confidential, and the obligation continues even after leaving the company.

One of Subex's most valuable assets is its intellectual property - patents, trademarks, copyrights and other proprietary information. It is Subex's policy to establish, protect, maintain and defend its rights in all commercially significant intellectual property and to use those rights in responsible ways. You must take steps to safeguard these assets regardless of whether they are labeled as proprietary or confidential, contain a copyright notice, or otherwise are explicitly designated as constituting important intellectual property of the Company.

In addition to protecting Subex's intellectual property rights, Subex respects the intellectual property rights of others. Unauthorized use of the intellectual property rights of others may expose Subex to liability. To avoid the risk of misusing a third party's confidential information (such as information from customers, vendors, service providers or business partners), you must not, directly or indirectly, loan, copy, download or distribute such information or disclose such information to any unauthorized persons (whether or not employed by Subex) unless you do so in accordance with the terms that have been formally agreed to by Subex and such third party. To avoid violating the law and/or licensing requirements of third parties, as well as to minimize the risk of computer viruses, you should take special care when acquiring software (which includes computer programs, databases and related documentation) from third parties. This applies both to purchased software and to software that is made available without charge, via the Internet. The terms and conditions of software license agreements – such as provisions not to copy or distribute programs - must be reviewed and followed. In no event should you copy any such software, especially any software constituting "open source code" into any development work you do for Subex unless Subex permits such usage explicitly.

### **f) Conducting Subex's Business**

- a) Never make oral or written misrepresentations or dishonest or misleading statements to anyone.
- b) Never make false entries in Subex's business records. It is your responsibility to ensure that any documentation or report that you submit or approve - such as a customer order, financial information, an expense report or time slip - is complete, accurate and contains the proper signatures. Subexians who are found to have knowingly submitted or approved any documentation, report or other information containing materially inaccurate, materially incomplete or other improper data or unauthorized signatures are subject to disciplinary measures, up to and including termination.
- c) Have all commitments to customers and agreements, whether verbal or written, reviewed and approved in accordance with company policies and procedures.
- d) Information about other companies and organizations, including competitors, must be gathered using appropriate methods. Illegal practices such as trespassing, burglary, misrepresentation, wiretapping and stealing are prohibited. In addition, you should not solicit or knowingly accept confidential data from a competitor's employees, ex-employees or customers.
- e) Subex does not permit bribes, kickbacks or any other illegal or improper payments, transfers or receipts. This prohibition is across-the-board and applies to both giving and receiving. No employee shall offer, give, solicit or receive any money or anything else of value for the purpose of obtaining, retaining or directing business or bestowing or receiving any kind of favored treatment.

### **g) Business Entertainment and Gifts**

Appropriate care should be exercised to ensure that business entertainment and gifts for customers, prospective customers, public officials, vendors and others are not excessive and cannot reasonably be construed as bribes or improper inducements. No business entertainment or gift should exceed the bounds of good taste or customary business standards in the community involved. All business entertainment and gifts should be kept at a reasonable level and be based on the expectation that they will become publicly known. All funds expended for business entertainment and gifts must be fully documented and reflected in the books of Subex. Subexians must refrain from requesting, directly or indirectly, that they be given business gifts, entertainment or favors by anyone with whom Subex does business. When such gifts, entertainment or favors are offered to Subexians, they may be accepted only in the event they do not exceed the bounds of good taste or customary business standards in the community involved. Acceptance



## - Code of Conduct for Subexians

should be based on the expectation that it will become publicly known. Cash in any amount or cash equivalents (such as gift certificates) shall not be accepted by any employee.

#### **4. Compliance with laws**

Subex will and expects Subexians to comply with all applicable rules and regulations while conducting business.

#### **5. Disciplinary Process and Committee**

This procedure is designed to help and encourage all Subexian's to achieve and maintain standards of conduct.



## - Code of Conduct for Subexians

### **6. Whistle-Blowing Policy and Committees**

Subex has formed this committee to ensure adherence to this code and to report any violations.

## **II Code of Conduct for Prevention of Insider Trading**

This document outlines the Code of Conduct applicable to Subex Limited in line with the regulations formulated by Securities and Exchange Board of India with regard to Insider Trading

## Contents

### Applicability

1. Title
2. Commencement
3. Definitions
4. Compliance Officer
5. Preservation of price sensitive information
6. Need to know
7. Limited access to confidential information
8. Prevention of misuse of price sensitive information
9. Pre-clearance of trades
10. Reporting requirements for transactions in securities
11. Penalty for contravention of the Code of Conduct
12. Information to SEBI in case of violation of SEBI (Prohibition of Insider Trading) Regulations, 1992
13. Power to amend the Code of Conduct

## Annexures

1. Code of Corporate Disclosures practices for prevention of insider trading
2. Application form for pre-clearance of trades
3. Undertaking
4. Initial disclosure of details of shares held by substantial shareholders/ Directors/ officers, designated Subexians
5. Periodic statement of shareholdings of Directors/ officers/ designated Subexians
6. Annual Disclosure
7. Names of designated Subexians notified under Regulation 3 (e)

***The Securities and Exchange Board of India (SEBI) has formulated the SEBI (Insider Trading) Regulations, 1992. These regulations prohibit an insider from dealing in the securities of a company listed on any stock exchange on the basis of any unpublished price sensitive information. It also prohibits the communication of any unpublished price sensitive information to any person except as required under law. Further, counselling or procuring any person to deal in the securities of any company on the basis of any unpublished price sensitive information is also prohibited under the regulations. Any insider who acts in contravention of these regulations is liable to be punished according to the law including imprisonment and/or fine as provided under Section 24 of the Securities and Exchange Board of India Act, 1992.***

**Subex Limited hereby notifies that the following code be followed by all Directors, Officers and Employees in order to prevent insider trading while dealing/trading in the securities of Subex Limited.**

**Applicability**

This code shall be applicable to all Directors, Officers and Employees of Subex Limited.

1. **Title** :

This Code shall be known as “**CODE OF CONDUCT FOR PREVENTION OF INSIDER TRADING FOR SUBEX LIMITED**”(“**Code of Conduct**”)

2. **Commencement** :

This Code shall come into force on 1<sup>st</sup> December 2004

3. **Definitions** :

In this Code unless the context otherwise requires,

- a) “Board of Directors” or “Board” means the Board of Directors of Subex Limited.
- b) “Company” means Subex Limited and its subsidiaries.
- c) “Dealing in Securities” means an act of subscribing, buying, selling or agreeing to subscribe, buy, sell or deal in any securities of the Company by any person either as principal or agent.
- d) “Dependent Family Members” means wife, husband, parents, son, son’s wife, unmarried daughter, dependent brother and unmarried sister.
- e) “Designated Subexians” shall include –
  - (i) officers comprising the top three tiers of the company management as notified from time to time by the Managing Director and attached in Annexure VII and all Subexians in the Finance & Accounts, Legal & Secretarial Department, Corporate Communications and Sales & Marketing; and
  - (ii) such Subexians, from time to time, as in the opinion of the Managing Director are likely to be in the possession of Price Sensitive Information.
- f) “Directors” shall mean and include any person occupying the position of Director by whatever name called.
- g) “Subexians” mean employees of the Company.
- h) “Officers” shall mean any person as defined in clause (30) of Section 2 of the Companies Act, 1956 including an Auditor of the Company.
- i) “Price Sensitive Information” means any unpublished information which relates directly or indirectly to the Company and which if published is likely to materially affect the price of securities of the Company.

**Explanation** :-

The following shall be deemed to be price sensitive information:-

- 1. periodical financial results of the company;
- 2. intended declaration of dividends (both interim and final);

3. issue of securities by way of public, rights or bonus issue, etc or buy-back of securities;
  4. any major expansion plans or execution of new projects;
  5. amalgamation, mergers or takeovers;
  6. disposal of the whole or substantial part of the undertaking;
  7. any significant changes in policies, plans or operations of the company.
- j) "Securities" include –
- i) shares, scripts, stocks, bonds, debenture, debenture stock or other marketable securities of a like nature in or of the Company;
  - (ii) derivatives and
  - (iii) rights or interest in securities of the Company.
- k) "Trading Window" means the period during which Subexian can trade in the Company's securities.
- l) Words importing the singular number include, where the context admits or requires, the plural number and vice-versa.
- m) Words incorporating the masculine gender shall be taken to include the feminine gender.
- n) Words and expressions used and not defined in this Code but defined in the Securities and Exchange Board of India (Prohibition of Insider Trading) Regulations, 1992 or the Securities and Exchange Board of India Act, 1992 or the Companies Act, 1956 shall have the same meaning respectively assigned to them in the said Regulations/ Acts.
4. **Compliance Officer** :
- a) The Company shall appoint a senior level Subexian as Compliance Officer who shall report to the Managing Director.
  - b) The Compliance Officer shall be responsible for setting forth policies, procedures, monitoring adherence to the rules for the preservation of Price Sensitive Information, pre-clearing of Directors', Officers' and Subexians' and their Dependent Family Members' trades, monitoring of trades and the implementation of the Code of Conduct under the overall supervision of the Board of the Company.
  - c) The Compliance Officer shall maintain a record of the Designated Subexians and any changes made in the list of Designated Subexians.
  - d) The Compliance Officer shall assist all the Subexians in addressing any clarifications regarding the Securities and Exchange Board of India (Prohibition of Insider Trading) Regulations, 1992 and the Company's Code of Conduct.
  - e) The Compliance Officer shall also implement and oversee the Code of Corporate Disclosure Practices for Prevention of Insider Trading as set out in Schedule II of the Securities and Exchange Board of India (Prohibition of Insider Trading) Regulations, 1992 attached hereto as **Annexure I**.

5. **Preservation of Price Sensitive Information:**

All Directors, Officers and Designated Subexians and other Subexians who are in possession of any Price Sensitive Information shall maintain the confidentiality of all Price Sensitive Information and shall not pass on such information to any person directly or indirectly.

6. **Need to know:**

Price Sensitive Information is to be handled only on a “need to know” basis i.e. Price Sensitive Information should be disclosed only to those within the Company who need such information to discharge their official duties.

7. **Limited access to confidential information:**

Files containing Price Sensitive Information as well as files containing other confidential information shall be kept secure. Computer files must have adequate security of login and password, etc.

8. **Prevention of misuse of Price Sensitive Information:**

a) All Directors, Officers and Designated Subexians and other Subexians who have got access to Price Sensitive Information shall be subject to trading restrictions as enumerated below :-

- (i) The Trading Window shall be closed from the time the information referred to in sub-para(a)(ii) below is available to the Director, Officer, Designated Subexian or other Subexians until 24 hours after it is published.
- (ii) The Trading Window shall be, inter alia, closed at the time of –
  - (a) Declaration of financial results (quarterly, half-yearly and annual);
  - (b) Declaration of dividends (interim and final);
  - (c) Issue of securities by way of public, rights or bonus issue etc or buy-back of securities;
  - (d) Any major expansion plans or execution of new projects;
  - (e) Amalgamation, mergers or takeovers;
  - (f) Disposal of whole or substantial part of the undertaking; and
  - (g) Any significant changes in policies, plans or operations of the Company.

The Compliance Officer shall notify the opening and closing of Trading Window through electronic mail to the Subexians.

Notwithstanding anything contained in this code the Trading Window will be deemed to be closed from the 15th day before the end of a quarter till 24 hours after the public disclosure of financial results and all Directors, Officers and Designated Subexians of the company are forbidden from dealing in the company's securities during the above period.

b) All Directors, Officers and Designated Subexians and other Subexians who have got access to Price Sensitive Information shall conduct all their dealings in the securities of the Company only in a valid Trading Window and shall not deal in any transaction involving the purchase or sale of the Company's securities during the period when Trading Window is closed, as

referred to in sub-para(a)(i) and (ii) above or during any other period as may be specified by the Company from time to time.

- c) In case of Employees Stock Options (ESOP's), exercise of option may be allowed during the period when the Trading Window is closed. However, sale of shares allotted on exercise of ESOP's shall not be allowed when Trading Window is closed.

9. **Pre-clearance of trades:**

- a) All Directors, Officers and Designated Subexians and their Dependant Family Members who intend to deal in securities of the Company shall do so only after the pre-clearance of the transaction as per the procedure mentioned hereunder. However, no pre-clearance shall be required if the total nominal value of the securities proposed to be dealt in does not exceed Rs. 50,000/- (Rupees Fifty Thousand only) in aggregate over in any Financial Year.
- b) An application in the prescribed form (being **Annexure II** to this Code) shall be submitted by the concerned Director, Officer or Designated Subexian to the Compliance Officer.
- c) An undertaking in the prescribed form (being **Annexure III** to this Code) shall be executed in favour of the Company by the concerned Director, Officer or Designated Subexian.
- d) All Directors, Officers and Designated Subexians and their Dependant Family Members shall execute the transaction in respect of securities of the Company *within 7 (Seven) days* after the approval of pre-clearance is given. If the transaction is not executed within the above period, the approval would lapse and the concerned Director, Officer or Designated Subexian shall pre clear the transaction again.
- e) All Directors, Officers and Designated Employees who buy or sell any number of shares of the Company shall not enter into an opposite transaction i.e. sell or buy any number of shares during the next six months following the prior transaction. All directors/ officers/ designated Subexians shall also not take positions in derivative transactions in the shares of the Company at any time.
- f) In case the sale of shares is necessitated by personal emergency, the holding period as stated at sub-regulation (e) above may be waived if such a request is forwarded to the Compliance Officer who shall record the same in writing his/her reasons in this regard.
- g) For the purpose of pre-clearance of trade, the request shall be sent by electronic mail (e-mail) and the approval requested will be deemed to be granted within 24 hours (holidays shall be excluded from the computation of this 24 hours) after sending the email unless any reply has been received from the compliance officer.

10. **Reporting requirements for transactions in securities:**

- a) All Directors, Officers and Designated Subexians shall be required to forward to the Compliance Officer the following details of their securities transactions including the statement of Dependant Family Members.
  - (i) A initial disclosure statement of all holdings in securities of the Company (**Annexure IV**);

- (ii) Half-yearly statement of any transactions in securities of the Company. However, such statement need not be furnished if pre-clearance has been obtained for all transactions in the relevant period (**Annexure V**);
    - (iii) An annual statement of all holdings in securities of the Company (**Annexure VI**).
  - b) The Compliance Officer shall maintain records of all the declarations in the appropriate form received from the Directors, Officers and Designated Subexians for a minimum period of 3 (three) years.
  - c) The Compliance Officer shall place before the Managing Director on a monthly basis all the details of the dealing in the securities by the Directors, Officers and Designated Subexians and their Dependant Family Members and the accompanying documents that such persons have executed under the pre-dealing procedure as envisaged in this Code of Conduct.
- 11. **Penalty for contravention of the Code of Conduct:**
  - a) Any Director, Officer or other Subexian who trades in securities or communicates any information for trading in securities, in contravention of this Code of Conduct, may be penalized and appropriate action may be taken by the Company.
  - b) Directors, Officers, Subexians who violate this Code of Conduct shall also be subject to such disciplinary action by the Company, as the Board may deem fit.
  - c) The action by the Company shall not preclude SEBI from taking any action in case of violation of SEBI (Prohibition of Insider Trading), Regulation, 1992.
- 12. **Information to SEBI in case of violation of SEBI (Prohibition of Insider Trading) Regulations, 1992:**

In case it is observed by the Company and/or the Compliance Officer that there has been a violation of SEBI (Prohibition of Insider Trading) Regulations, 1992, SEBI shall be informed of the same.
- 13. **Power to amend the Code of Conduct:**

The Board shall have absolute power to amend, modify, rescind and/or substitute this Code of Conduct and shall also have the powers to remove difficulty or settle any question that may arise under this Code of Conduct or any re-enactment thereof, subject, however, to the condition that this Code of Conduct shall not dilute in any manner the provisions prescribed under the Model Code of Conduct specified under Schedule I of SEBI (Prohibition of Insider Trading) Regulations, 1992.

**CODE OF CORPORATE DISCLOSURES PRACTICES  
FOR PREVENTION OF INSIDER TRADING**

[Regulation 4(e) of the Code of Conduct and Regulation 12(2) of SEBI (Prohibition of Insider Trading) Regulations, 1992]

---

**1.0 Corporate Disclosure Policy**

1.1 To ensure timely and adequate disclosure of price sensitive information, the following norms shall be followed by listed companies:-

**2.0 Prompt disclosure of price sensitive information**

2.1 Price sensitive information shall be given by listed companies to stock exchanges and disseminated on a continuous and immediate basis.

2.2 Listed companies may also consider ways of supplementing information released to stock exchanges by improving investor access to their public announcements.

**3.0 Over seeing and co-coordinating disclosure**

3.1 Listed companies shall designate a senior official (such as compliance officer) to oversee corporate disclosure.

3.2 This official shall be responsible for ensuring that the company complies with continuous disclosure requirements, overseeing and co-coordinating disclosure of price sensitive information to stock exchanges, analysts, shareholders and media and educating staff on disclosure policies and procedure.

3.3 Information disclosure/dissemination may normally be approved in advance by the official designated for the purpose.

3.4 If information is accidentally disclosed without prior approval the person responsible may inform the designated officer immediately, even if the information is not considered price sensitive.

**4.0 Responding to market rumours**

4.1 Listed companies shall have clearly laid down procedures for responding to any queries or requests for verification of market rumours by exchanges.

4.2 The official designated for corporate disclosure shall be responsible for deciding whether a public announcement is necessary for verifying or denying rumours and then making the disclosure.

**5.0 Timely Reporting of shareholdings/ownership and changes in ownership**

5.1 Disclosure of shareholdings/ownership by major shareholders and disclosure of changes in ownership as provided under any Regulations made under the Act and the listing agreement shall be made in a timely and adequate manner.

**6.0 Disclosure/dissemination of Price Sensitive Information with special reference to Analysts, Institutional Investors**

Listed companies should follow the guidelines given hereunder while dealing with analysts and institutional investors:-

**(i) Only Public information to be provided**

Listed companies shall provide only public information to the analysts, research persons, large investors like institutions. Alternatively, the information given to the analyst should be simultaneously made public at the earliest.

**(ii) Recording of discussion**

*In order to avoid misquoting or misrepresentation, it is desirable that at least two company representative be present at meeting with analysts, brokers or Institutional Investors and discussion should preferably be recorded.*

**(iii) Handling of unanticipated questions**

*A listed company should be careful when dealing with analysts questions that raise issues outside the intended scope of discussion. Unanticipated questions may be taken on notice and a considered response given later. If the answer includes price sensitive information, a public announcement should be made before responding.*

**(iv) Simultaneous release of Information**

*When a company organizes meetings with analysts, the company shall make a press release or post relevant information on its website after every such meet. The company may also consider live web casting of analyst meets.*

**7.0 Medium of disclosure/dissemination**

- (i)** *Disclosure/dissemination of information may be done through various media so as to achieve maximum reach and quick dissemination.*
- (ii)** *Corporates shall ensure that disclosure to stock exchanges is made promptly.*
- (iii)** *Corporates may also facilitate disclosure through the use of their dedicated internet website.*
- (iv)** *Company websites may provide a means of giving investors a direct access to analyst briefing material, significant background information and questions and answers.*
- (v)** *The information filed by corporates with exchanges under continuous disclosure requirement may be made available on the company website.*

**8.0 Dissemination by stock exchanges**

- (i)** *The disclosures made to stock exchanges may be disseminated by the exchanges to investors in quick and efficient manner through the stock exchange network as well as through stock exchange websites.*
- (ii)** *Information furnished by the companies under continuous disclosure requirements, should be published on the web site of the exchange instantly.*
- (iii)** *Stock exchanges should make immediate arrangement for display of the information furnished by the companies instantly on the stock exchange website.*

**APPLICATION FORM FOR PRE-CLEARANCE OF TRADES**  
[See Regulation 9(a) and (b) of the Code of Conduct]

Employee Code :	
Name of the Subexian	
Designation	
Region	
Date of Joining the Company	
Name of holder of securities	
Relation to the Subexian	
Kind of securities proposed to be dealt in	
Number of securities proposed to be dealt in	
Estimated Market Value of the securities proposed to be dealt in	
Name of the depository	
Folio No./Client ID No.	

I hereby declare that all information in this form is true and correct to the best of my knowledge. I also understand that any misrepresentation of facts in this form is sufficient cause for disciplinary action by the Company.

Date:

Place:

\_\_\_\_\_ (Signature of Applicant)

**PRE-CLEARANCE ORDER**

This is to inform you that your request for dealing in .....(nos) shares of the company as mentioned in your above mentioned application is approved. Please note that the said transaction must be completed on or before \_\_\_\_\_ (date) that is within 7 days from today.

Date:

For .....

Compliance Officer

**CONFIRMATION OF DEAL**

To: The Compliance Officer

I confirm that the share dealing for which approval was granted on ..... was completed on ..... by purchasing / selling ..... (nos). equity shares of the company.

Date:

Signature

**Annexure III**

**UNDERTAKING**

[See Regulation 9(c) of the Code of Conduct ]

I, \_\_\_\_\_, residing at \_\_\_\_\_ do hereby solemnly declare and undertake as follows:

1. I am Director, Officer, Designated Subexian of Subex Limited, a public limited company, incorporated under the Companies Act, 1956, and having its Registered Office at Adarsh Tech Park, Outer Ring Road, Devarabisanahalli, Bangalore-560 037 (hereinafter referred to as "the Company")
2. I am working with the Company as its \_\_\_\_\_ at \_\_\_\_\_.
3. I hereby declare that I do not have any access to Price Sensitive Information / I have not received Price Sensitive Information upto the time of signing this undertaking. *(Strike off whichever is not applicable)*
4. I further hereby agree, undertake and declare that in case I obtain access to or receive Price Sensitive Information after the signing of this Undertaking but before the execution of the transaction, I shall inform the Compliance Officer of the change in my position and that I will completely refrain from dealing in the securities of the Company till the time such information becomes public.
5. I further hereby declare that I have not contravened the Code of Conduct for Prevention of Insider Trading for Subex Limited as notified by the Company from time to time.
6. I further declare that I have made a full and true disclosure in the matter.
7. I agree that after a buy or sell transaction, I shall not enter into an opposite transaction i.e. sell or buy, any number of shares during the next six months following the prior transaction. I also agree that I shall also not take positions in derivative transactions in the shares of the Company at any time.
8. I confirm that any misrepresentation on my part as to what is undertaken by this undertaking will amount to fraudulent conduct/ misconduct on my part and the Company will be entitled to take disciplinary action against me as it may deem fit.

Date :

Place :

\_\_\_\_\_  
( Signature of Applicant )

**Annexure IV**

**FORM FOR INITIAL DISCLOSURE OF DETAILS OF SHARES HELD BY SUBSTANTIAL SHAREHOLDERS/ DIRECTORS/ OFFICERS, DESIGNATED SUBEXIANS**

[See Regulation 10(a)(i) of the Code of Conduct ]

To: The Compliance Officer

\_\_\_\_\_

Date: \_\_\_\_\_

**1. DETAILS OF SHAREHOLDING OF SUBSTANTIAL SHAREHOLDERS/ DIRECTOR / OFFICER/DESIGNATED SUBEXIANS HELD IN THEIR OWN NAME**

Name	Designation	Department / Date of Joining	Date of becoming substantial shareholder/ Director/Officer	No. of shares held	Date of Acquisition	Folio No/ DP ID/Client ID

**II. DETAILS OF SHARES HELD BY DEPENDENT FAMILY MEMBERS**

Name of Relative	Relationship	No.of shares held	Folio No/ DP ID/Client ID

**Annexure V**

[See Regulation 10(a)(ii) of the Code of Conduct ]

To

The Compliance Officer

Date

**I. PERIODIC STATEMENT OF SHAREHOLDINGS OF DIRECTORS / OFFICERS/ DESIGNATED SUBEXIANS:**

Name	Designation	Department	No.of shares held on 1 <sup>st</sup> April	No.of shares bought during the period	No.of share sold during the period	No, of shares on 30 <sup>th</sup> Sept.	Folio No./DP Id/Client ID

**II. DETAILS OF SHARES HELD BY DEPENDENT FAMILY MEMBERS**

Name	Relationship	No. of shares held on 1 <sup>st</sup> April	No. of shares bought during the period	No. of share sold during the Period	No. of shares on 30 <sup>th</sup> Sept.	Folio No./DP Id/Client ID

**Annexure VI**

To

The Compliance Officer

\_\_\_\_\_

Date

**ANNUAL DISCLOSURE**

[See Regulation 10(a)(iii) of the Code of Conduct ]

**I. STATEMENT OF SHAREHOLDINGS OF DIRECTORS / OFFICERS/ DESIGNATED SUBEXIANS:**

Name	Designation	Department	No. of shares held on 1 <sup>st</sup> April	No. of shares bought during the year	No. of shares sold during the year	No. of shares held on 31 <sup>st</sup> March	Folio No./DP Id/Client ID

**II. DETAILS OF SHARES HELD BY DEPENDENT FAMILY MEMBERS**

Name	Relationship	No. of shares held on 1 <sup>st</sup> April	No. of shares bought during the year	No. of share sold during the year	No. of shares held on 31 <sup>st</sup> March	Folio No./DP Id/Client ID

I/We declare that after a buy or sell transaction, I/we have not entered into an opposite transaction i.e. sell or buy any number of shares during the next six months following the prior transaction. I/We also declare that I/We have not taken positions in derivative transactions in the shares of the Company at any time.

I/We further declare that the above disclosure is true and correct and is in accordance with the previous disclosures given to the Company.

Date:

Signature

***Annexure VII***

**NAMES OF DESIGNATED SUBEXIANS NOTIFIED UNDER REGULATION 3 (e)**

1. **Directors**
2. **All Subexians in Finance & Accounts**
3. **All Subexians in Sales & Marketing**
4. **All Subexians in Legal & Secretarial**
5. **All Subexians in Corporate Communications & Corporate Directorate**
6. **Such other Subexians as the Managing Director may, from time to time specify.**

### III. Subex Corporate Communications Policy

This policy describes the basic principles of conduct that we share as Subexians. This Code also applies to Subex's Directors. This Code is intended to provide a broad overview of basic ethical principles that guide our conduct. In some circumstances, we maintain more specific policies on the topics referred to in this Code.

#### Contents

1. Responsibilities
2. Definitions
3. Disclosure Policy
  - a. Responding to inquiries
  - b. Prohibition on selective disclosure
  - c. Inadvertent disclosures
  - d. Responding to market rumors
  - e. Referring to or distributing analyst reports on Subex
4. Dissemination of non-public information to Subexians
5. Publishing of news about Subex
6. Placing of advertisements
7. Handling information requests
  - a. Trade media queries
  - b. Business/ Financial media queries
  - c. Local media queries of any other nature
  - d. Individual shareholder inquiries
  - e. Analyst queries
8. Speeches and Presentations
9. World Wide Web
10. Internet Discussion Threads/ Chat Rooms

#### Annexure 1: Contact details

Subex discloses information about its operations and performance to accommodate the mutual interests of Subex and the general public. Subex supports regular communication with Subexians, shareholders, customers, communities, media and other groups that have an interest in the company.

As a publicly owned corporation, Subex has an obligation to make available and disseminate certain "material" information to its shareholders and other public stakeholders. At the same time, the improper release of proprietary information could have serious ramifications for Subex. The Subex Communications Policy (SCP) defines areas of responsibility and requirements for material and non-material communication.

### **A. Responsibilities**

*I. Corporate Communications Department is responsible for:*

- Effective communication with Subexians, customers, industry, trade media and other parties with an interest in the company.
- Reviewing information prior to public disclosure for materiality (see Section B). If information is believed to be potentially material, it must be referred to Investor Relations for review.

*II. Subexians are responsible for directing information requests to the Corporate Communications Department within Subex as detailed in the following sections.*

### **B. Definitions**

"Material" Information - Information is material if there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision. Earnings information and "guidance" regarding earnings forecasts should both be considered as being material. Earnings guidance includes indications that earnings are "up," "down," or "flat," along with such statements as "I would not be troubled by that," "that sounds about right," and "that's in the ballpark." Other types of information or events that Regulatory Bodies have indicated are likely to be considered material include (but are not limited to) the following:

- mergers, acquisitions, tender offers, joint ventures or changes in assets; default on debt obligations;
- new products, discoveries, orders, or developments regarding customers or suppliers, such as the acquisition or loss of a contract;
- changes in control or in management;
- a change in auditors or an auditor notification that the issuer may no longer rely on an auditor's reports;
- events regarding the issuer's securities, such as calls of securities for redemption, repurchase plans, stock splits or changes in dividends, changes in the rights of security holders, public or private sales of additional securities by the issuer;
- bankruptcies, insolvency or other significant liquidity events; and litigation.

*"Non-public" Information* - Any information that has not been disseminated in a manner reasonably designed to make it generally available to investors.

*"Proprietary" information* - Any information that, if disclosed, would harm Subex competitive advantage

### **C. Disclosure Policy**

Subex is committed to providing timely and accurate information to the public, consistent with legal and regulatory requirements. When releasing material information, it is imperative that consistent disclosure practices be applied, and that all members of the investment community, including individual investors, have prompt and simultaneous access to the disclosed information. The Disclosure Policy applies to all Subexians and all of its subsidiaries and members of the Board of Directors. It covers disclosures in documents filed with Regulatory Bodies/ Stock Exchanges and written statements made in Subex annual reports, news and earnings releases, letters to shareholders, speeches by senior management and



## - Code of Conduct for Subexians

information provided by Subex on its Internet Web site. In addition, it covers oral statements made in group and individual meetings with analysts and investors, phone calls and webcasts with analysts and investors, and interviews with the media as well as press conferences and all other communications of material information reasonably likely to be transmitted directly or indirectly to the public.

Under this policy, the President & CEO and the CEO are designated as the Primary Spokespersons for Subex. Others within Subex, including those persons designated from time to time by a Primary Spokesperson, will serve as Authorized Spokespersons for a specific period of time/ specific communication, to speak on behalf of Subex or to respond to specific inquiries from the investment community, financial media or the general media. No one but a Primary or Authorized Spokesperson is authorized to talk to investors/ investment community/ analysts/ financial media/ general media. All inquiries from such sources must immediately be referred to the Corporate Communications Department.

### **Responding to inquiries**

Subexians (other than the Primary or Authorized Spokespersons) are not authorized to respond under any circumstances to inquiries from investors/ investment community/ analysts/ financial media/ general media unless specifically authorized to do so by a Primary Spokesperson. Subexians are instructed to refer all such inquiries to the Corporate Communications Department.

### **Prohibition on selective disclosure**

Subex, its directors, executive officers, investor relations personnel, and other people with similar functions, are prohibited from selectively disclosing material nonpublic corporate information to securities market professionals and holders of the issuer's securities, as well as potential investors or anyone else that is not subject to a confidentiality agreement or possesses another duty against disclosing such information.

Methods for public disclosure of material information - Subex will disseminate material information through an appropriate Regulatory Body/ Stock Exchanges filing and, in addition, if deemed appropriate, another method of disclosure that is reasonably designed to provide broad, non-exclusionary distribution of the information to the public. All news releases or other material written public disclosures will be made available on Subex Web site. Subex will publicly disseminate the information before making that information available on a selective basis to the investment community, such as analysts and institutional investors or holders of Subex shares, or any other member of the public.

### **Inadvertent disclosures**

Should a Company official or member of the Board of Directors make an inadvertent disclosure of material, non-public information on a selective basis (e.g., at an analyst meeting or on a phone call with an analyst or investor that was not previously broadly disseminated), Subex will, as soon as reasonably practicable (but in no event later than 24 hours or before the market opening), broadly disseminate that information publicly. Inadvertent material disclosures are required to be reported promptly to a primary spokesperson for Subex.

### **Responding to market rumors**

So long as it is clear that Subex is not the source of the market rumor, Subex spokespersons will respond consistently to those rumors concerning potentially material developments saying, "It is our policy not to comment on market rumors or speculation.". Should the Stock Exchanges request Subex to make a definitive statement in response to a market rumor that is causing significant volatility in Subex stock, the Investor Relations/ Corporate Communications department will consider the matter and make a recommendation to the CEO on whether to make a policy exception.

### **Referring to or distributing analyst reports on Subex**

Subex regards analyst reports as proprietary information belonging to the analyst's firm and will not provide such reports on Subex's Internet website or through any other means to persons outside of the company. Analyst reports on Subex and available industry reports available may be provided periodically to Subexians via e-mail on a timely basis. Distribution of these reports internally is for information purposes only and shall not be represented as an endorsement of the analyst's opinion.

#### **D: Dissemination of non-public information to Subexians**

During the course of normal business activities, material or proprietary information will need to be shared among Subexians. Discretion should always be exercised to limit such information to only those who need to know as part of their job responsibilities. When disseminating such information, it is important to reiterate its confidential nature and take steps to ensure that this information will be protected from misuse or improper release.

#### **E: Publishing of news about Subex**

All news releases to be distributed are to be reviewed and approved in advance by the Corporate Communications Department. In addition, the release date and time must be approved by Corporate Communications Department. This includes news releases generated by Subex as well as news releases generated by others that mention Subex. The Corporate Communications Department will be responsible for the transmission of all news releases. No other department or external agency is authorized to send a news release directly to a media.

#### **F: Placing of advertisements**

No Subexian or agency will place a print, broadcast or web advertisement or sign an advertising contract (with the exception of employment ads, which must be coordinated through human resources) without the approval of the Corporate Communications Department. All advertisements, including those for trade, business or consumer publications, sponsorships and trade shows, must be approved by the Corporate/Marketing Communications Department prior to publishing.

#### **G. Handling information requests**

Information requests can be received by phone, email, fax, letter or even during casual conversation at trade shows and other events. Regardless of the method of inquiry, information requests should be handled as follows:

##### **Trade media queries**

Trade media inquiries should be directed to the Marketing Communications Department or to the Corporate Communications Department. Trade media inquiries for previously undisclosed material information and/ or information which is not readily available from divisions or local offices should be directed to the Marketing Communications Department.

##### **Business/ Financial media queries**

Business/ financial media inquiries should be directed to the Corporate Communications Department.

##### **Local media queries of any other nature**

Local media inquiries of any other nature should be directed to the Corporate Communications Department. Some business units may have created programs for other Subex offices to encourage relationship building with local media to enhance local sales and recruitment efforts, as well as to establish a positive local company image. Inquiries about these local programs should be directed to the Primary Spokesperson at Subex. In addition, the Primary Spokesperson may designate spokespersons to discuss local issues with members of the media.

##### **Individual shareholder inquiries**

Individual shareholder inquiries, including requests for copies of Company reports to shareholders should be directed to the Investor Relations department.

##### **Analyst queries**



## - Code of Conduct for Subexians

Security analysts or other investment professionals requesting information must be directed to the Primary Spokesperson/ Investor Relations Department/ Corporate Communications Department. Under no circumstances should a Subexian provide information to security analysts or investment professionals about Subex, its products, or its forecasts.

### **General information requests**

General public information requests should be directed to the Corporate Communications Department.

**When in doubt, forward inquiries to the Corporate Communications Department.**

### **H: Speeches and Presentations**

Representatives of Subex regularly make speeches or participate in conferences. Such appearances must be approved by the appropriate business heads in the case of marketing-related presentations, or by the Marketing Communications Department for presentations that involve Subex overall, its strategies or its financial performance. In general, presentations should include only information covering the Subexian's areas of responsibility and generally known and public information about Subex. Under no circumstances should speakers disclose material non-public information in the presentation or in any subsequent question and answer or other breakout meeting.

### **I: World Wide Web**

1. The only authorized Subex World Wide Web (WWW) presence is [www.subexworld.com](http://www.subexworld.com). This medium's global reach and instantaneous nature present some unique challenges related to legality, security and content. Therefore, centralized content control is required for all visual and written information contained on the site. Standards for the Subex web presence are created and managed by the Corporate Communications Department.
2. No Subexian, agency or other party is to place information of any kind regarding Subex, its products, operations or plans on any portion of the WWW.
3. Individual Subexians are prohibited from using, or approving the use of, the Subex logo, copyrighted material or proprietary material of Subex, Inc. on the WWW without approval from the Corporate Communications Department.
4. All requests to register domain names on behalf of Subex anywhere in the world must be coordinated through the Corporate Communications Department. This is necessary to ensure consistency, protection of our trademark, and functionality of our web presence.
5. Use of the logo on a third-party Web site requires prior consent of the Corporate/ Marketing Communications Department. If used as a hyperlink, the logo should point to the Subex home page at [www.subexworld.com](http://www.subexworld.com).

### **J. Internet Discussion Threads/ Chat Rooms**

1. Subex will not comment on or reply to rumors, statements or questions posted on Internet discussion groups.
2. Subexians are not authorized to speak on behalf of Subex, or to disclose any news about Subex, on Internet discussion groups.

**Annexure 1:**

**Contact details**

**Primary spokespersons:**

**Founder Chairman, Managing Director & CEO**

Subash Menon

Ph: +91 80 66598700, Ext: 8989, Mobile: +91 98450 40426, E-mail: subash.menon@subexworld.com

**Chief Operating Officer**

Sudeesh Yezhuvath

Ph: +91 66598700, Ext: 8990, Mobile: +91 98450 40428, E-mail: sudeesh.yezhuvath@subexworld.com

**Corporate Communications Department**

Mansi Chouhan

Ph: +91 66598700, Ext: 4157, Mobile: +91 9740997222, E-mail: mansi.chouhan@subexworld.com

**Marketing Communications Department**

Farhath Farooqui

E-mail: farhath.farooqui@subexworld.com

**Investor Relations Department**

Ramanathan J

Ph: +91 66598700, Ext: 8785, Mobile: +91 98456 78905, E-mail: ramanathan.j@subexworld.com  
or investorrelations@subexworld.com

## IV. Subex Customer Interaction Code of Conduct

### 1. Introduction

The customer interaction code of conduct helps ensure compliance with legal requirements and our standards of business conduct. All Subexians (this includes trainees and consultants representing Subex at customer sites and meetings) are expected to read and understand this customer interaction code of conduct and ethics, uphold these standards in day-to-day activities, comply with all applicable policies and procedures and ensure that they understand and adhere to these standards while at customer sites and/or during customer meetings.

We are committed to continuously review and update our policies and procedures. Therefore this customer interaction code of conduct is subject to modification at the discretion of Subex Ltd.

- **Access control system:** In case the customer sites are equipped with access control system, Use the access control cards to enter and exit at the premises or any other location as mentioned by customer. The access control cards should be carried whenever entering or exiting from a customer site.
- **Email accounts:** In case the customer has provided an Email account for official use. This must not be used to distribute or store, defamatory, fraudulent, harassing or obscene messages and files, or otherwise engage in any illegal or wrongful conduct. This includes use on insulting, sexist, racist, obscene or suggestive electronic mail.
- **Legal Adherence Clause:** You may not violate any local, state, national or international law or regulation.
- **Non-Harassment Clause:** You may not harass or threaten any customers of Subex Ltd
- **Non-Vulgarity Clause:** You may not use any sexually explicit, harmful, threatening, abusive, defamatory, obscene, hateful, religious, sexually oriented or ethnically offensive language. You may not attempt to communicate these by way of acronyms, abbreviations or suggestions while at the customer site or during your interaction with the customers.
- **Non-Impersonation Clause:** You may not impersonate any customer of Subex Ltd, past or present.
- **Anti-Piracy Clause:** You may not arrange for the exchange or transfer of any pirated or illegal software while at the customer site.
- **Orderly Conduct Clause:** You will follow the instructions of authorized personnel or designated person while at customer site.
- **Tolerance Clause:** You may not organize nor be a member of any associations or groups that are based on, or supports any racist, sexist, anti-religious, anti-ethnic, anti-gay, or other hate-mongering philosophy.
- **Internet:** You may not upload or transmit on the network of the customer any content without prior written permission from the customers.
- **Anti-Hacking Clause:** You may not attempt to interfere with, hack into, or decode any transmissions to or from the servers running at the customer site
- **Use of customer premises:** A written permission should be obtained from the customer on the timelines of activities, which will be carried out at the customer site. In case of use of facilities and premises after office hours or weekends/holidays, prior approval should be obtained in writing
- **Access to Restricted Areas:** Subexians working at client site are requested to confine themselves to areas allotted by the customer to carry out their official activity. Entry into any unauthorized/restricted area should be done only with the prior approval of the customers.

- **Changes in system:** Any change to be made in the system of the customers need to have prior approval from customers.
- **Access to customer systems and network:** Subexians should have prior written permission from the customer to access any systems or network at their site either from the premises directly or remotely from any other locations.
- **Security Policy:** Subexians at customer site should strictly follow the security policy laid down by our customers while carrying out the activities at the clients place.
- **Infrastructure:** Subexians can use the internet, phone; fax etc provided and approved by the customer only for the job, activities or tasks related to the customer. Any use of this infrastructure for other purpose than that it was indented to, should have a prior written approval from the customer. If an emergency situation demands usage of such infrastructure for any purpose other than the specified, the same needs to be communicated immediately to the customer in writing with the reasons.
- **Drug and Alcohol Abuse:** To meet our responsibilities to customers, Subex must maintain healthy and productive work environment. Misuse of controlled substances and/or selling manufacturing, distributing, possessing, using or being under the influence of illegal drugs and alcohol on the job is absolutely prohibited
- **Dress Code and other personal standards:** Each Subexian is a representative of the company in the eyes of the public, we must report to work properly groomed and wearing appropriate clothing. Subexians are expected to dress neatly and in a manner consistent with the nature of work performed
- **Payments or Gifts:** Under no circumstances may Subexians accept any offer, payment, promise to pay, authorization to pay any money, gift, or anything of value from customers directly or indirectly, to influence any decision, any act or failure to act, any commitment of fraud, or opportunity for the commission of any fraud. Inexpensive gifts, infrequent business meals, celebratory events and entertainment, provided that they are not excessive or create an appearance of impropriety, do not violate this policy. Before accepting anything of value from a customer, please contact the human resource department
- **Handling the confidential information of Customers:** All confidential information pertaining to the customer known to Subexians working at site should not be disclosed to a third party without a prior written approval of the customer.

## 2. Disciplinary Action:

The matters covered in this are of the utmost importance to Subex and are essential to the company's ability to conduct its business in accordance with its stated values. We expect all Subexians to adhere to these rules in carrying out their duties for the company.

The company will take appropriate action against any Subexians whose actions are found to violate these policies or any other policies of the company. Disciplinary actions may include immediate termination or business relationship at the company's sole discretion. Where the company has suffered a loss, it may be forced to take appropriate action for the damage caused. Where laws have been violated, the company will cooperate fully with the appropriate authorities.

## V. Data protection policy

### Contents

1. Scope
2. Policy statement
3. Related policies
  - a. Access control policy
  - b. Acceptable use policy

#### 1. Scope

The scope of this policy is to establish guidelines for achieving appropriate protection of Subexian's personal information from unauthorized access, use, disclosure, disruption, modification or destruction. The policy aims to formulate guidelines for the collection, storage, transmission, use and deletion of any personal information obtained from Subexians in electronic and hard copy media by Subex.

This policy applies to all Subexians and vendors or contractors working on behalf of Subex, in addition to applicable laws. The Executive Management Board of Subex reserves the right to modify this policy at its discretion.

Securing the information requires the participation of and support from all Subexians with access to Subex's network and information. It is the responsibility of every user to help ensure that all information and data are kept confidential, secure and only accessible to those individuals that have a need to know such information.

#### 2. Policy Statement

Subex records, stores and uses Subexian's personal information, including sharing some of that required information with third parties, in order to operate its business and meet its obligations as an employer. As is the case with all sensitive, valuable business data, Subex will exercise reasonable care in protecting Subexian's personal information from unauthorized access, use, modification and disclosure both internally and externally.

A key principle of this policy is that only authorized users may have access to Subexian's personal information and those authorized users must adhere to the general requirements of the Access Control Policy and Acceptable Use Policy. This policy specifically prohibits any unauthorized or unlawful disclosure of Subexian's personal information and is designed to ensure, to the extent practicable, the confidentiality of Subexian's personal information. However, certain Subexian's personal information will be provided when either required by law or when requested by third parties for verification purposes. Furthermore, any violations of this policy will result in disciplinary action in addition to legal sanctions. Nothing in this policy prevents an employee from disclosing his/her own personal information or engaging in any other conduct that is protected by law.

#### 3. Related Policies and Documents

- a. Access Control Policy
- b. Acceptable Use Policy

#### A. Access Control Policy

The scope of this security policy includes all Subex networks and/or equipment that are owned or operated by Subex whether the information is on electronic media, printed as hardcopy, or transmitted over public/private networks. Subex shall ensure that our data collection supports reasonable business



## - Code of Conduct for Subexians

requirements, and does not use Subexian's personal information for purposes that are incompatible with its business requirements.

Access to Subexian's personal information Systems must be managed according to this policy.

### **Access Control**

Access controls are technical mechanisms that restrict Subexian's personal information access to authorized users. Such measures shall be implemented to ensure that security objectives are in compliance with all applicable laws and Subex's policies.

This policy applies to all Subex users who have access to, support, administer, manage, or maintain Subex network systems. All internal servers at Subex is managed by Systems Administration department.

### **Policy Statement**

Subex's networks are essential to its success. Therefore, access to all network will be granted in a controlled manner driven by business requirements subject to the approval of the concerned System administration department with the approval of System Administration Head. Subexians will be explicitly granted access to information or systems. There is no implicit right of access.

The process to manage access to information includes:

- Proper documentation, management and responsibilities of all users;
- Development and implementation of access control mechanisms, both technical and non-technical, to protect unauthorized access to applications and systems;
- Proper monitoring of access and use of applications and systems; and,
- Proper controls for authorized remote access to information.

Controls are developed, implemented, monitored and maintained by Subex to create user accountability and to ensure confidentiality, availability and integrity of Subex network and systems.

Access control measures adopted by Subex include secure and accountable means of *authorization* and *authentication*.

- Authorization is the process of determining whether or not an identified individual has been granted rights to Subexian's personal information and determine what type of access is allowed, e.g read only, create, delete, and/or modify.
- Authentication is the process of confirming that a known individual is correctly associated with a given electronic credential, for example, by use of passwords to confirm correct association with a user or account name.

Access control typically consists of but are not limited to

- Login accounts set directly on Subex application and systems to be accessed or
- Use of a "Net ID" which is associated with an authentication mechanism, incorporated in the application and systems.

Subex provides all Subexians with reasonable access to their own personal information and the ability to review and correct it, as applicable. It is the concerned Subexian's responsibility to ensure that all of his or her personal information is accurate, complete and current at all times. It is also the responsibility of the concerned Subexian not to share his passwords to individual accounts with other individuals. Further all Subexians are urged to change the passwords if they suspect any leakage of the same.

### **Third Party Access to Subexian's personal information**

Subex does not transfer or provide access to Subexian's personal information to third parties. Sharing of personal information will occur only if it is required for business requirements, those third parties agree to give the data the equivalent level of protection that Subex provides, or another suitable level of protection as determined by Subex and only with the consent of the concerned Subexian. Third parties that store, transmit or process Subexian's personal information must sign a required documents for this purpose.

### **Monitoring Access to Subexian's personal information**



## - Code of Conduct for Subexians

When users access Subexian's personal information Systems, access logs may record their actions. System administration team is responsible for reviewing access logs related to Subexian's personal information.

### **Acceptable Use Agreement**

All users who have been given access to Subexian personal information and must read and acknowledge the Acceptable Use Policy prior to being granted access to Subex networks.

### **Background Checks**

Subex reserves the right to conduct background checks before providing access to any user. Background checks may include criminal checks and verification of employment records.

### **User Role Changes**

When authorized users change roles within the company, their access will be immediately changed to reflect the new job responsibilities; new access must be added and old access that is no longer required must be removed.

### **User Responsibility**

When access is granted, users are responsible for all system activity under their unique account. Users have the responsibility to protect their account by creating and maintaining passwords compliant with this policy in addition, users are responsible for maintaining the confidentiality of their unique ID and password by not sharing it with any other party.

### **Anti-Virus**

Subex networks and servers are configured with updated anti-virus software. User must never attempt to disable anti-virus software.

### **Review of Access Privileges**

Subex periodically reevaluates the access granted to ascertain that the access is still commensurate with the user's job responsibilities.

User IDs found to be invalid must be disabled. Non-employee User IDs and access privileges, including vendor and business partner IDs, must be re-evaluated every six months. User IDs found to be invalid must be disabled and investigated immediately.

### **Terminated Employees and Contractors**

User IDs of terminated or resigned users must be disabled from all information systems immediately upon notification from Human Resources and/or the responsible business unit or department. Every week, Human Resources must send a summary email notification of all new departures to all relevant system administration teams.

## **B. Acceptable Use Policy**

Subex adheres to these minimum requirements described in this policy when storing and disposing of Subexian's personal information. These are not exhaustive measures and Subex reserves the right to modify these measures in its endeavor to provide adequate security all proprietary information.

### **Use of personal information**

Subex will use personal information provided by Subexian's solely for conducting its business and in accordance with all applicable laws. Subex will provide the concerned Subexian the required access to his/her personal information to modify or update the same. In no event other Subexians or third parties are permitted to access or modify the personal information of fellow Subexians.

**Physical Security of Hard Copy Subexian's personal information**

Hard copy Subexian's personal information must be secured in locked containers such as file cabinets whenever not in use. Keys must be available only to authorized users and must not be shared with any body.

**Taking back- up of personal information**

Copies of Subexian's personal information must be backed up to tape or other removable storage media for disaster recovery purposes. Back-up media containing Subexian's personal information must be stored in a locked Subex or other Subex-authorized location only accessible by authorized users. Unauthorized persons are not permitted to modify or to take back up of any personal information belonging to others.

**Disposal**

When Subexian's personal information is no longer required by the business and is not subject to any data retention policy, law or regulation, it must be disposed using a paper shredder, incinerator, or pulping. Alternately, a contracted service provider that applies one of these methods may be approved by the applicable authorized department head.

When electronic Subexian's personal information is no longer required by the business and is not subject to any data retention policy, law or regulation, it must be irretrievably deleted from systems, databases, e-mail servers, PC hard drives, and other storage devices. When the electronic media itself requires disposal, it must be degaussed, shred or incinerated.

**Non disclosure obligations**

All Subexians are contractually bound not to disclose any personal information of others and any confidential information in their possession. This continues to apply even after their employment relationship has been terminated.

## VI. Protection of Assets Policy

### Contents

1. Introduction
2. E-Mail policy
3. Password protection policy
4. Anti Virus Process
5. Anti Virus Policy
6. Server security policy
7. VPN security policy
8. Wireless LAN Policy
9. Dial-In Access Policy
10. Extranet Policy
11. Internet Usage Policy

### Introduction

These are the assets, which need to be protected, if not the proper functionality of the business processes can get affected;

Application servers, database servers, Intranet Services, Extranet Services , CVS Servers, Ftp servers, Pas Server, Back up Servers, business plans, projects in development, Mail Server etc.

### 1. E-Mail Policy

#### Purpose

To prevent tarnishing the public image of Subex when email goes out from Subex as the general public will tend to view that message as an official policy statement from Subex.

#### 1.2 Scope

This policy covers appropriate use of any email sent from a Subex email address and applies to all Subexians, vendors, and agents operating on behalf of Subex

#### 1.3 Policy

##### 1.3.1 Prohibited Use

The Subex email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Subexians who receive any emails with this content from any Subex employee should report the matter to their supervisor immediately. Incoming/Outgoing mail size is limited to 1MB.

##### 1.3.2 Personal Use

Using a reasonable amount of Subex resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from Subex email account is prohibited. Virus or other malware warnings and mass mailings from Subex shall be approved by the concerned Manager before sending. These restrictions also apply to the forwarding of mail received by a Subexian.



### 1.3.3 Monitoring

Subex may monitor messages stored, sent or received on the company's email system without prior notice.

## 2 Password Protection Policy

### 2.1 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of security of entire corporate network. As such, all Subexians (including contractors with access to Subex's systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

### 2.2 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

### 2.3 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Subex facility, has access to Subex network, or stores any non-public Subex information.

### 2.4 General

All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.

All production system-level passwords must be part of the SysAdmin administered global password management database.

All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.

User accounts that have system-level privileges granted through group memberships or programs such as "pseudo" must have a unique password from all other accounts held by that user.

Passwords must not be inserted into email messages or other forms of electronic communication. All user-level and system-level passwords must conform to the guidelines described below.

### 2.5 Guidelines

#### A. General Password Construction Guidelines

Passwords are used for various purposes at Subex. Some of the more common uses include: user level accounts, Intranet accounts, Extranet Account, VPN Account, email accounts, screen saver protection, voicemail password, and local router logins. Passwords should contain both upper and lower case characters (e.g., a-z, A-Z) Have digits and punctuation characters as well as letters e.g., 0-9, !@#%&\*( )\_+|~- =\`{}[]:; '<>?,./)

Are at least eight alphanumeric characters long. Is not a word in any language, slang, dialect, jargon, etc? Are not based on personal information, names of family, etc. Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be:

"This May Be One Way to Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

**Note:** Do not use either of these examples as passwords!

#### B. Password Protection Standards

Do not use the same password for Subex accounts as for other non-Subex access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Subex access needs. For example, select one password for the Infrastructure systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share Subex passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Subex information.

Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger, and Evolution).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months. If an account or password is suspected to have been compromised, report the incident to Sysadmin and change all passwords.

### **C. Use of Passwords for Remote Access Users**

Access to the Subex Networks via remote access is to be controlled using either a one-time password authentication

## **3 Anti-Virus Process**

Recommended processes to prevent virus problems:

- As per corporate security standards, update the software and patches regularly in a timely manner provided by sysadmin.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding, the same.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan a floppy diskette from an unknown source for viruses before using it.
- If there is a virus attack on the system, run the anti-virus utility to ensure a clean machine. When the anti-virus scan is running, do not run any applications that could transfer a virus, e.g., email or file sharing.
- New viruses are discovered almost every day. Periodically check the intranet for the patches and Recommended Processes for updates.

## **4 Anti-Virus Policy**

### **4.1 Purpose**

All computers connected to Subex network needs to have antivirus installed on the systems.

### **4.2 Scope**

This policy applies to all Subex computers that are PC-based or utilize PC-file directory sharing. This includes desktop computers, laptop computers, file/ftp/proxy servers, and any PC based equipments such as Access control, Voice Billing, EPBAX traffic generators.

### 4.3 Policy

All computers must have anti-virus software installed and scheduled to scan the complete system at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up to- date. Virus-infected computers will be removed from the network until they are verified as virus-free. Sysadmin Admin Manger / System Admin department are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into Subex's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited

Refer to Subex's Guide lines to anti virus process to help prevent virus problems.

Noted exceptions: Machines with operating systems other than those based on Microsoft products are exempted.

## 5 Server Security Policy

### 5.1 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server that is owned and/or operated by Subex. Effective implementation of this policy will minimize unauthorized access to Subex proprietary information and technology.

### 5.2 Scope

This policy applies to following servers like Source Code Server, HR server, Finance Server, Mailing System, File Servers, Intranet, Extranet, FTP server.

### 5.3 Policy

#### 5.3.1 Ownership and Responsibilities

All internal servers deployed at Subex is owned by an Systems Admin Dept that is responsible for system administration. Approved server configuration guides must be established and maintained by the Systems Admin Manger, based on business needs and approved by System Admin HOD. Systems Admin Dept should monitor configuration compliance and implement an exception policy tailored to their environment. Systems Admin Dept must establish a process for changing the configuration guides, which includes review and approval by System Admin HOD.

- Servers must be registered within the Hard Ware Register. At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location, and a backup contact
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable
- Information in the Hard Ware Register must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

#### 5.3.2 General Configuration Guidelines

- Operating System configuration should be in accordance with approved System Admin HOD.
- Services and applications that will not be used must be disabled where not required.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Always use standard security principles of least required access to perform a function.

- Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.

### 5.3.3 Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
  - All security related logs will be kept online for a minimum of 1 week.
  - Daily incremental tape backups will be retained for at least 1 Week.
  - Weekly full tape backups of logs will be retained for at least 1 month.
  - Monthly full backups will be retained for a minimum of 2 Months.
- Security-related events will be reported to Systems Admin Manger, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include,
  - Port-scan attacks
  - Evidence of unauthorized access to privileged accounts
  - Anomalous occurrences that are not related to specific applications on the host.

### 5.3.4 Compliance

- Audits will be performed on a quarterly basis by authorized person within Subex.
- Audits will be managed by the System Admin HOD, in accordance with the company policy. Systems Admin Manger will filter findings not related to a specific operational group and then present the findings to the Systems Admin Dept for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

## 6 Virtual Private Network (VPN) Policy

### 6.1 Purpose

The purpose of this policy is to provide guidelines for Remote Access IPSec, PPTP or L2TP Virtual Private Network (VPN) connections to Subex network.

### 6.2 Scope

This policy applies to all Subexians, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access Subex network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

### 6.3 Policy

Approved Subex Subexians and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a Subex managed service.

Additionally,

1. It is the responsibility of Subexians with VPN privileges to ensure that unauthorized users are not allowed access to Subex internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a public/private key system with a strong passphrase.
3. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed. 5. VPN users will be automatically disconnected from Subex network after thirty minutes of inactivity. The user must

- then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open and the same will be allowed.
5. The VPN connection is limited to an absolute connection time of 24 hours.
  6. Users of computers that are not Subex owned equipment must configure the equipment to comply with Subex VPN and Network policies.
  7. Only VPN clients approved by Subex may be used.
  8. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Subex network, and as such are subject to the same rules and regulations that apply to Subex owned equipment, i.e., their machines must be configured to comply with Subex Security Policies.
  9. Security Policies.

### **7 Wireless Communication Policy**

#### **7.1 Purpose**

This policy prohibits access to Subex networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by Sys Admin Dept are approved for connectivity to Subex networks.

#### **7.2 Scope**

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of Subex internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to Subex networks do not fall under the purview of this policy.

#### **7.3 Policy**

##### **7.3.1 Register Access Points and Cards**

All wireless Access Points / Base Stations connected to the network is registered and approved by Sys Admin Dept. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in laptop or desktop computers must be registered with Sys Admin Dept

##### **7.3.1.1 Approved Technology**

All wireless LAN access must use corporate-approved vendor products and security configurations.

##### **7.3.1.2 Encryption and Authentication**

All computers with wireless LAN devices must utilize a corporate-approved encryption configured to drop all unauthenticated and unencrypted traffic. To comply with this policy, wireless implementations must maintain point to point hardware encryption of at least 128 bits. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address.

##### **7.3.1.3 Setting the SSID**

The SSID shall be configured so that it does not contain any identifying information about the organization, such as the company name, division title, employee name, or product identifier.

### **8 Dial-In Access Policy**

#### **8.1 Purpose**

The purpose of this policy is to protect Subex electronic information from being inadvertently compromised by authorized personnel using a dial-in connection.

#### **8.2 Scope**



The scope of this policy is to define appropriate dial-in access and its use by authorized personnel.

### **8.3 Policy**

Subexians and authorized third parties (customers, etc.) can use dial-in connections to gain access to the corporate network. Dial-in access should be strictly controlled, using one-time password authentication.

It is the responsibility of Subexians with dial-in access privileges to ensure a dial-in connection to Subex is not used by non-employees to gain access to company information system resources. An employee who is granted dial-in access privileges must remain constantly aware that dial-in connections between their location and Subex are literal extensions of Subex network, and that they provide a potential path to the company's most sensitive information. The employee and/or authorized third party individual must take every reasonable measure to protect Subex assets.

### **8.4 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action.

## **9 Extranet Policy**

### **9.1 Purpose**

This document describes the policy under which third party organizations connect to Subex networks for the purpose of transacting business related to Subex.

### **9.2 Scope**

Connections between third parties that require access to non-public Subex resources fall under this policy, regardless of whether a telco circuit (such as frame relay or ISDN) or VPN technology is used for the connection.

### **9.3 Policy**

#### **9.3.1 Pre-Requisites**

#### **9.3.2 Security Review**

All new requests for extranet connectivity will go through a security review with approvals from senior Subexians.

#### **9.3.3 Third Party Connection Agreement**

Approval from Management is required, can be in electronic format.

### **9.4 Establishing Connectivity**

Department within Subex that wish to establish connectivity to a third party are to file a new site request with the proper extranet group. The extranet group will engage Systems Admin Ltd to address security issues inherent in the project. If the proposed connection is to terminate within a particular location at Subex network, the Department must engage the [name of team responsible for security]. The Department must provide full and complete information as to the nature of the proposed access to the extranet group and Sys Admin Dept, as requested.

All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review. In no case will Subex rely upon the third party to protect Subex network or resources.

### **9.5 Modifying or Changing Connectivity and Access**

All changes in access must be accompanied by a valid business justification, and are subject to security review. Changes are to be implemented via corporate change management process. The Sponsoring Organization is responsible for notifying the extranet management group and/or Sys Admin Dept when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

### **9.6 Terminating Access**

When access is no longer required, the sponsoring organization within Subex must notify the extranet team responsible for that connectivity, which will then terminate the access. This may mean a modification of existing permissions up to terminating the circuit, as appropriate. The extranet and Subex security teams must conduct an audit of their respective connections on an annual basis to ensure that all existing connections are still needed, and that the access provided meets the needs of the connection. Connections that are found to be depreciated, and/or are no longer being used to conduct Subex business, will be terminated immediately. Should a security incident or a finding that a circuit has been deprecated and is no longer being used to conduct Subex business necessitate a modification of existing permissions, or termination of connectivity, Sys Admin Dept and/or the extranet team will notify the POC or the Sponsoring Organization of the change prior to taking any action.

## **10 Internet Usage Policy**

### **10.1 Purpose**

Ensure that Subexians don't abuse Internet usage at the workplace.

### **10.2 Scope**

The scope of this policy is to define appropriate use of internet

### **10.3 Usage Policy**

As part of this organization's commitment to the utilization of new technologies, many/all of our Subexians have access to the Internet. In order protect us from being victimized by the threat of viruses or hacking into our server, the following is effective with immediate effect

1. It is (Organization's) policy to limit Internet access to official business. Subexians are authorized to access the Internet for personal business after- office hours, in strict compliance with the other terms of this policy. The introduction of viruses, or malicious tampering with any computer system, is prohibited.
2. Subexians using (Organization's) internet are acting as representatives of Subex. Subexians should act accordingly to avoid damaging the reputation of the organization (When we access the internet our ip would be know to the outer world).
3. Files that are downloaded from the Internet must be scanned with virus detection software before installing or execution. All appropriate precautions should be taken to detect for a virus and, if necessary, to prevent its spread.
4. Subexians shall not place company material (copyrighted software, internal correspondence, etc.) on any publicly accessible Internet computer without proper permission.
5. The Internet does not guarantee the privacy and confidentiality of information. Sensitive material transferred over the Internet may be at risk of detection by a third party. Subexians must exercise caution and care when transferring such material in any form.
6. Unless otherwise noted, all software on the Internet should be considered copyrighted work. Therefore, Subexians are prohibited from downloading software and/or modifying any such files without permission from the copyright holder.
7. Any infringing activity by an employee may be the responsibility of the organization (For example using P2P software's like Kazza, Gautella, edonkey for sharing data). Therefore, Subex may choose to hold the employee liable for the employee's actions.
8. Subex Ltd reserves the right to inspect an employee's computer system for violations of this policy.
9. Any Subexian working on a clients system may not access the internet or intranet unless required for the delivery of agreed services.

## VII. Subex Electronic Mail Policy

### Contents

1. Introduction
2. Scope
3. Electronic Mail Policy
  - 3.1 Asset and disclosure
  - 3.2 Illegal use
  - 3.3 Privacy
  - 3.4 Mass distribution of email/ unsolicited mass email/ broadcast rights
  - 3.5 Exceptions to unsolicited mass distribution of email
  - 3.6 Security
  - 3.7 Personal use
  - 3.8 Internet email
  - 3.9 Consequences of violations of Electronic Mail Policy
  - 3.10 Email which addresses a group email ID
- 4 Changes to this policy

This policy applies to all Subexians, consultants and others, who utilize Subex's computer systems and other information resources and assets. It recognizes that all users have a responsibility towards the integrity and confidentiality of information, through their respective conditions of employment and conditions of engagement and defines more specifically, accountabilities, responsibilities and guidelines for ensuring all information resources and assets are adequately protected.

### 1. Introduction

This Electronic Mail Policy and the supporting Standards and Guidelines reflect the operating philosophy of Subex.

Its underlying objectives are:

- To promote awareness and to highlight to all users the importance of maintaining good electronic mail practices.
- To prevent the misuse of Subex's electronic mail infrastructure.

This policy defines accountabilities, responsibilities and guidelines for ensuring the most efficient use of Subex's electronic mail infrastructure.

### 2. Scope

This policy complements the Protection of Assets Policy which lists email policies relating to prohibited use, personal use and monitoring. All areas of the Protection of Assets Policy apply to this email policy as well. Electronic mail (email) is an important part of Subex's corporate culture and has a significant impact on the organization in terms of the security of its information resources and its overall efficiency. There is also an increasing reliance on email infrastructure to support routine corporate communications and business operations. Information stored in these systems is growing in quantity and becoming an increasingly important and valuable asset. The integrity, confidentiality and availability of this information are essential for Subex to remain a leading provider of telecom software products. Confidentiality assures that the email information is protected from abuse and unauthorized access. Availability assures that the email infrastructure is on-line and accessible by authorized staff as required. Integrity safeguards the accuracy and completeness of information. This policy attempts to cover all possible aspects of email usage. If however a particular issue has not been addressed within the policy it does not imply that it is condoned by the organization. In these cases users must always use their judgment in determining whether a particular activity is likely to breach the policy and is therefore contrary to the best interests of Subex's business.

### 3. Electronic Mail Policy

### 3.1 Asset and Disclosure

Email information resources held by Subex are considered to be assets of the company and all email users are responsible and accountable for their proper use and for their protection from unauthorized use or disclosure. Email users must not disclose Subex information to external parties without proper authorization.

### 3.2 Illegal Use

Email users must not use Subex's email systems to infringe copyrights or other intellectual property rights of third parties, to distribute or store, defamatory, fraudulent, harassing or obscene messages and files, or otherwise to engage in any illegal or wrongful conduct. This includes the use of insulting, sexist, racist, obscene or suggestive electronic mail.

### 3.3 Privacy

Email users can have a general expectation of a reasonable degree of privacy; however, they should be aware that email is not guaranteed to be private. In some instances Subex may access or disclose the electronic messages or files of a user. This will only be undertaken by the responsible System Administrator or delegate. This access will be undertaken to:

- Protect system security
- Investigate any potentially illegal, unlawful or improper conduct.
- Investigate serious misconduct involving the harassment of staff or other individuals
- Comply with legal process
- Protect the rights or property of Subex
- Provide access for a colleague to access information stored in an email account if the user is absent, unavailable, or on leave and it is necessary to view email or other files.
- Conduct regular audits on email usage and content to ensure compliance with the Electronic Mail Policy. No unauthorized Subex email user or any other individual has permission to view any email that is not intended for them or to open any file for which the author has not granted them access.

### 3.4 Mass distribution of email/ unsolicited mass email/ Broadcast rights

Subexians who wish to send a mass, unsolicited email that is not intended as part of their work or is deemed unofficial given their scope of work (including personal wishes for an occasion), to all others or to one of the email distribution lists, need prior approval to do so, since it uses valuable bandwidth resources and infringes on the privacy and work time of other Subexians. Specifically, someone who wishes to send an email to all Subexians in a particular geographical location or all locations should make a request to the Human Resources Department ([hr@subexworld.com](mailto:hr@subexworld.com)), if such a mail is perceived to be outside their scope of work.

### 3.5 Exceptions to unsolicited mass distribution of email

- A personal wish to a known set of Subexians (known peers/ seniors/ others) is allowed. In essence, do not use one of the mailing groups (for instance, Subex – Bangalore) to convey your wishes. Instead, send it to a set of people you are familiar with.
- Members of Subex Culture Club are permitted to use email distribution lists to broadcast announcements.
- All unsolicited mails pertaining to medical emergencies (blood donation, organ donation etc.) of known people (relatives, friends etc.) are exempt and may be sent directly by the Subexian to a chosen mailing list/ group. If the medical emergency pertains to a person not known to the Subexian (typically, forwarded mails from outsiders), the mail should be forwarded to the Human Resources Department ([hr@subexworld.com](mailto:hr@subexworld.com)) with a request to broadcast the message across the organization. Human Resources will have the sole discretion to accept or dismiss such requests.
- Mails about invitation to personal occasions such as wedding, parties etc. are allowed as long as it is sent to the appropriate mailing list (For instance, a India-Bangalore focused wedding invite should be sent only to Subexians in Bangalore, and not to all Subexians across the world).

### 3.6 Security

- An appropriate level of security must be adopted by users when using Subex's email systems for transmission over Public Network Services (eg. the Internet, bulletin boards, blogs etc.) of (a) confidential documents or (b) sensitive material that may adversely impact Subex's business.
- Forging another's identity or attempting to conceal the origin of a message in any way is prohibited.

- Any suspected breach of security or email policy must be reported immediately to the relevant line Manager.

### **3.7 Personal Use**

- Unauthorized use of Subex's email systems for commercial purposes or personal monetary gain is prohibited.
- Use of Subex's email systems for incidental personal purposes, though not encouraged, will be tolerated provided it is kept to a minimum and it does not adversely affect the performance of the email system.
- Personal mail is subject to the same conditions of privacy as work related mail.

### **3.8 Internet Email**

Users must be aware that the correspondence and any discussions into which they enter when using Subex's email system and the Internet may be construed to be representative of Subex's position. This may have significant legal implications. Where the user does not have the authority or is not aware of Subex's position or where their personal view may vary from that of Subex's, they must clearly state that the opinion expressed, is that of the writer, and not necessarily that of Subex's. Where the user is representing the views of Subex (and is authorized to do so), then a notation must be appended to the communication identifying the individual and the position held within Subex. Special care must be taken when commercial or contractual matters, quotes or tenders are dealt with by email. There may be significant legal implications. Think twice before you email.

### **3.9 Consequences of Email Policy Violations**

Any security exposures, misuse or non-compliance must be reported as soon as an occurrence is identified. Failure to comply with the Protection of Assets Policy/ Electronic Mail Policy may lead to disciplinary procedures.

Failure to comply with Policies may result in any or all of the following:

- Suspension and/or termination of access to Subex's systems
- Additional disciplinary action as determined by relevant Line Managers in line with existing policies.
- Referral to law enforcement authorities for criminal prosecution
- Other legal action, including action to recover civil damages and penalties

### **3.10 Email which addresses a group email id**

- Any email which addresses a group email id (for ex: subex-bangalore@subexworld.com), should always use this group email id in the 'Bcc' field of the email.
- Any accidental "Reply All" will not result in unsolicited email to every member of the group.
- An email which necessitates a group reply (for ex: a discussion thread).
- If the email client has a problem with accepting just 'Bcc' addresses, the sender can just address the email to self with 'Bcc' to group.

## **4 Changes to this Policy**

Subex reserves the right to amend this Policy from time to time, without notice. Users must ensure that they abide by the latest version of this Policy. Copies of this policy will be made available on Subex's internet (external) and intranet sites.

## **VIII. Software compliance policy**

Subex licenses software from third parties for specific business purposes. As a licensee of third party software, Subex must comply with the requirements set forth in all third party software license agreements. Non-compliance with these agreements may result in significant legal liability, loss of reputation, and financial loss. Only fully licensed software that is approved by IT management may be used on Subex Applications and Systems.

Since compliance with policies is of vital importance to Subex's success, various teams are authorized to conduct assessments at their discretion with any scope they deem appropriate to measure Subex's compliance with software license agreements. All Subex users are responsible for their own compliance with software license requirements.

### **Software License Agreements**

#### **User Responsibilities**

Users authorized to purchase software licenses on behalf of Subex must comply with third party licensing agreements. These licensing agreements often contain specific restrictions (e.g., number of copies allowed to be installed, the number of computers the software can be installed on, or the number of concurrent users of the software allowed at any one time). Users must not install software in a manner inconsistent with the licensing agreement.

Contractors who install Subex licensed software on their non-Subex equipment are responsible for removing it at the end of the contract. If a contractor chooses to keep the software, he or she must purchase or license it. All software licenses must be reviewed and approved by Subex Legal in advance of being signed.

#### **Shareware and Freeware**

There are many freeware and shareware programs available on the Internet and other locations that perform a wide variety of tasks. Some of these programs are ineffective, inefficient, not secure, or actually include malicious code to harm a computer or network. Because of this, only shareware and freeware approved by the IT management may be installed on Subex Applications and Systems. In addition, open source licenses must be reviewed by Corporate Legal.

#### **Software Copyrights**

All users of licensed software or shareware must strictly abide by applicable copyright laws and restrictions.

#### **Software License Compliance Monitoring**

IT Management or concerned department heads must monitor software usage on workstations and servers and determine whether Subex is in compliance with its licensing agreements. IT Management and department heads may use automated or manual processes and may work with Procurement team to monitor software compliance. When software is in violation of a license agreement, it must be immediately removed or purchased in accordance with Subex purchasing procedures. Violations of software licenses may result in disciplinary action, up to and including termination.

## IX. Subex provided Laptop / Desktop and Mobile Facility Usage

Subexians using / carrying company provided laptop / desktop and mobile facilities should not be used for the following:

- Storing, transmission, obtaining possession, demonstration, advertisement or requesting the transmission of objectionable / inappropriate material(s);
- Viewing, transmission or storage of pornographic material;
- Viewing, transmission or storage of material promoting or causing racial, sexual or disability discrimination;
- Viewing, transmission or storage of material promoting or causing disability discrimination;
- Viewing, transmission or storage of material promoting or causing violence;
- Viewing, transmission or storage of material associated with, promoting or causing criminal activity;
- Viewing, transmission or storage of material in connection with harassment or which can reasonably be expected will cause offence.
- Storing, using, disseminating materials in violation of copyright laws including articles, music, videos, games, software, etc.
- No Subexian is to use a camera phone or camera in any area where customer work is being carried out without authorisation. Failure to comply with this request may result in disciplinary action.

## ABOUT THIS DOCUMENT

<b>DOCUMENT REF:</b>	Code of Ethics and Business Conduct
----------------------	-------------------------------------

## AUTHOR

The author of this document may be contacted at:

Human Resources  
Bangalore

Tel: +91 80 6696 8700

e-mail: [hr@subexworld.com](mailto:hr@subexworld.com)

## COPYRIGHT

© 2011 Subex Limited ALL RIGHTS RESERVED

Copyright in the whole and every part of this document belongs to Subex Limited (the "Owner") and may not be used, sold transferred, copied or reproduced in whole or in part in any manner or form or in or on any media to any person other than in accordance with the terms of the Owner's Agreement or otherwise without the prior written consent of the Owner.

## HISTORY

ISSUE	DATE	AUTHOR	REASON
v 1.0	13-Jun-2008	HR	
v 1.1	12-Oct-2008	HR	E-Mail Policy
v 1.2	24-Oct-2008	HR	Prevention of Insider Trading
v 1.3	19-Mar-2009	HR	Laptop / Desktop and Mobile Facility Usage
v 1.4	27-Jan-10	HR	Disciplinary & Whistle-Blowing Policy
v 1.5	27-Jan-11	HR	Update RKC's name in Page 5, section 5(b) Update the contact details in Page 30