CONCEPCION
INDUSTRIAL CORPORATION

GENERAL

L&G - 001

POLICY ON CONFIDENTIAL INFORMATION

CHANGE / AMENDMENTS / MODIFICATION HISTORY

Version No.	Date	Change		Author	Approved by
		Section	Particular		
1	**10.18.2016**	**NA**	**NA**	**Wehrly Mendez**	**Vicky Betita**

TABLE OF CONTENTS

1. PURPOSE / OBJECTIVE

1.1. This Policy establishes the rules governing the handling of Confidential Information

1.2. This Policy is not intended to be all inclusive. In instances where something is not stated in this Policy, it should be interpreted along with the Company's values, Code of Ethics, and other related Policies

2. SCOPE

2.1. This Policy applies to all employees of CIC and of each of its subsidiaries, and is binding even after separation of employment.

3. POLICY

3.1. CONFIDENTIAL INFORMATION IN GENERAL

3.1.1. Any information that is:

(a) owned by the Company or by another
(b) not in the public domain and
(c) intended to be protected from disclosure in order to prevent the same from being used
   i. against, or to the disadvantage of, the Company, or
   ii. in favor of, or the advantage of, any of its competitors

3.1.2. These include the following:

Trade Secrets
Any form of non-public information that has economic value or gives a company a competitive edge over its competitors on account of its secrecy, such as:

- manufacturing processes and methods
- product development data
- raw materials
- technical know-how and drawings
- test data`
- new product, prior to launch or placement in the market

Business Information

- price of raw materials
- product liability claims
- delivery schedules
- computer programs and data compilation
- network architecture
- marketing / promo materials
- budgets and forecasts
- strategies / plans
- financial data
- bid or contract data and terms
- client/customer lists and data
- supplier lists and data
- employee lists
- incentive, commission, dealer support or other compensation structure
- playbook and other instructions or parameters for negotiation
- work product developed by an employee during employment, including emails, reports, memorandums, research, etc.
- employment of key executives
- opinions or advice of legal counsel
- financial investments and resources
- sensitive HR programs
- audit reports
- executive travel schedules

Employee Relations Information

- employee relations issues
- disciplinary actions
- impending layoff / terminations
- investigations of employee misconduct
- employee survey results
- Dialog reports

Personal Information

(of current, past or prospective employees, customers, business partners, providers)

These information may only be shared by the owner

- government issued ID number
- home address or telephone number, or other personal contact information
- internet identification name or password
- email address

- mother's maiden name
- birthdate and birthplace
- medical / health condition and history
- account numbers
- salary (should not be shared, even by owner)
- any other information
  - about an identified or identifiable person
  - that, when associated with an individual, can be used to identify him or her

3.2. **CONFIDENTIAL INFORMATION BELONGING TO THE COMPANY**

3.2.1. Must not be disseminated to anyone outside of the Company.

3.2.2. May be shared inside the Company but only on a need to know basis.

3.2.3. Must be accessed or used only for legitimate business purposes of the Company.

3.2.4. Must not be used for the personal benefit or profit of anyone other than the Company.

3.2.5. Precautionary measures must be taken when viewing or sharing to prevent unauthorized, inappropriate, unnecessary or inadvertent dissemination.

3.3. **CONFIDENTIAL INFORMATION BELONGING TO OTHERS**

3.3.1. Must be handled with the same degree of care as the Company's own Confidential Information.

3.3.2. Must be used only within the limits of the authorization given by the owner.

3.3.3. Must not be sought or accepted through illegal, unethical or disreputable means.

3.3.4. Current, past or prospective employees or business partners must not be allowed, pressured, induced, or encouraged to provide Confidential Information from a previous employer or client, or to otherwise breach duties of confidentiality they may owe to others

3.4. PRECAUTIONARY MEASURES

3.4.1 Storage Security

- Keep and store materials within Company premises and company owned devices only
- Only use company approved portals for storing information
- Place materials in locked file cabinets when not in use, or in rooms accessible only to those who have a business need to know
- Clear desks and ensure drawers are locked before leaving the office
- Refrain from leaving confidential information visible on computer monitors when leaving work stations
- Physically and electronically secure laptops, mobile devices, and removable media at all times, and do not leave them unattended. Avoid leaving them in the car; if this cannot be avoided, do not leave in plain sight.
- Use only strong passwords for devices (combination of numbers, letters and characters, at least 8 characters long); do not write them down and leave in plain view
- Protect electronic information via firewalls, encryption and passwords

3.4.2 Email Security

- Avoid using e-mail to transmit sensitive or controversial information
- Do not forward internal emails to customers, business partners, providers, or anybody outside of the company, or include them in internal communications
- Use "auto-complete" and "reply to all" sparingly and mindfully, or avoid using them at all
- Double check email addresses before sending, to ensure the message is sent to your intended recipients only

3.4.3 File / Information Sharing

- Label all "Confidential Information" as such
- Limit the acquisition of information to those necessary to the business transaction
- Restrict access to information on a "need-to-know' basis
- Refrain from discussing confidential information in public places
- Do not install file sharing applications on any of your devices
- Do not save company data into a file sharing software

3.4.4 Proper Disposal – when no longer needed:

- Shred or destroy materials
- Destroy CDs, DVDs and computer drives
- Delete information from a departing employee's electronic devices
- Sanitize hard drives by using software programs to wipe out data

3.5. **RESPONSIBILITY**

3.5.1 Confidential Information may have to be disclosed in exceptional cases for legitimate reasons, e.g. upon request of a regulatory body or for business purposes. In such cases, the explicit consent of the responsible SBU head must be obtained beforehand, and the disclosure must be limited only to the information relevant to the request or inquiry.

3.5.2 Each employee is responsible for:

- classifying all Confidential Information that its team generates or receives in terms of sensitivity or severity of the potential damage (or the lack of it) that its disclosure could cause the company
- assigning the relevant parties to whom it can be shared
- determining and communicating the terms of disclosure, including the obligations of the persons possessing the information
- instituting control measures to prevent or manage unnecessary disclosure

3.5.3 All employees are required to immediately report to the manager and SBU concerned, HR or BPO (or ProActive, if so desired) any violation of this policy, and any data breach, leakage or loss, whether actual, suspected, potential, deliberate or unintentional.

4. NON-CONFORMANCE

4.1. Any non-conformance with this Policy shall be dealt with as a violation of the Code of Ethics, punishable by up to termination, and without prejudice to civil and/or criminal action as may be warranted by the circumstances.