Policy: Confidentiality Policy

1) Why this policy?

Most of us while working for as a deputee of CIEL in the due course of business, come in contact with data and information pertaining to various stakeholders – our clients, vendors and co-workers. These data and information are often private or personal used for business processes and hence, we must know what the right way to handle these. Hence, this policy!

2) Guiding principles for this policy:

While all attempt is made to define the specifics in the following sections of this Policy, it is important to understand the spirit behind the policy and the guiding principles based on which this policy has been evolved. And secondly, in case of any un-clarity or confusion, these principles are to be used as the touchstone.

a) We learn with humility. This means to us, all stakeholders for the business are important and we listen to them while designing and delivering our solution. In the process, we gather, process and create significant amount of data, information and knowledge which are private to our stakeholders. This policy helps us protect the information and prevent misuse.

b) We serve with dignity. This defines our engagement with all the stakeholders. We operate from a body of knowledge, partner with them on equal footing and not let any of them force their intent on us. This policy delineates the processes to handle the information and protect them.

c) We grow with integrity. This defines how we abide the law of the land, respect the right to privacy and prevent misuse of the information.

3) What does this Policy cover?

a) **Private and Confidential Information:** During the course of deputation, you will come to know of a lot of information and gather knowledge pertaining to client's business. All the data (hard copies as well as soft copies) pertaining to the stakeholders of the business which are not available in the public domain for example: information about customers, quotations, commercial details, trade practices, technical knowhow, competing brands, supplier brands, products, raw materials and other inputs etc.) and your salary, system password or any other password used to login/access data at client's premise are private and confidential information. They need to be protected.

b) **Stakeholders** such as client managers, CIEL team and other authorities might have queries pertaining to your job and business practices. This policy defines the process of handling the information.

c) **Who needs to observe this Policy?** This policy applies to all the deputees who are employed with CIEL. The policy defines the methods to organize, edit, store, retrieve, disclose and destroy the information.

d) **Sensitive Personal Information** such as religious beliefs, political opinions, financial status, lifestyle, personal preferences are not required for day to day business and hence, such information are not gathered. Thus, the issue of storing, retrieving, disseminating or protecting does not arise.

e) **Legitimacy:** CIEL ensures that the information gathered in due course of business is for specific purpose of the business. *E.g. daily performance report, market visit report, various kinds of MIS etc.* This information is valuable for client's business and will NOT be used for any other purpose.

4) Processes:

a) **Handling the Data:**

i) All the information must be processed fairly and lawfully.

Fair handling of information means, the users gather and rely on the facts; make all the efforts consciously to remove any personal bias while handling the information.

Lawful handling means, being aware of the local legislations and using them while handling the information at work.

ii) The users of the information have to use them with Accuracy, Timeliness and Sensitiveness.

It is important that the users take all the care to access and apply the information accurately. Also, take timely actions based on the request received from the clients/vendors.

b) **Maintenance of the Data:**

i) **Confidentiality, Integrity and Availability** are essential for any work processes carried out by CIEL's deputees. CIEL asks of its deputees to use data when authorised to do so, maintain the accuracy and suitability of the same; and ensure that the relevant stakeholders are able to use the data when required.

ii) **Relevance:** Deputees of CIEL will do their best to ensure that the personal data are kept up to date to the extent it may be reasonably required and relevant for the purpose.

iii) **Security:** Deputees will have access to information as much as their job requires them to. The IT systems and governance processes in CIEL/client's premise are typically designed accordingly. CIEL insists its deputees to prevent unauthorised access and accidental damage to the data.

iv) **Protection of Data in cases of Third party involvement:** There are specific situations where third party or vendors are involved in the work CIEL's deputees do. In such cases, the deputee has to take steps to ensure that the confidential data is protected; the information is handled lawfully, sensitively and in a secured manner.

c) **Preventive steps against misuse**

i) CIEL's deputee shall not engage in any act subversive of discipline in the course of her/his duty/ies in the property of the client or outside.

ii) CIEL advises its deputees to seek authorisation from the right person before accessing the IT systems and network. Further, the deputee must learn and follow the operating guidelines to use the IT systems.

iii) Deputees must store, retrieve and manage the data in hard copy form neatly in files and cupboards as per standard operating processes followed at CIEL's client location.

d) **Dealing with Queries from the others outside CIEL's Client Organization**

Deputee must check the identity of the outsider and answer the query based on the sphere of concern of the enquirer. Sphere of concern refers to the authority and responsibility of the enquirer with respect to CIEL's client organization.

For example, a customer's queries pertaining to her/his purchase are legitimate queries and within the sphere of concern. However, queries about other customers are outside of it and hence, not answered.

The deputee protects the confidentiality of the information and informs relevant authority at CIEL's client organization about the query.

e) **Non-adherence** to the policy must be discussed with the line manager. They will study the matter, take appropriate action, if any. Deputees are advised to provide the complete information about the suspected non-adherence and stay away from rumours and hearsay.

Non-adherence to this policy could lead to termination from the employment and commencement of legal action to make good the losses that CIEL or its clients may suffer directly or indirectly by such violation.

5) Grievance or Suggestions for improvement in the policy can be brought up by an email to the CEO of CIEL at info@cielhr.com

6) Policy Review

Management review is held each year to review implementation of this policy and draw upon further improvements for the following year. These improvements will include the policy itself and the associated business processes to attain objective of this policy.