LUMINA DATAMATICS LIMITED

INFORMATION SECURITY POLICY

We will ensure an effective Information Security Management System that maintains the privacy, confidentiality, integrity, availability and continual improvement of the information to its users, as required.

- **Introduction**

  Lumina Datamatics is practicing ISO 27001:2013 standard (Information Security Management System). As a pre-requisite for this certification, there is a set of rules that every person entering LDL premises needs to follow. These rules have been implemented in the form of policies and procedures and it is mandatory for each person using LDL's facilities to follow the same. Employees (from non- ISMS certified facilities such as Noida) need to follow these policies whenever LDL premises are being used for any reason.

- **Objective**

  The objective of this document is to provide the necessary awareness among employees of Lumina Datamatics, pertaining to information security and adherences to the procedures and guidelines while being at LDL facilities.

- **Coverage**

  The Information Security related processes are applicable to all employees belonging to Lumina Datamatics, while working inside LDL premises. Currently, Lumina Datamatics has following facilities that follow ISO27001 compliant guidelines.

  - Chennai Ascendas
  - Mumbai SDF-IV (Unit No. 117-120)
  - Puducherry LD 1
  - Puducherry LD 2

- **Physical Security**

  i) All employees should wear access card along with the LAN yard while on production floor at all location. The access cards also serve as identity cards and must be displayed at all times while in the premises. The color of the LAN yard used is indicative of the nature of the employment – e.g. full-time, contract, guests etc.

  ii) Visitors are issued special visitor's access cards. It is employees' duty to ensure that visitors, vendors who come to meet him/her follow necessary security guidelines.

iii)   Employees shall not entertain the practice of accompanying their visitors, vendors through an entrance exclusively used for employees.

iv)   While being in the facilities all employees shall keep their mobile in the vibrator mode. Any incoming calls / outgoing calls shall be attended to outside the periphery of production floor.

v)   Bags of all employees shall be checked to verify if there is no data theft through CDs, USB's, DVDs, MP3/MP4 players and any other storage devices being taken out of the premises. Every such data storage device will be verified to prevent potential confidentiality threat.

- **Logical Security**

i)   Proxy based internet access will be provided to employee's desktop and subjected to approval from his/her supervisor.

ii)   An access to any of the folder on LDL's resources will be provided subject to approval from his/her supervisor.

iii)   Employee will follow password & clear screen, clear desk policy as a part of Windows Domain.

iv)   As per laptop usage policy an employee who wants laptop needs to fill up Processing Device requisition form. Issuance of laptop is subjected to its availability and approval from Head – IT Operations.

v)   While on premises or production floor whenever an employee who encounters a breach of security, suspects weaknesses in, or threats to systems, services or software, shall report the same in **Incident Register (iConnect ->CQ->Incident Register).**

vi)   Installation of operating system / third party software requires authorization either from Head – IT Operations or Information Security Manager (ISM). Depending upon software availability user will be authorized for installation of these software.

vii)   External laptops are permitted to connect to power and projector only in the conference rooms.

viii)   LDL official electronic mail should be restricted to official use only

ix)   Endpoint protection (Antivirus) will be installed on all information processing assets, this should never be stopped or uninstalled.

x)   Using of External proxy sites is prohibited as per LDL policy.

Since it is mandatory for employees to follow security policies as their role, anyone (vendors, guest, third party) working or entering LDL premises are expected to respect the rules, standard procedures & policies that pertain to ISO27001 standard.

Approved by
For and on behalf of Board of Directors

Sd/-
Sameer Kanodia
Managing Director & CEO