Bharat Electronics Limited

Corporate Office

Preventive Vigilance

Corruption Risk Management Policy

INDEX

PREVENTIVE VIGILANCE

CORRUPTION RISK MANAGEMENT POLICY OF BHARAT ELECTRONICS LIMITED

1.0 INTRODUCTION:

1.1 Bharat Electronics Limited (BEL), a premier Defence Public sector undertaking of the country, strives continuously to identify, evaluate. prioritize, mitigate and eradicate the existing as well as the potential risks related to the business of the Company.

1.2 Risk is defined as the probability or threat of quantifiable damage, injury, liability, loss or any other negative occurrence that is caused by external or internal vulnerabilities and that may be avoided through pre emptive action.

1.3 Corruption risk is different from other types of risks. Corruption risk emanates because of greed, avariciousness and impropriety of the person in office in particular, and improper systems and procedures in the company, in general. If unchecked, it corrodes the vitals of the organisation.

2.0 CORRUPTION RISK MANAGEMENT POLICY STATEMENT:

It is BEL policy to conduct all the company's business in an honest and ethical manner. BEL take a zero-tolerance approach to corruption and are committed to act professionally, fairly and with integrity in all the business dealings, Human Resource administration, Resource management and relationships. The Corruption Risk Management Policy commits to implement effective systems to counter corruption by promoting the values of transparency, integrity and accountability, for the organic growth of the organisation.

3.0 PURPOSE OF THE POLICY:

3.1 Corruption is a special category of risk, The Corruption Risk Management Policy of BEL, determines the key principles and requirement aimed at preventing corruption and compliance of anti corruption laws of India. BEL, believes in integrity, transparency and Accountability in all sphere of activities of Recruitment, Promotions, Marketing, Finance and Public Procurement processes, and has zero tolerance towards any form

of corruption. BEL incorporates these Values into its Systems, Processes and procedures, which are well equipped to combat Corruption.

3.2 Goals of the Policy

(1) The Policy reflects commitment of BEL and its management to high ethical standards of carrying on business in an open, transparent and honest ways aimed at improving corporate culture, compliance with the best practices in Corporate governance and maintaining the business reputation of BEL.

(2) To eliminate the potential corruption risks by the Board of Directors, the Chairman, Senior Executives, other executives and employees of BEL, in Corruption prone activities.

(3) To create an uniform understanding of the Company's policy on anti corruption measures by all stake holders of the Company.

(4) To collate and to create awareness among all executives and employees, the main requirements of Corruption risk management in the Company in compliance of the Anti corruption laws of the country to make BEL, a corruption free Company.

(5) To establish an obligation on the part of the Executives and employees to know and comply with the principles and requirement of this policy and to have adequate procedures and compliances for prevention of corruption in all the processes.

4.0 FACTORS THAT LEADS TO CORRUPTION RISKS :

(1) Incentives or pressure - Incentives or pressure for Management or employees to make undue favour, wrongful gain or losses, committing fraud,

(2) Opportunity – existence of weak internal controls, flawed procedures

(3) Attitude – individuals possess an attitude, character or set of unethical values that allow them to rationalize and commit a dishonest act.

5.0 LIABILITY FOR CORRUPT OFFENCES:

Both Company and the individuals are liable for offences related to corruption under the relevant Anti Corruption Laws in India.

5.1 Individual liability. An individual may incur liability for corruption as follows:

(1) **Those directly involved:** Any individual who is directly involved in corruption offence.

(2) **Those indirectly involved:** An individual may be liable for a corruption offence where he is indirectly involved in committing the offence.

(3) **Those in authority:** A person of highest authority including Functional Directors, may be liable for a corruption offence even where not directly involved in committing the offence, but either expressly authorised the offence or that type of offence, or knew of the offence and either consented to it or turned a blind eye to it.

(4) **Aiding and abetting:** An individual may also be liable for the offence of aiding and abetting where he has somehow facilitated the committing of the offence.

5.2 An individual may incur criminal liability even where:

(1) He was not aware of, but involved in the activity that constituted a crime.

(2) He did not or would not make any personal gain from the activity, but became part of corrupt practice.

(3) He did not pay or receive the bribe personally, and instead the bribe was paid or received through or by another person, such as an agent, subsidiary company, joint venture partner, friend, spouse or other third party.

(4) He did not commit a fraud personally, and instead the fraud was committed by or through another person.

(5) He was following the instructions of a superior in the organisation, which are not in line with laid down procedures of the company even if he believed that his actions were in the interests of his employer.

(6) There were threats of adverse consequences made to him in order to make him commit the offence

(7) The bribe or fraudulent activity did not involve money, but instead involved the provision of a non-cash advantage, a future contract, gift of jewellery or gift of other kind, entertainment, facilitations etc.,

(8) The amount of the bribe was less than the financial damage which could result from failure to pay the bribe.

(9) The conduct constituting the offence was widely practised and considered to be normal business practice.

(10) The conduct constituting the offence was believed to be necessary for a party to remain competitive.

5.3 Corporate liability. In many jurisdictions, companies may be liable for offences related with corruption risks. This liability may arise in a number of ways including:

(1) **Through the acts of its employees.** A company may incur criminal liability through the corrupt act of an employee, if the employee was acting within the course of his employment. Thus, if a junior employee responsible for preparing work records submits a false work record to another company in support of a claim, then the company as well as the junior employee could be liable for fraud.

(2) **Through the acts of its related companies or business partners.** A company could be liable for a corrupt act committed by a subsidiary or associated company, joint venture or consortium partner, sub-contractor or supplier, where that corrupt act could benefit the company's business. Such liability could arise where the company authorised, approved, condoned or turned a blind eye to the corruption.

(3) **"Turning a blind eye"** or wilful blindness occurs where a party in authority suspects corruption in relation to a business transaction in which the company is involved, but deliberately refrains from making further inquiries and taking preventive steps. It is extremely important for company officers and managers to make proper inquiries, should they suspect corruption in relation to the company's affairs, and to take steps to prevent or stop the corruption. Otherwise their inaction may make the company liable.

5.4 Range of persons (both individuals and companies) who may be liable. A wide range of persons could be liable for a corruption offence. For example, a bribe is agreed to be paid by a Vendor side or Contractor side , to the person in office, and in order to conceal the bribe, it is paid by the Sub contractors, agents, intermediaries, representatives of the Vendors, who in turn appoints an individual agent and bribe managers to pay the bribe. In such circumstances, the following may incur liability where they are aware of or are wilfully blind to the corrupt circumstances:

(1) those agents, sub contractors, intermediaries, middlemen, 'undesirable persons', reps and bribe managers etc., who makes payments of bribe, attempts to bribe, tacitly or expressly;

(2) the persons-in-office who attempt to receive or receives the bribe jointly or conjointly.

(3) the contractor and sub-contractor (where they are companies), their liability being incurred through the knowledge and actions of their directors and managers.

5.5 Overseas bribery: As a result of the OECD Convention on Combating Bribery which came into force in 1999, all countries which have ratified the Convention have made it a crime for their companies or individuals to bribe a foreign public official abroad.

6.0 WHY SHOULD CORRUPTION BE AVOIDED?

6.1 Corruption should be avoided because of:

(1) the risk of criminal prosecution ((individuals as persons-in-office and bribe givers and the Company);

(2) the risk of financial loss.

(3) damage to reputation, esteem, demoralisation of organisation and colleagues and individuals.

Risk of criminal prosecution

6.2 A real risk. Until recently, there has been a little risk of prosecution for corruption in relation to the PSUs. However, due to a number of factors, recent increasing stringent anti corruption laws (***see note below***), individuals and companies are facing an increasing risk of prosecution. These factors are as follows:

(1) **Increased awareness.** There is growing awareness of the scale of corruption and of both the social and commercial damage that this is causing.

(2) **Increased pressure.** There is as a result increased pressure to take steps to eliminate this corruption. Civil society, aid organisations, multi-lateral development banks, governments, Print media, Electronic media, Public interest litigation petition, RTI, Whistle Blowers and the stake holders of the Company are all responsible for this increased pressure.

(3) **Better laws and an increased risk of prosecution.** CVC, CBI, Enforcement Directorate, DOPT, DPE guidelines and Reports by C & AG against irregularities and ratification of a number of anti-corruption conventions (in particular the United Nations Convention against Corruption and the OECD Convention on Combating Bribery). Countries which have ratified such conventions are required to enact the necessary laws to prohibit domestic and overseas bribery of public officials and also to ensure that those laws are enforced.

(4) **Increased risk of detection.** Far greater attention is now being paid to methods of detecting corruption in PSUs through monitoring by CVC, CBI and C& AG, Media (both Print and Electronic). Transparency agencies. There is also increased protection for and encouragement of whistle-blowing. Thus, there is now a far greater risk that corruption will be uncovered with resultant actions.

(5) **Increased willingness to prosecute and punish white-collar crime.** There is law and increasing pressure to ensure that everyone including persons of white-collar crime involved in corruption offences are punished suitably. This means that there is a growing likelihood that when an individual is convicted of corruption, more severe penalties may be imposed than previously.

***Note** : Prevention of Corruption Act, 1988, CRPC, Indian Penal Code, Money Laundering Act, CVC, MOD, DoPT, DPE guidelines, RBI, FEMA, SEBI, Companies Act, 2013, BEL CDA Rules , Employee Standing Orders and UNCAC Resolutions etc.,*

(6) **Serious penalties.** The penalties for corruption offences can be severe. In most jurisdictions, such penalties for individuals may include several years' imprisonment and heavy fines. For companies, not only substantial fine is imposed, but reputation of the Company is also at stake, resulting in loss of business.

(7) **Company directors and employees.** Corruption now presents a real risk of increased punishment for both junior and senior employees up to the level of Directors.

6.3 Risk of financial loss: As it becomes more acknowledged that corruption must be prevented and penalised, so governments, funders, project owners, competitors, and employers will become less tolerant of corruption. There is, therefore, an increasing tendency for the above parties to adopt stronger measures against corruption. Such measures may include:

(1) **Black listing/Debarment of companies** because of corruption involvement**.**

(2) **Exclusion of companies from projects because of unsuitability.** Public Sectors Units are increasingly carrying out better due diligence in order to determine the risk of corruption, in dealing with certain companies which are known to be prone for corruption. CVC guidelines stipulates signing of Integrity pact before bidding. Otherwise, the vendors were considered unsuitable for tenders.

(3) **Termination of corrupt contracts.** A contract which has been obtained through corruption is often either void, or can be terminated, and this can have significant financial consequences.

(4) **Reputational damage for companies.** The increasing attention given to corruption issues and the growing desire for ethical investment means that companies which are associated with corruption may suffer in terms of share value and may also find that they are increasingly considered to be undesirable business partners. It may also mean that the company may find it more difficult to win work, raise financing, and employ good staff.

(5) **Reputational damage for individuals.** Involvement by an individual in corruption may irreparably damage an individual's reputation. Companies are paying increasing attention to their own reputation and consequently to

corporate social responsibility and are therefore increasingly unlikely to employ an individual who has been involved in corruption.

(6) **Dismissal of individuals from employment.** The growing trend of anti-corruption requirements by governments, funders and project owners has the effect that employers must now be seen to be imposing stricter disciplinary measures against employees who have been involved in corruption. It is becoming more common for an officer or employee of a company to be dismissed from employment because of involvement in corruption. A company may prefer to lose an employee rather than damage its business.

(7) **Disciplinary action against individual members by professional associations.** Now a days, Professional associations are becoming more conscious of their duty to deter corruption by their members, and may impose fines on, or suspend or disqualify from practice, members who have engaged in corruption.

(8) **Litigation against individuals and companies for losses caused by corruption.** Significant financial loss can be caused to a company which is the victim of corruption. It is becoming increasingly likely for such companies initiate take legal proceedings to recover their losses. Such proceedings may be taken against both the corrupt company and the individuals involved in the corruption. These proceedings can be costly in terms of lawyers' and consultants' fees, lost management time and emotional stress.

6.4 Corruption in the public sector means involving bribery or fraud being perpetrated against the Government. It is, therefore, the taxpayer that ultimately pays for this corruption.

6.5 Corruption arising out of interaction with private sector takes the same form as corruption in the public sector but the cost of corruption is not directly borne by public funds. It nevertheless can have widespread and serious consequences. Corruption may have an immediate adverse effect on the cost and quality of the private sector works. It may result in an increase in the financing, capital, operating and maintenance costs of projects. This in turn may result in increased charges or defective works.

7.0 CORRUPTION RISK ASSESSMENT

7.1 The corruption risk is the possibility of the occurrence of an event resulting in corruption which would adversely affect the achievement of the objectives. The risk assessment is the process of assessing the likelihood of the event that may leads to corruption and its impact on the organization. The impact may be classified as serious, less serious and non serious. Corruption risk assessment is a careful examination of which could lead to corruption. It is to assess corruption risk exposures within functional areas and develop mechanisms to mitigate against such risks.

CORRUPTION RISK = IMPACT x CORRUPTION LIKELIHOOD

7.2 The primary objective of the corruption risk assessment is to better understanding the risk exposure, so that informed risk management decisions may be taken. A structured approach for conducting an corruption risk assessment is outlined in the steps below.

7.3 **Establishing the process :** An understanding of corruption risks and potential legal consequences is a prerequisite for an effective corruption risk assessment. Therefore, it is necessary to raise awareness among all stakeholders about corruption risks exposure in all the processes which the company is engaged in realizing the Organizational objectives. The objective is to address the sensitive issues of corruption and identify the steps to explore the risk exposure.

To identify its risk exposure and commit to a robust corruption risk assessment, it is necessary to consider:

- Who owns the different processes and who needs to be involved?
- How much time will be invested in these processes (planning including milestones, deliverables, decision dates)?
- What type of data should be collected and how is to be collected?
- What internal and external resources are needed?
- What additional analysis should be made?
- What methodology is going to be used?

7.4 **Identify the risks** *An* enterprise would identify corruption risk factors in the various processes and activities. Identification of

various business processes within the Company, which are exposed to corruption risks, what type of transactions and arrangements with members of the Company and third parties could result in creating corruption risks. And what locations where we do business, pose a greater corruption risk than others? There are many different ways for an enterprise to collect relevant data on the Corruption risk areas. These can include:

(1) Desktop research.

(2) Internal Audit Reports on compliance risks,

(3) Audit committee observations

(4) Annual Audit reports of Statutory auditors

(5) past experiences and past incidents of noncompliance

(6) Internal Reporting System

(7) Surveys and questionnaires

(8) Complaints/suggestions from employees, Customers and other stake holders.

(9) Feed back from Vendors and Customers in Vendors/Customer meet.

(10) Workshops and brainstorming sessions to explore Corruption risks

(11) Conducting of Interviews with experienced and knowledgeable staff

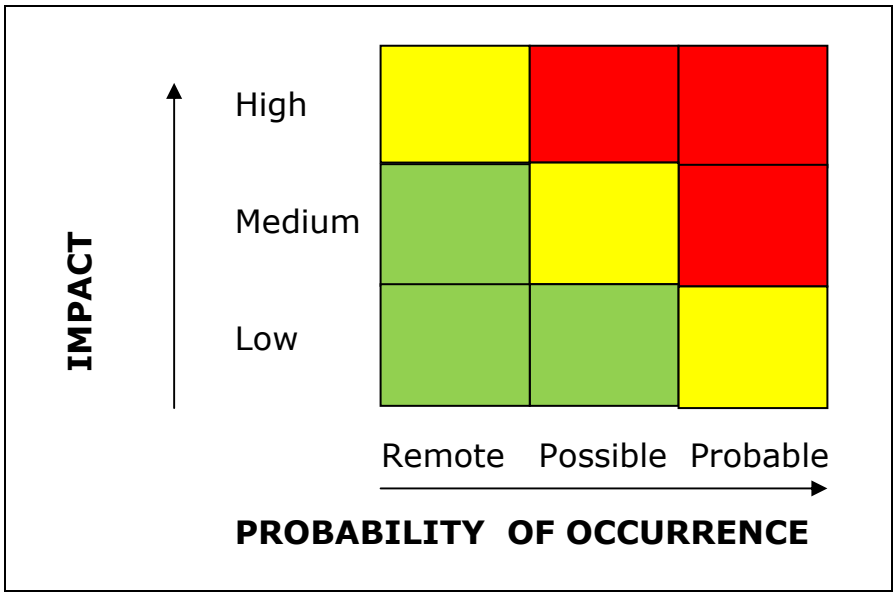
(12) CTE Intensive examination reports

(13) Training and awareness program of employees

(14) Direct observation methods

7.5 Rate the Inherent Risk : In order to allocate resources efficiently and effectively on the Company's identified corruption risks, one good practice is to rate both the probability of corruption risk that may occur in each process and the corresponding potential impact of that occurrence. The aim is to prioritize the responses to these corruption risks in a logical format based on a combination of their probability of occurrence and their potential impact should they occur. Each Corruption risk can be classified as (i) high, medium, or low, or (ii) very high, high, medium, low, and very low, based on the probability of occurrence or potential impact, it has on the Company. Combining the probability and potential impact

assessments for each corruption risks produces an assessment of inherent corruption risk involved in each process. The inherent risk represents the overall corruption risk level in each process without consideration of existing controls.



7.6 Calculate the residual risk: Generally residual corruption risk is the extent of risk remaining after considering the risk reduction impact of mitigating controls. In spite of anti-corruption programs and their internal controls for mitigating the corruption risks, it is still possible for such risks to occur. As a result, there will normally be some level of residual corruption risk in each of processes in the Company. An assessment of residual risk is thus an important consideration as it can be used to assess whether existing controls are effective and proportionate to the level of corruption risk. One of the key determinant of the Corruption risk management of BEL is to identify the residual risk and to marginalize them towards zero level.

7.7 Action plan, identification and rating of mitigating controls, The Corruption risk assessment team should consider undertaking the process of mapping existing controls and mitigating activities to each Corruption risk. This is important because the controls should be commensurate with the probability and potential outcomes of corruption. In documenting controls, an enterprise should differentiate between **scheme-specific** controls and **general (entity-level)** controls, and **preventative** vs. **detective** controls. Most identified controls are labeled as either preventative or detective.

8.0 ORGANISATION STRUCTURE FOR CORRUPTION RISK MANAGEMENT:

BEL has Nine Manufacturing Units and 14 Strategic Business Units (SBUs) , subsidiaries, other support centres and offices located across the Country and outside. These Units/SBUs/Offices have their respective core business areas, infrastructure and neighbourhood. These Units have to address individually the entire process of identification of Corruption risks, implementation of risk mitigations measures. However, in addition to the Unit specific risks there will always be many risks which affect the company as a whole, and these need to be addressed in a centralized manner at the Corporate level. In view of these reasons, two tier structured frame work has to be visualized for risk management i.e., (i) centralized risk management framework and (ii) Unit specific risk management framework.

9.0 ROLE OF LEADERSHIP IN BEL:

9.1 Corruption prevention strategies require thought, effort and commitment from the Management. The way that an Company's senior executives, middle managers and supervisors behave, can influence the conduct of individual members of staff and this helps to form a Organisation culture. Senior Executives can show leadership by modelling appropriate behaviour and ensuring that their junior colleagues do likewise.

9.2 The efforts and support of Senior executives are needed to support and endorse specific corruption prevention initiatives and to ensure that existing systems operate effectively.

9.3 Staff notice the behaviours, that Senior Executives reward and the behaviours that result in penalties, and this reinforces their learned behaviour. In addition, the behaviour of Senior Executives provides an example of the way in which organisational systems should be implemented. Senior Executives have a responsibility to comply with organisational policies and procedures themselves, and also to act openly, honestly and consistently with staff. Senior Executives should be seen to act honestly and to practice what they preach, encouraging and emphasising honest behaviour in the workplace, and treating all staff fairly and equally. Building trust in this way is particularly important for corruption prevention initiatives.

9.4 Strategies for building trust include consistent and clear communication, communication about ethics and corruption prevention that comes from the top management. consistent management throughout the organisation and managing staff expectations from the time of their employment.

9.5 Periodicity of Corruption risk assessment: The effective Risk assessment to be performed periodically e.g. on annual basis There also may be triggering events such as entry in to new markets, significant re organisations, mergers and acquisitions that will create opportunities for refreshing the risk assessment. Continually deploying the resources in the most effective manner requires a current and accurate understanding of the risks.

10.0 APPROPRIATE POLICIES AND PROCEDURES:

10.1 In BEL, Management ensure that appropriate policies and procedures exist and they are adequate. It is important to enforce these policies and procedures, and to monitor for their effectiveness. Senior executives have responsibility to incorporate corruption prevention into existing governance processes such as strategic planning and risk management and ensure that the organisation stays true to its stated values.

10.2 The ability of an organisation to appropriately penalise corruption is an important prevention tool. Senior Executives should take appropriate action against corruption and should be seen to take such action when wrongdoing is reported and against those who have acted dishonestly. Lack of action, or the perception that no action has been taken, can send a message to staff that nothing will be done when corrupt behaviour occurs.

10.3 Following proper procedures and having a regard for principles such as natural justice is vitally important when investigating or taking action against someone regarding corrupt behaviour. This will minimise the possibility of an incorrect action being taken, or of a decision being challenged.

11.0 RISK REGISTERS :

During the planning stage of the anti-corruption risk assessment, it is important to determine how the risk assessment will be documented. A common and Practical approach is to identify and document each risk factor, risk, and scheme individually and include in a spreadsheet or word document as part of a "risk register". This risk register would also be used to document the ratings for each risk and scheme as well as the programmes and controls that mitigate each risk. During the risk identification stage of a corruption risk assessment, there are benefits to identifying detailed information for each scheme, such as potential parties who may perpetrate the scheme (both from within the enterprise or by third parties). In addition, if there is more than one programme/control mitigating a scheme, the risk register would capture the different programmes and controls that mitigate the scheme. The format of the

Risk Register is given in **Annexure RR. This is required to be maintained mandatorily.**

12.0 ORGANIZATIONAL STRUCTURE OF CORRUPTION RISK MANAGEMENT OF BEL:

12.1 The Committee of Corruption risk management at Units/SBUs: Each Unit/SBU/CRL and Corporate Office shall have a Corruption Risk Management Committee **(UCRM),** the Role of this Committee is

(1) to identify and update Unit Specific areas of Corruption risks,

(2) to address the current status of corruption risk management in the Unit/SBU/CRL,

(3) implement mitigation measures for the identified corruption risk,

(4) Evaluate the effectiveness of the implemented mitigation measures,

(5) Review the Corruption Risk management status periodically,

(6) Report to Corporate Vigilance on the status of Corruption Risk Management in the Unit/SBU/CRL /CO for periodic reporting to CVC.

(7) Collate data collected at various levels and recommend System improvement for the benefit of the Unit.

(8) Periodically reporting to Standing Committee of Corruption Risk Management at Corporate Office on the status of implementation of Corruption Risk assessment and management in the Units/Offices.

12.2 The Unit Head/SBU Head/CRL Head and Chairman of Vigilance Committee at Corporate Office is the Chairman of the respective UCRM. The members of the committee to be drawn from functional areas like Finance, HR, Marketing, Material Management. The Unit/SBU Vigilance Officer is the Member Secretary of the committee.

12.3 Corruption Risk Manager (CRM) in Units/SBUs/CRL/Officers: The Vigilance Officers of the respective Unit/SBU/CRL/Officers shall be the Corruption Risk Manager of the Unit /SBU/CRL/Office.

12.4 The Corporate Standing Committee on Corruption risk management : A Standing Committee is formed at Corporate Office . The Role of this Committee is:

(1) to identify, assess, prioritize and update the areas/processes involving corruption risks for the company as a whole.

(2) to address the current status of corruption risk management in these areas /processes.

(3) Recommend mitigation measures for the identified risk.

(4) Recommend the implementation of corruption mitigation measures,

(5) Evaluate the effectiveness of the mitigation measures,

(6) Review the Corruption Risk management status across the Units periodically,

(7) Collate data collected at various levels and recommend System improvement for the benefit of the Company.

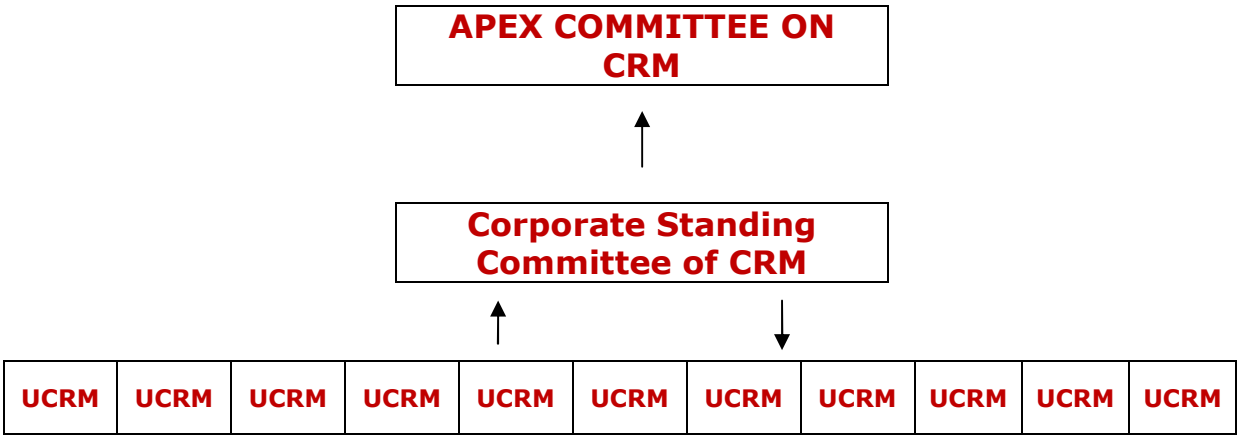
(8) Periodically report to Corporate Vigilance on the status of Corruption Risk Management in the Unit/SBU/CRL /CO for reporting to CVC, MoD etc.,

(9) Periodically report to Apex Committee, on the status of Corruption Risk Management in the Unit/SBU/CRL /CO for reporting to Board.

12.5 The Chairperson of the Standing Committee at Corporate is General Manager (IA)/CO. GM(HR), GM(Finance), GM(IMD) and GM(TP) are members of the Corporate Standing committee. AGM(Vigilance)/CO is the Member Secretary of the Corporate Standing Committee. : General Manager (IA/CO) shall be the Corruption Risk Champion at Corporate level.

12.6 There is an Apex Committee formed at Corporate Office which will review, monitor and issue necessary guidelines for the implementation of Corruption Risk Management in the Company. CMD is the Chairperson of the Apex Committee and all the Functional Directors is the member of the Apex Committee. CVO is the Facilitator of this committee.

12.7 The Entire Organization structure of the Corruption Risk Management of the company is as outlined below:



12.8 The UCRM at Unit level/SBU level meets before 15th of every month to review the status of Corruption Risk assessment and management in the Unit/SBU. The progress report should be sent to Corporate Standing Committee and Corporate Vigilance within one week from the date of completion of monthly review.

12.9 The Corporate Standing Committee will meet once in every two months to review the status of implementation of Corruption Risk assessment and implementation across the Units/SBUs/Offices and report the status to Corporate Vigilance and the Apex Committee. The Apex Committee will make a half yearly review of implementation of the Policy across the Company and submit its report for a yearly review by Board.

13.0 ORGANISATIONAL CULTURE, VALUE AND ETHICAL STANDARDS :

13.1 Underlying most definitions and descriptions of organisational culture is the idea that "Official policies specify what management wants to happen. Corporate culture determines what actually happens, and which rules are obeyed, bent or ignored." An organisation might espouse particular stated values but its culture will show its true values.

13.2 The importance of an BEL's culture to the prevention of workplace corruption lies in the effect it can have on the behaviour of employees. In an organisation, which has a strong culture, employees can feel pressure to comply with the prevailing culture and behave in the same way as most other people in the organisation. If the culture is one that encourages and rewards compliance with policies and the organisation's values, then corruption will be less likely to occur. Senior Executives are in the best position to influence the ethical culture of an organisation by promoting and enforcing policies and accountability controls.

13.3 The values that are expected from BEL employees are the basic professional standards or ethics of public service. The focus is on two essential concepts:

- Impartiality – best demonstrated by the principle of merit-based decision-making, and
- Public accountability – which can be seen in the practices of transparency, honesty, record-keeping and financial stewardship.

These values should be evident in the culture of the Organisation. Many Organisations also endorse other values, such as respect, excellence and Consumer service, that support the particular work that they do.

13.4 The Company, by developing and communicating an explicit set of organisational values encourages consistent decision-making and appropriate resolution of ethical dilemmas. The laws, policies, codes, directives and other written regulations that the Company has enables employees to promote the values and make sure that they are applied in the work.

14.0 POLICY FRAMEWORKS :

14.1 Organisations develop policies, procedures and administrative systems to support their efficient management and good governance. Policy frameworks express the principles that will govern most aspects of an organisation's work and decisions, while an organisation's procedures and systems give effect to those rules and enable them to be complied with.

14.2 Policies, procedures and systems work best when they are applied to events that occur frequently in the work of an organisation. When they work as they should, policies, procedures and systems enable, like situations to be treated alike, individuals to be dealt with equitably and decisions to be made in an accountable way and on their merits.

14.3 Like a code of conduct, a policy framework is an important element in an effective corruption prevention strategy. In BEL, policy framework is used to give effect to public sector values and ethics. For example, accountability is implemented through policies and procedures that require record-keeping and reporting. Merit-based decision-making is embodied in Policies for recruitment and selection, Purchase Procedure, Sub Contract Procedure, Works Contract Manual.

14.4 In BEL**,** Policies are exists to establish minimum standards of conduct and controls to enforce the Company's values, especially in specific corruption risk areas like conflicts of interest or the receipt of gifts and benefits.

14.5 Periodical review and update of various manual and policies are also required in line with changed environment and business circumstances and to ensure compliance of all concerned.

15.0 MAJOR CORRUPTION RISK AREAS AND CORRUPTION PREVENTION STRATEGIES IN BEL:

This Policy guidelines are formulated to develop an appropriate Corruption prevention strategies which are commensurate with the nature and extent of risk identified. The Strategies are guided by the principles of Transparency, Accountability and Integrity**.**

15.1 Delegation of authority

Delegations of authority in an Organisation means the authority who is empowered to make decisions and to take action on behalf of the organisation. The powers are principally vested with Board of Directors of BEL, which are delegated to Chairman cum Managing Director of BEL. CMD, in turn sub delegated certain powers, down the level to Functional Directors, Unit/SBU Heads and other Senior management executives. The Powers delegated to be used effectively. Misuse of delegated authority and improperly exercising authority can constitute corrupt conduct.

Corruption Risks identified	Strategies to mitigate Corruption risks
• An employee using delegated authority to make a decision for corrupt purposes. • An employee acting outside their delegation for corrupt purposes.	• Notifying, in writing, of delegation levels to any affected employees, committees and teams. • Establishing a register, available to the public, of delegations that demonstrates who is acting on delegated authority and for what purpose. • Ensuring that the delegations system provides for automatic reporting of decisions made under delegated authority. • Ensuring that the delegation system includes processes to verify whether the delegation is current: • check that temporary delegations are properly authorised, notified, recorded and archived.

	• remove delegations that are no longer needed and store superseded delegations for future reference. • Reviewing delegations regularly, in accordance with any applicable statutory requirements to ensure that they are appropriate to the capabilities, qualifications and needs of the positions to which they apply. • Decision taken should be based on acknowledged facts. • The delegated authority should ensure that all decisions are not taken arbitrarily or based on mere speculation or suspicion. • Justification to be provided for all decisions. • Introducing a process to audit and review the performance of delegated functions and ensure compliance with operating procedures. • Establishing a system to check that financial payments are processed and the person approving the payment has delegation to do so. • the delegated officer has not been involved in a transaction they authorised to approve.

15.2 Procurement : Procurement in BEL and its subsidiaries encompasses the whole process of acquiring goods, services and Works. It starts with identification of need and involves the process of risk assessment, seeking and evaluating alternative solutions, award of contract, delivery and payment of goods and services and where relevant, the ongoing management of the Contract.

Public procurement is one of the highest Corruption risk area. This is primarily due to the fact that it involves large quantities and substantial monetary amounts in its dealing. An efficient and effective procurement rely mainly on the principles of "fairness, impartiality, free competition" and ensure competitive prices to the Company.

Corruption Risk	Strategies to mitigate Corruption risks
• Bidders as cartel to loading of the loser fees of unsuccessful bidders in the prices of successful bidder. • Manipulation of pre qualification to restrict the number of bidders. • Bribery to get the contract award or get the sub contract procurement. • Manipulation of design and drawings to overprice the procurement requirement. • Specification of overly sophisti-cated design by Project manager and the vendor. • Obtaining quotation only for the purpose of price comparison • Generating and Submitting a fictitious quotation by procure-ment personnel to create a false picture of competition. • Insufficient assessment of requirement due to shortage of time, lack of capacity and lack of competence by the procurement manager. • Potential alternatives are not adequately studied. • Improper planning and budgeting • Bidding documents or specifications are tailored to benefit undue advantage to one bidder. • Complex bidding documents to hide corrupt actions. • Firms are shortlisted or prequalified due to bribery rather than qualifications. • Bidding procedures are non competitive or unclear without justification. • Splitting of contract value so as	• Procurement to be strictly based on Customer's firm indent/ Order/ Budgetary support. • Bills of material to be firmed up before preparing the Purchase Requisition. • RFQ/RFP to be issued after PR is raised. • RFQ to consider available stock and inventory. • Technical / Financial approval to be taken before going for procurement • Conducting proper market study/research periodically to broaden the Vendor base. • Alternate Vendor development programs. • Criteria for tender evaluation to be done beforehand and brought out in the tender. • Open Tender, advertised process of tendering. • E procurements/e-bidding/reverse auction to ensure transparency in the process of tendering. • Tender to be prepared with more clarity and correct specifications and reviewed at various levels before issue. • Signing of Integrity Pact to made obligatory on high value procurements and to be enforced till the completion of the Contract. • Pre qualification meet of bidders to meet to assess the technical capabilities before finalising the Vendor to whom the tender to be issued. • Establish a Tender opening committee on a case to case

to remain below the competitive bidding threshold. • Emergency or urgency of situation is exaggerated. • Extension to existing contracts without adequate justification. • Inconsistent application time frame for all bidders. • Relevant information is not shared to all bidders. • Public notices for bids are published with very limited time for response. • The criteria for selection of winning bids are not made public, • Lack of competition leading to an unreasonably high price. • Tender opening not conducted publicly • Unexplained delays in the closure of tenders. • Decision makers are biased due to corruption in the evaluation process. • Unclear definitions in the selection or evaluation criteria. • Decision makers misapply the announced criteria or add new criteria during the evaluation. • Evaluation period is too short to perform a comprehensive evaluation of the bidders. • The record of the award procedure are not accessible • Unexplained delays in the decision making giving scope for manipulation behind the scenes.	basis. • Ensure that the Bid evaluation committee has the right composition, members possess the necessary technical skills and it is permissible for a external technical expert to be the part of evaluation. • Members of tender assessment panels are required to declare in writing any conflicts of interest with bidders. Disclosure documents are to be signed and dated by each panel member and countersigned by the convenor, and kept with the tender records. • If alternative or non-complying tenders/offers are considered the conditions for doing so are specified in writing. • Tender panel decisions and the reasons for these decisions are made in writing and records kept in line with relevant legislation and policy. • Communicating with all bidders in writing, and keeping the tender documents in safe custody. • Improve the Tender assessment and evaluation process • Ensure that the Bid evaluation committee has the right composition, members possess the necessary technical skills and it is permissible for a external technical expert to be the part of evaluation.

15.3 Contracts Administration: Contract administration is highly prone to corruption because it often requires high technical and professional; knowledge with complicated and detailed works procedures and involves substantial amount of Money.

The Corruption within Contract administration resulting in sub standard works that may seriously threaten public safety and undermining public confidence. The risk of corruption can be reduced if appropriate safeguards are built in to the System Contract administration and the administration is performed in an accountable and transparent manner

Corruption Risk	**Strategies to mitigate Corruption risks**
• Inflating the resources (manpower, equipment) and time requirements at the estimation stage, in collusion with project manager and contractors. • Lower quality materials or sub specification performance compared to contracted quantity. • Lower priced materials goods and services to accommodate bribe • Contract revision to allow for more time, decorated outputs, lower specifications or higher prices. • Variation in quantities to demand increased payments • Goods and services not supplied but recorded as supplied. • Poor supervision allows substandard work to go undetected. • Extra work/extra time to complete the project. • Extension of time without proper justification. • False invoicing and supply of inferior materials by supplier.. • False invoicing and supply of less quantity of materials • False work certificates by inspections agencies for completion of work. • Excessive repair work charged by contractor and accepted by the concerned authority.	• Wherever applicable the sanction for the estimated cost of the project to be taken before acceptance of the works • Prior approval of the management before award and commencement of the work • Regular site visits to ensure compliance with respect to quality and timeliness of the work done. • After each site visit, a site visit report should be produced • Regular site meeting with the stake holders to ensure that progress of work is in accordance with the programme of work. These meeting should be minuted. • All instruction to the Contractor should be made in writing. • Approval to be taken before for all variation in the work and price to be finalised before hand. • Any extension of time is to be accorded after due approval by the Competent authority. • All measurement of work to be done in the performed in the presence of technical officers and to be signed by the Project manager. • All the calculations with respect to measurement should be properly recorded and produced when required for preparation of Interim/Final payment certificate

• Overstating man day requirements by the sub contractors and allowed by the concerned authority. • Inflated claim for variation and false variation claim made and allowed. • Issue of false delay certificate. • False extension of time application • Concealing defects. • Delay in issue of payment certificates • Refusal to issue final certificates or issue of payment certificates • Fraudulent claims are made • Lack of supervision • Renegotiation of the contract allowed. • Unexplained delay in making payment. • Intention to withhold payment • Forcing to accept lower payment than is due • Extortion by Project owner's representative • Concealment of documents. • Submission of false supporting documents • Bribery and blackmail of witness	

15.4 Recruitment and selection: The principle that positions are filled on the basis of merit is fundamental to the recruitment and selection of employees in BEL. To ensure that the best person is selected, accurate information about the skills, training and qualifications of applicants should be available to Management before going for the actual selection of candidates. The fundamental principle in recruitment is;

- all eligible candidates to have a fair chance to gain a job in the Company.
- selection to be based on a person's ability to perform the work
- the best person is selected, resulting in a quality workforce capable of effectively designing and delivering services and programs to the Organisation.
- It is essential that favouritism, nepotism, and other conflicts of interest should not influence recruitment and selection processes.

Corruption Risks identified	Strategies to mitigate Corruption risks
• The Senior Executive or an Executive, as a Chairman or a member of the Selection Committee, manipulating selection procedures to secure the appointment to his friend or family member. • A selection panel member failing to declare a conflict of interest and acting to advance the interests of an applicant who is a close friend or a relative. • The Chairman of the selection committee appointing members to the selection panel whom he can influence in order to ensure their favoured candidate will be selected. • An applicant falsifying qualifications or employment history to enhance his or her prospects of securing a position.	• Advertising positions widely enough to maximise the potential field and including appropriate selection criteria. • Filling vacancies promptly so that periods during which employees undertake more senior duties are not unduly extended, to the disadvantage of other potential applicants. • Including independents from outside the organisation on the selection panel. • Informing all applicants in clear terms that falsely claiming qualifications will lead to their dismissal and/or prosecution for any relevant offence. • Ensuring all applicants sign a certificate declaring that the qualifications they assert are genuine and that they acknowledge any falsely claimed qualifications can lead to their dismissal. • Including a provision that permits an employer to terminate the employment of an applicant who falsely claims qualifications in all letters of appointment or other contractual documentation. • Recording verification of all academic and professional qualifications. • Pre employment screening of candidates thorough reference checks. • Each referee should be asked the same set of questions relating to the selection criteria and responses documented. • Retaining interview notes made

	by each member of the selection committee on the recruitment file. • All recording in the selection sheet/matrix to be made in ink to reflect the on the spot assessment of the Chairman/Panel member. • Verifying personal details with original documentation or certified copies. • Demonstrating fairness and impartiality when dealing with internal applicants by ○ Not involving potential internal applicants in any part of the recruitment process, such as acting as the contact person for potential candidates, preparing position descriptions or framing advertisements. ○ Keeping information confidential prior to the interview. • Avoiding preferential treatment of internal applicants such as coaching or providing advice not available to other applicants or encouraging an expectation of success or failure. Verifying qualifications of job applicants as part of their claim to a position prior to appointment. • Recording if no referees were consulted in making a selection decision and the reason the selection committee found it was not necessary to do so. • Recording all the reasons where it was deemed appropriate that competitive processes were not used and keeping these reasons in a manner and place that

	readily permits scrutiny, if required. • Clearly stating in the selection committee reports the reasons for removal of candidates who were considered unsuitable. • Including selection committee comments on each applicant interviewed with reference to each selection criterion in these reports • Providing copies of the selection panel reports to all members of the selection panel and integrating these comments into the joint deliberations of the selection panel.

15.5 Accounts management: The management of accounts includes functions such as accounts payable and accounts receivable as well as the general use and maintenance of the Company's financial accounts.

The need for employees to access Company's funds to perform official functions can increase the possibility of misuse, and makes the identification and management of corruption risks in this activity extremely important. False invoicing, for example, is one of the most common types of fraud.

Corruption Risk	Strategies to mitigate Corruption risks
• An employee manipulating the system to make payments to a non-existent vendor, and indirectly to their own account. • An employee colluding with a supplier to produce an invoice price that is higher than necessary. • An employee approving invoices of their private expenses or colluding to do so for others. • An employee creating a false payment instruction. • An employee submitting a false travel or reimbursement claim	• Ensuring that there are appropriate supervision and approval processes for accounts management. • Ensuring delegating limits are specified and complied with so that there are appropriate approvals in place for each stages of payments/ expenditure. • Validating invoices with supporting documentation such as Purchase Orders, GRs, acceptances to ensure that all payments are for legitimate

and receiving a benefit to which he or she is not entitled. • An employee using company's funds for purchasing goods for his private use . • A Service provider/contractor providing false invoices resulting in the payment for goods not received.	goods and services received in the Company. • Segregating duties between the officer who incurs expenditure and the officer who authorises payment to have internal controls over purchasing. • Ensuring regular, accurate capture and reconciliation of all transactions to decrease the risk that inappropriate transactions occur. • Frequently spot checking transactions to identify anomalies. • Establishing effective internal audit checks to regularly check transactions for authenticity. • Controlling electronic payments with passwords and regular audits, and using secure emails and websites. • Monitoring and reviewing on periodic basis all payments, expenses as compared with budget allocations, sanctions and identify anomalies. • Where possible, limiting the number of cost centres and accounts in the general ledger, so that the accounting system is clear and straightforward enough to be able to track payments.

15.6 Electronic transactions : Many agencies use electronic facilities for making e-payments like ECS, RTGS, NEFT, Bank transfers, On line payments towards payment of Income Tax dues, Excise Duty, Service Tax and Property and Sales tax remittances.

The increased efficiency and accessibility of electronic transactions can facilitate corrupt conduct with the potential for greater financial loss and disruption to the Company. Hence, adequate security measures and checks should be in place to reduce the risk of corruption. This is particularly important when traditional security

and verification methods (such as countersignatures and face-to-face identification) are not practical.

Corruption Risk	Strategies to mitigate Corruption risks
• An employee gaining access to electronic records without proper authority or approval. • An employee making an electronic payment to a non-existent vendor. • An employee improperly transferring money from the Company's bank account to an associate or an account under their control. • An employee using Company's funds to purchase goods or services electronically for private benefit**.**	• Ensuring that internet-based payments are made only to secure sites. • Using digital signatures to verify the authenticity of electronically transferred information. • Establishing internal controls to authorise all payments. • Ensuring electronic transactions cannot be authorised and processed by the same person. • Periodically testing and checking confirmation procedures and data processing controls. • Ensuring the systems can automatically identify large and unusual transactions for review.

15.7 Information Technology Systems : Due to invent of technology and IT Systems, the company is completely reliant on information technology (IT) systems for operational functions and many for their service delivery. It is important to ensure that the information maintained on these systems is accurate and complete. It is also critical that this information is easily accessible for legitimate purposes and at the same time protected from misuse.

Corruption Risk	Strategies to mitigate Corruption risks
• An employee falsifying electronic records to obtain financial benefit (eg. inappropriate overtime or reimbursement payments). • An employee electronically	• Ensuring outdated electronic records, including emails, are stored in formats, and on media, that are accessible to modern IT systems. • Ensuring employees are made

creating fraudulent documentation and providing it to the public • An employee altering or deleting electronic data to prevent evidence of other wrongdoing from being detected or to aid a third party. • An employee taking advantage of temporarily inoperative IT systems to act in a corrupt way. • An employee placing malware (eg. viruses, spyware) on an agency's IT systems in an attempt to damage them. • An employee providing log-in details to a member of the public, who uses them to remotely access the Company's IT systems. • An employee using another employee's computer and/or log-in to act in a corrupt way. • An outsider obtaining mobile computing/removable storage devices (eg. laptops, memory sticks) containing Company's data. • An IT contractor providing information about the Company's IT systems to a third party who uses this information to launch a successful attack on these systems. • A contractor copying electronic data and providing it to third parties for their benefit. • An IT contractor building a 'back door' into IT systems that allows inappropriate secret access to alter or delete electronic data. • An IT contractor damaging IT systems to prolong their employment. • An employee or consultant	aware of their electronic recordkeeping requirements, including those pertaining to emails of business value. • Implementing an electronic records system. • Including secrecy provisions in IT-related contracts. • Including secrecy provisions in written agreements when IT services are shared with, or used by, another organisation. • Incorporating IT provisions into any disaster recovery/business continuity plan. • Requiring password access to IT systems which is changed on a regular basis. • Limiting access to IT systems to current employees with a legitimate need to access the relevant information or service. • Governing the rights to alter or delete electronic data by operational necessity. • Implementing programs to protect databases against irregular activity. • Regularly testing firewalls and other security systems. • IT security that contains standards for Systems security, data integrity and preventing unauthorised access to data and misuse of information. • Limit access to the Central Computer server and other network and back up equipment • Control access to terminals and install security measures to prevent database from being tampered. • Ensure that the air conditioning and humidity control systems for Local Area Network (LAN) server are adequate. • Protect devices from natural

developing an IT proposal that creates deliberate system vulnerabilities.	disasters • Allocation of password to access the system • Allocation of unique log-in Ids to system so as to identify users. • Reminding staff to keep their passwords strictly confidential and change them periodically • Ensuring that only authorised persons have access to those modules/options required for their duties • Installation of anti-virus, intrusion detection and firewall systems • Installations of monitoring system to tract abnormal activities. • Establishing of a system to identify locations and users accessing computers and information from database • Encryption over transmission of data • Adequate controls over staff working in the Information System Department • Develop a disaster recovery plan • Keep a complete inventory of files • Maintain back up copies, both within and outside the organisations of all data and computer programmes to protect against loss of information. • Ensure that no single person has control over the entire computer programmes • Ensure modification to the programmes are authorised • Ensure feasibility study is carried out before changes are brought out • Ensure proper testing of

	programmes before transferring to live environment. • Involve users at the time of development

15.8 Post-separation employment

Post-separation employment is the situation where an Executive leaves the organisation and secure employment in the Private Sector. The principle underlying the management of post-separation employment is the need to ensure that employees should not use their position to obtain opportunities for future employment. They should not allow themselves or their work to be influenced by plans for, or offers of, employment outside the department. The type of employment which may be cause for concern is that which bears a close or sensitive relationship with the person's former position as a PSU employee/executive.

The risk of corruption is higher if the post-separation work involves contact with the former department, colleagues, or staff of the former public official and the executive/employee has no restrictions imposed on the type of employment they can obtain after they leave the organisation.

Corruption Risk	Strategies to mitigate Corruption risks
• The present PSU executive/ employee using their position to obtain an advantage for their future employment. • A former PSU executive/ employee attempting to influence former colleagues to make decisions that favour their new employment or private business. • A former PSU executive/ employee establishing their own business in the same field as the Parent Organisation and approaching its clients for business, using confidential information gained from the agency. • A former PSU executive/ employee becoming a lobbyist	• Managing external relationships by: ○ Including information about post-separation employment in the Company's statement of business ethics. ○ Including a specific statement in the Company's code of conduct about the ethical issues and corruption risks raised by post-separation employment and stating the restrictions on employees. ○ Requiring employees to advise the Company when they are contemplating leaving the public sector for employment that may have a sensitive relationship to their work as a PSU Executive.

for a private organisation or specialist group and trying to gain confidential information or favourable treatment from former colleagues. • A current PSU executive/employee stealing information, intellectual property, or other resources to develop their own business and/or to enhance employment prospects with other agencies and organisations.	○ Considering implementing "cooling off periods" (Period of two to three years) for positions where it is likely that PSU executives may take up employment in businesses that have a close or special relationship to their former roles as public officials. ○ Requiring current employees to conduct their official dealings with former colleagues at arm's length. ○ Requiring current employees to report all dealings with former colleagues which involves attempts to influence or lobby the remaining employees. ○ Assigning all Company's documents a security rating that is recorded on all printed and electronic copies and denotes their accessibility. ○ Maintaining a record of who has access to confidential information with an audit trail to monitor this access. ○ Keeping a record, as part of the Company's exit processes and protocols, of the return of all Company resources allocated to departing employees.

15.9 Intellectual property

Intellectual property (IP) "represents the property of your mind or intellect. It can be an invention, trade mark, original design or the practical application of a good idea". Examples of IP owned by the Company are Computer programs and designs, Software, Product design, Technical documents, developed by the Design & Engineering Group.

Intellectual property is often referred to as an intangible asset. Like any asset, it should be managed responsibly, in the same way that PSUs manage tangible assets.

Corruption Risk	Strategies to mitigate Corruption risks
• An employee using an Company's IP for their secondary employment. • An employee soliciting a secret commission from a private individual or organisation in exchange for Company's IP. • An employee providing IP to another organisation in the hope or expectation of securing employment. • An employee responsible for managing the Company's IP, including implementing security measures for the protection of IP, deliberately failing to do so for the purpose of misusing this information for their own or another's benefit. • A departing employee or consultant deliberately breaching the agreement by using the IP they gained for private benefit.	• Assessing whether sufficient resources have been assigned to the management of IP. • Including references to IP protections in contracts and information for external parties including the internet. • Maintaining a register of IP and IP that the Company has permission to use. • Considering possible IP issues in relation to prospective tenders or consultants. • Specifying in employment documentation the ownership of any IP developed by the employee in the course of their employment belongs to the Company. • Establishing an IP committee to manage the IP interests. • Requiring employees to notify the committee of any IP they create in the course of their employment. • Including references to IP in conflicts of interest management procedures. • Ensuring departing employees sign an agreement about the use of IP.

15.10 Management of resources

The Company use publicly-owned resources to enable their employees to do their jobs. Poor management of these assets can undermine the integrity and operational efficiency. It can also provide opportunities for corrupt conduct. Opportunities exists for

the misuse of Company's resources such as High value Capital items, Computers, Laptop, office supplies, stationery, tools etc.,

Physical assets are items such as land, buildings, information technology, infrastructure, collections, equipment or fleet, owned or controlled by the Company for providing future economic benefits and having a definite business function or supporting the delivery of services.

This policy was introduced to achieve better planning and management of the physical assets, both existing and planned.

Corruption Risk	**Strategies to mitigate Corruption risks**
• An employee regularly taking resources home for their own use, or to sell for personal benefit. • An employee deliberately over-ordering resources with the intention of misusing the surplus goods. • An employee colluding with a client to submit false or inflated invoices. • An employee destroying or distorting records to hide the misuse of resources. • An employee manipulating weak or inadequate log-in procedures for personal benefit. • An employee misusing company's resources for secondary employment. • An employee failing to return company property upon ceasing employment. • An employee misappropriating valuable item	• Maintaining asset management systems that include asset registers and inventories of resources so that any losses can be easily identified. • Keeping records that show when resources are allocated to employees and returned. • Establishing a procedure to make sure that employees return resources when they leave the Company or no longer require the resource for their duties. • Conducting regular valuations and stock takes of assets and regular reconciliations of cash resources to identify irregularities. • Securing all resources using methods commensurate with their value to reduce the likelihood of theft. • Securing hard and soft copies of sensitive and confidential asset records with limited access to storage units/computer codes in which they are stored. • Establishing a procedure for handling cash to reduce the risk of theft. • Segregating duties in the management of resources so

	that individuals are not responsible for approving their own usage. • Regularly reviewing records kept for the purchase, disposal and valuation of resources to identify irregularities. • Regularly auditing the use of resources.

15.11 Disposal of goods and property

As a prudent commercial organisation, the Company regularly dispose of depreciated, redundant or excess stock to outsiders. There is a need to ensure that standardised methods exists to manage the disposal of unwanted resources in a transparent and accountable manner.

Goods to be disposed of are public resources and, even if redundant or depreciated, may still have financial value to the Company. Consequently disposing of goods should be carefully planned and conducted in a way that obtains value for money and reduces opportunities for exploitation by individual employees, private persons or organisations.

Corruption Risk	Strategies to mitigate Corruption risks
• An employee deliberately undervaluing the goods that are to be disposed of with the aim of purchasing the items for him/herself. • An employee responsible for arranging the disposal of goods directing the contractor to make the payments directly to him/her. • An employee involved in conducting an in-house tender for the disposal of goods providing information about tender prices to a potential bidders, prior to the completion of the process. • An employee destroying records concerning the disposal of	• Conducting regular reviews of the procedures for ordering goods and services to check for compliance. • Where appropriate, making arrangements with suppliers that unused goods can be returned. • Segregating duties in the decision-making process when disposing of goods. • Keeping goods secure and consistently applying an asset control system for the valuation and storage of goods. • Obtaining appropriate external valuation of resources prior to disposal.

goods to cover his/her corrupt activity. • An employee deliberately over-ordering resources to use the 'surplus' for personal gain • An employee regularly misappropriating goods.	• Keeping details concerning the date of purchase of resources, length and condition of warranty, maintenance and repairs undertaken, and other related information for consideration in the valuation and disposal of goods. • Conducting and recording regular inventories of goods. • Keeping a checklist of each stage in the disposal process including the decision to dispose, valuation of items, and who approved the disposal of the goods, plus the method of disposal. • Keeping a record of the external valuations. • Maintaining a register of all the assets held by the Company. • Regularly auditing the asset register to ensure no items have been improperly disposed of. • Putting asset maintenance systems in place to determine and report on when goods become surplus and/or unwanted and what their monetary value is at that point.

15.12 Conflicts of interest

A conflict of interest occurs when the private interests of the executive/employee come into conflict with their duty to act in the public interest. Conflicts of interest are particularly relevant where the executive/employeel has a decision-making role.

Corruption Risk	Strategies to mitigate Corruption risks
• An executive/employee not disclosing a private interest and favouring that interest when making decisions. • An executive/employee carrying	• Including information on processes for managing conflicts of interest in documents aimed at external

out his/her function/duties in such a way as to benefit a business interest, property interest or prevent that interest from being adversely affected. • An executive/employee carrying out his/her function/duties in such a way as to benefit a relative, close associate or secondary employer or prevent adverse outcomes. • An executive/employee carrying out his/her function/duties in such a way as to benefit a future employer or potential future employer or prevent them from being adversely affected. • An executive/employee carrying out his/her function/duties in such a way as to adversely affect a person or group that they dislike or are prejudiced against.	stakeholders • Ensuring employees complete a statement of private interests (such as secondary employment, business dealings, property, shares) on commencement, annually or at another appropriate time. • Putting processes in place to ensure that statements of interest are updated at regular intervals. • Formally recording arrangements for addressing each conflict so that the company can demonstrate how each conflict of interest was managed.

16.0 SUMMARY:

Bharat Electronics protects its most important business asset, that is **INTEGRITY** and recognizes corruption is a threat to the business and counter to company's culture. The Enforcement, Prevention and Generation of awareness are the three important pillars of anti corruption for which BEL stands for. BEL is committed to its customers, communities, shareholders and employees to conduct business pursuit with high ethical standards. Corruption risk assessment is a careful examination of factors that could lead to corruption. It is to detect and assess corruption risk exposures within functional areas and develop mechanism to mitigate and eliminate corruption to make the organization "an expanding Corporate with best practices"

Annexure RR

Format of Risk registers:
(Paragraph 11.0)

Corruption Risk Factor	Corruption Risk	Process	Probability	Potential Impact
1	***2***	***3***	***4***	***5***
Refer to policy and Unit specific	As enlisted in the policy and Unit specific	As enlisted in the policy and Unit specific	High, Medium or Low (on 1 to 3 metrics)	High, Medium or Low (on 1 to 3 metrics)

Total risk (Col 4 x 5)	Inherent Risk	Anti Corruption Controls	Control Risk Rating	Residual Risk Rating (if applicable)
6	***7***	***8***	***9***	***10***
High, Medium or Low (on 1 to 9 metrics)	Unit Specific	Measures in practice and proposed good practices	Reduction in Col 3,, 4 5 over a Qtrly	Unit Specific report

Appendix I

RECOMMENDED STEPS TO FACILITATE ANTI CORRUPTION MEASURES

(1) Corporate framework

(a) Ensure that there is well established and systems and procedures in place:

(i) for officers and employees to report corruption, and

(ii) to advise and assist officers and employees who are confronted with a corrupt situation.

(b) Ensure that this system enables officers and employees to make reports of corruption and receive advice confidentially and without fear of adverse discrimination.

(2) Legal framework

Ensure the availability of legal advice as to the following:

(a) Whether, under the relevant law:

(i) it is a defence to bribery if it can be proved that a person paid a bribe only because there were threats of imminent harm to him or another;

(ii) it is an offence to fail to report corruption;

(iii) there is protection from self-incrimination;

(iv) there is protection for whistle-blowers;

(v) reporting of corruption may provide immunity from prosecution or mitigate any potential liability or penalty for corruption.

(b) How reports of corruption may be made to the criminal authorities.

(c) How records and witness statements of corrupt incidents should be made so that they are valid under the relevant law.

(d) How a report of corruption should be made so as to avoid any risk of liability for defamation for the person making the report.

(3) Informing officers and employees

(a) Ensure that officers and employees of the company are made aware, in writing, of all information under (1) and (2) above.

(b) Train officers and employees in Corruption prevention and Reporting.

(4) Possible actions by Companies

A company may become involved in corruption or may need to report corruption where:

(a) An officer or employee of the company reports that someone has demanded a bribe from him which he has not paid.

(b) An officer or employee of the company reports that he has paid a bribe under threat of personal harm.

(c) An officer or employee of the company, in the course of his employment, commits bribery or fraud which has not been authorised by the company.

(d) An officer or employee of the company, in the course of his employment, commits bribery or fraud which has been authorised by the company.

(e) A related company or business partner of the company pays a bribe or commits fraud in relation to which the company could be implicated.

(f) The company is involved in a cartel.

(g) The company discovers that it has been the victim of bribery or fraud committed by another company.

Appendix II

PRECAUTIONERY MEASURES

(1) Cautions

There are certain risks inherent in taking action in response to corruption. They include:

(a) Risk of personal harm to those reporting the corruption or seeking to remedy it.

(b) Risk of discrimination against individuals and companies who speak out against the corruption.

(c) Risk of incurring liability for defamation if accusations of corruption cannot be substantiated.

(d) Risk of financial loss if reports of corruption are made against an organisation or individual which owes money to or has some other financial hold over the organisation reporting the corruption.

(e) Risk of financial or commercial harm if reports are made against an influential organisation or individual.

It is necessary to keep these risks in mind when considering the possible actions listed below.

(2) Safety

The safety of the individual is paramount. If an officer or employee is at personal risk as a result of reporting corruption or being involved in a corrupt situation, the company should take reasonable steps to protect the individual. This could include making the appropriate payment to avoid the individual being harmed, removing the individual from the dangerous situation, and/or requesting police protection.

(3) Making proper enquiries and collecting evidence

The company should establish the facts and collect all necessary evidence by:

(a) Where possible and reasonable, requesting reports of corruption to be made in writing and signed by the individuals making them.

(b) Making enquiries to establish the facts.

(c) Collecting together all relevant documents and other evidence.

(d) Obtaining legally valid witness statements.

(e) Preserving all evidence for a period of at least 20 years.

(4) Protecting whistle-blowers

If the company does not have in place a reporting system whereby reports can be made anonymously by employees, then it should ensure that officers or employees who have reported corruption are protected by:

(a) Keeping their identity confidential.

(b) Keeping details of the incident confidential, save for the need to make further reports, as suggested below.

(c) Ensuring that they do not suffer adverse discrimination from other officers or employees within the company

(5) Obtaining legal advice

The company should obtain legal advice as to its position under local law and under the law of its home country as to:

(a) Which individuals and companies may have incurred liability for the corruption offences in question.

(b) The penalties that might apply to each individual and company implicated.

(c) Whether failure to report the corruption to the criminal authorities would be an offence.

(d) Whether the law provides protection from self-incrimination.

(e) In the case of corruption perpetrated by the company, whether the corruption can be remedied or other steps taken so as to mitigate or avoid liability.

(f) In circumstances where the company is part of a cartel, whether the company would receive immunity from prosecution, or some mitigation of liability, if it reported the cartel.

(g) The nature of evidence that would be legally valid in a court of law.

(h) What civil action may be taken *against* the company

(i) What civil action may be taken *by* the company

(j) What other steps should be taken to protect the interests of the company and its relevant officers and employees.

(6) Reporting corruption

(a) **Reporting corruption** - where failure to report corruption is a criminal offence, but the company and its employees are not implicated in the corruption

In this situation, the company should make such reports as are necessary to comply with the law.

(b) **Reporting corruption** - where failure to report corruption is a criminal offence, and the company and its employees are implicated in the corruption. In deciding whether or not to make a report, the company should consider, and take legal advice regarding, the following factors:

(i) What are the risks of being prosecuted for failing to report the corruption and the likely penalties?

(ii) What are the risks of being prosecuted for the corruption offence(s) in question and the likely penalties?

(iii) Is there any protection against self-incrimination under the relevant law?

(iv) Would reporting the corruption:

_ result in immunity from prosecution for the corruption in question?

_ mitigate any criminal penalty that may be imposed for the corruption in question?

_ mitigate any other penalty (such as debarment) that may be imposed for the corruption in question?

(c) **Reporting corruption** – where failure to report corruption is not a criminal offence, and the company and its employees are not implicated in the corruption

In this situation, the company should consider the following factors in deciding whether or not to make a report:

(i) Is the company under some other legal obligation to report the corruption (for example, if a company has signed an anti-corruption agreement which obliges reporting)?

(ii) Would reporting the corruption mitigate:

_ any criminal penalty that may be imposed for any **other** corruption for which the company is or might be liable? and/or

_ any other penalty (such as debarment) that may be imposed for **other** corruption for which the company is or might be liable?

(iii) Is the company generally committed to trying to eradicate corruption and would reporting corruption assist in doing this?

(iv) What are the penalties for corruption under the relevant law? Are they extreme (such as execution), and would the company be comfortable reporting corruption in such circumstances?

(v) Can the persons or companies responsible for the corruption be persuaded to undo the corruption without having to report the matter to the criminal authorities?

(vi) Would the company or any of its employees be placed in any danger if the corruption was reported?

(d) **Reporting corruption** – where failure to report corruption is not a criminal offence, but the company and/or its employees are implicated in the corruption

In this situation, the company would probably incriminate itself and/or its employees if it reported the corruption. In considering whether or not to make a report, it should inter alia consider whether reporting the corruption would:

(i) result in immunity from prosecution for the corruption in question;

(ii) mitigate any criminal penalty that may be imposed for the corruption in question;

(iii) mitigate any other penalty (such as debarment) that may be imposed for the corruption in question;

(iv) mitigate any criminal penalty that may be imposed for any **other** corruption for which the company is or might be liable;

(v) mitigate any other penalty (such as debarment) that may be imposed for any **other** corruption for which the company is or might be liable.

(7) Undoing or remedying corruption

If the company discovers that an officer or employee of the company has perpetrated some corruption which has or may result in the company receiving some illicit benefit, then consider how to undo or remedy the situation. This may involve:

(a) Taking legal advice as to how to remedy the corruption without self-incrimination.

(b) Withdrawing from any procurement process, or resultant contract, where the company has been or may be awarded the contract because of corrupt activity.

(c) Repaying any benefit obtained as a result of fraud.

(d) Considering any other consequences of the initial corruption which may themselves constitute criminal offences.

Such offences may include false accounting which may occur where a bribe is falsely described as an agency commission in the accounts, a tax offence where a bribe is wrongly deducted from income, or money-laundering where the proceeds of the crime are dealt with.

(8) Seeking a remedy for corruption

Where the company has been or may be a victim of corruption, the company should consider:

(a) Requiring the corrupt party to take remedial action.

(b) Requesting other parties who are in a position to do so to take remedial action.

(c) Informing all other parties who may be affected by the bribery or fraud (such as other bidders) of the corruption.

(d) Taking legal action against the corrupt company and any other party who participated in the bribery or fraud

(e) Reporting the matter to the criminal authorities

(9) Disciplining officers or employees

Officers and employees who have engaged in corrupt activity during the course of their employment should be appropriately dealt with by the company. Disciplinary action would range from a warning for a minor offence to dismissal
for a serious offence.

(10) Reviewing company policy and procedures

Both where the company has perpetrated corruption and where the company has been a victim of corruption, the company should:

(a) Examine whether the situation arose because of some inadequacy in its procedures.

(b) If so, it should take immediate steps to improve its procedures.

(11) Reviewing response and assistance provided by governments, funders, embassies and the criminal authorities

Where the company has sought the assistance or advice of government departments, funders, embassies or the criminal authorities, the company should:

(a) Assess the quality and speed of the response and assistance, if any, provided by those bodies.

(b) Make reports to those bodies as to their response and assistance, stating how such response should be improved

(c) Make reports to other authoritative bodies where response and assistance has been inadequate and request them to take action to require the relevant bodies to improve their response.

Appendix III

ANTI-CORRUPTION - DO's and DONT's FOR INDIVIDUALS

1. Act at all times honestly and without deception.

2. If you are Senior executive or Executive involved in decision making or given any management responsibility for, a company,

   - You must make proper enquiries regarding any suspicion of corruption of which you become aware.

   - You must take reasonable preventive measures to stop corruption for which the company may be liable.

   - You must not instruct, authorise or condone, expressly or impliedly, any corrupt activity.

3. Do not knowingly, with wilful blindness or recklessly do any of the following, or participate in any activity which involves any of the following:

   - Offer, give, demand or accept any bribe or other improper advantage.

   - Participate in any dishonest or deceptive activity in relation to any pre-qualification, tender or Nomination process.

   - Provide, conceal, or approve work, materials, equipment or services which are not of the quality and quantity required under contract.

   - Provide false, inaccurate or misleading information.

   - Dishonestly withhold information.

   - Make or submit false, inaccurate, misleading or exaggerated records, invoices, Claims, applications for variations or extensions of time, or requests for payment.

   - Dishonestly refuse or fail to approve, or delay in approving, work, materials, equipment, services, invoices, claims, applications for variations or extensions of time, or requests for payment.

   - Dishonestly refuse or fail to pay, or delay in paying, sums due.

4. Do not involve in offering, paying, requesting or receiving bribes.

5. Do not involved in any fraudulent or dishonest activity.

6. Do not One must not authorise, expressly or impliedly, any corrupt activity.

7. Do not participate in any activity which could facilitate corruption. Such activity may include authorising payment of bribes, drafting illegal agreements, drafting fraudulent claims, falsifying evidence, and giving false evidence in legal proceedings.

8. Do not assist in the concealment of any corrupt activity. This does not necessarily mean that a party must report corrupt activity It means that he must not take any positive steps to conceal the corruption.

9. Do not commit corrupt activity because he has been requested to do so by his company or by any senior manager.

10. Where in a position of authority, do not turn a blind eye to corrupt activity. If one suspects that corruption has occurred, is occurring, or is likely to occur, make proper enquiries to establish what has happened or may happen, and take steps to prevent or stop it.

* * * * *