CONFIDENTIALITY POLICY

Legal Department
CHAINSBERG | 103375 NOLU CD, 2G, 19 NO

Contents

1. Introduction and Purpose:

The Confidentiality Policy has been designed to bring to light how our employees and partners are expected to handle Sensitive Information. Employees and partners receive sensitive data as a part of their duties which should be treated uniquely to guarantee the data is distributed to only respective and authorized entities and individuals. The Information must be protected against misuse for reasons such as being subject to legal regulations and being this Information a backbone of our business.

2. Scope:

This policy affects all ChainsBerg's staff, suppliers, contractors, and volunteers who may access Sensitive Information.

3. Policy Statement:

Sensitive Information refers to data or items meant to be kept safe and unreachable except for authorized individuals. This generally includes documents, images, audio or video materials. If the Information is not public, it is subject to being private and has an owner. Employees and partners who do not respect our Confidentiality Policy are subject to disciplinary and possibly, legal actions. This policy is a binding agreement even after the separation of employment.

3.1Examples of Confidential Information

Confidential Information is valuable and expensive, which must always be regulated in order not to reach hands other than intended by the company.

a) Data of customers, partners, and vendors
b) Data entrusted to our company by external parties.
c) Prices of items received from vendors and customers.
d) Documents and processes marked as Confidential.
e) Unpublished financial data
f) Employees' governmental ID cards, TAX numbers, photos, passports, and other personal documents
g) Suppliers' information such as products, bank information, and any other documents provided by suppliers subject to a pre-qualification or inspection.
h) Patents and modern technologies
i) Employees and partners addresses
j) Supplier and customer lists
k) Financial statements
l) Contracts
m) Unpublished strategies and goals in addition to business operations
n) Passwords
o) Biometric data
p) Patients' data
q) Products specifications and formulas
r) Credit and debit cards information

3.2Procedures for Safeguarding Confidential Information

3.2.1 Employees

a) Secure and lock confidential information.
b) Disposing of the confidential documents by shredding them when they are of no use and according to the ChainsBerg documents retention policy.
c) Only disclose information to employees when necessary and authorized
d) No to share their passwords to ChainsBerg's databases.
e) Use proper passwords when creating login accounts in ChainsBerg's databases (more than 8 numbers including upper and lower case alphabet and symbols)

3.2.2 Suppliers

a) Disclose their information only via the approved and announced means to ChainsBerg (such as on the website)
b) Use safe and secured internet connection.
c) Handle hardcopies only to the authorized ChainsBerg personnel as per the agreements
d) Adhere to this policy and other ChainsBerg policies.

3.2.3 Management

a) Ensure populating this policy to employees and partners.
b) Ensure all employees and suppliers sign off the Confidentiality Policy or agreement
c) Ensure this policy is included as an attachment or a URL link in the RFx and contract for supplies to be aware of our approach to confidential information.
d) Carry out training sessions for employees and suppliers on ChainsBerg's Confidentiality Policy

e) Ensure all internet and file transfer are strongly encrypted.
f) Ensure employees sign of non-disclosure agreement.

3.3Legal Confidential Information Disclosure

Sensitive and Confidential Information may be disclosed to certain external parties as a part of regular inspection or audit. Such examples include:

a) Governmental bodies seeking investigation or auditing the company or specific breach allegations.
b) Audits and inspections carried out by certain customers based on a pre-defined scope of work and non-disclosure agreement within the legal boundaries.

ChainsBerg intends to safeguard its and its stakeholders' interest by keeping Confidential Information secure and undisclosed except with the consent of the information owner. No Confidential Information as defined in section 3.1 may be disclosed to other parties without the consent of the company and the information owner.

3.4 Breach of Confidentiality

Breach of confidentiality is a common law tort, which may be brought as a civil lawsuit against an entity or individual. Penalty may range from employment/contract termination to monetary damages depending on the damage caused by the breach. If the breach occurs, the employee or partner responsible for it will be subject to lawsuit/penalties or other disciplinary actions.