Data Protection Policy

1) Why this policy?

Most of us while working for CIEL in the due course of our business, come in contact with data and information pertaining to various stakeholders – our clients, candidates, deputees, vendors, members and investors. These data and information are often private or personal. Our business processes use these and hence, we must know what the right way to handle these is. Hence, this policy!

2) Guiding principles for this policy:

While all attempt is made to define the specifics in the followings 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:** 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: business plans of a client, a confidential search mandate, Candidate's personal information such as those available in the CV, the intentions to change the job, salary levels etc, pricing agreed with vendors such as background verification, insurance policies etc, salary information, promises made to a member in CIEL, activities of an investor in CIEL*) are private and confidential information. They need to be protected.
b) **Stakeholders** such as Police, Statutory authorities, the Judiciary, the Media and other Government authorities might have queries pertaining to CIEL, its business, its employees 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 members of CIEL who handle such information. The policy defines the methods to organise, 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 CIEL's business and hence, such information are not gathered; hence, the issue of storing, retrieving, disseminating or protecting do not arise.
e) **Legitimacy:** CIEL ensures that the information gathered in due course of business is for specific purpose of the business. *E.g. candidate information is used in recruitment, deputee information is used for payrolling, statutory payouts, billing, client reporting and future recruitment*. This information is valuable for CIEL'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. For example, while assessing suitability of a candidate with a job, the user must assess fitment of a candidate or the applicant based on facts mentioned in the records and gathered in the interview.

Lawful handling means, being aware of the local legislations and using them while handling the information at work. For example, a client might have reservations to apply the benefits of maternity to the employee. The right way of handling this information is to combine the knowledge of the legislation with the information of the candidate and take the lawful stance.

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 e.g. matching a job with the candidate's qualifications and other details accurately, fixing the wages of a deputee to reflect the market rates accurately. Similarly, taking actions on a timely basis is important for us e.g. request from another employer to verify employment of an ex-employee needs to be handled with timeliness and sensitivity that the requirement is for the employment of someone who worked with us in the past.

b) **Maintenance of the Data:**

i) **Confidentiality, Integrity and Availability** are built into the work processes at CIEL so that the people authorised get to use the data; accuracy and suitability of the same are ensured; and the relevant stakeholders are able to use the data when required.

ii) **Relevance:** Members at 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. E.g. CVs of candidates, personal information of Deputees, vendor information. Information which is not accurate or suspected to be outdated, reasonable efforts are to be made to update them or archive the same as per statutory requirements. E.g. information regarding deputees who have not reported to work for long

iii) **Security:** Members at CIEL will have access to information as much as their job requires them to. The IT systems and governance processes in CIEL are designed to systemically provide this. This is practised 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, e.g. background verification agencies, assessment partners. In such cases, CIEL signs contracts with qualified partners, binds them contractually to protect the data and emphasises regularly with them to ensure that the information is handled lawfully, sensitively and in a secured manner by them.

c) Preventive steps against misuse

i) CIEL workspace is restricted for visitors and entry into office is monitored.
ii) The IT systems and computer network are duly secured by firewalls, anti-virus, spyware, passwords.
iii) The data in hard copy form are stored neatly in files and cupboards. These are stored on premise for 1 year and henceforth archived at a Data Storage Facility. They are destroyed after they have been utilised.
iv) Information received in re-usable storage media such as USB sticks need to be erased once they have been transferred to CIEL's network.

d) Training

a) We regularly conduct trainings to sensitise members about data handling, processing and storage at all levels

b) Advanced training for key stakeholders in roles that handle client and employee data

e) **Dealing with Queries from the others outside CIEL**

CIEL members will check the identity of the outsider.

i) If it is a client or a deputee, the query is answered based on the sphere of concern of the enquirer. Sphere of concern refers to the authority and responsibility of the enquirer. For example, a deputee's queries pertaining to her/his own payroll, job prospects, industry trends etc are legitimate queries and within the sphere of concern. However, queries about co-workers and business plans of the client company etc are outside of it and hence, not answered and the enquirer is discouraged to ask in future.

ii) If the query is from anyone else, the relevant spokesperson is informed and the query is addressed without compromising on the privacy of the data. For example, a query from a marketing agency to understand about the database of candidates or clients cannot be serviced because the information with CIEL was gathered ONLY for the purpose of providing HR services to our clients and not anything else. However, a query from the Police who is investigating a crime is serviced based on the statutory and legal laid out by the Government, as advised by the Legal team of CIEL.

f) **Non-adherence** to the policy must be discussed with the line manager and reported to Head – HR or Head – Legal or any of the Directors on the Board. They will study the matter, take appropriate action against the concerned members, if any, communicate the same back to the person who reported the issue, review the systems and processes to improve it further and communicate to the entire company about the incident and changes in processes, if any.

5) Grievance or Suggestions for improvement in the policy can be brought up by an email to the CEO.