NAPEC

CODE, POLICIES AND DIRECTIVES
(Declarations, acknowledgment of receipt and employee commitments)

1. CODE AND POLICIES:

- ❍ Code of Professional Ethics and Business Conduct (the « Code »);
- ❍ Insider Trading Policy;
- ❍ Whistleblowing Policy;
- ❍ Information Disclosure Policy and Procedure;
- ❍ Information Technology Policy;
- ❍ Corporate Directive: Information Technology Employee Guidelines;
- ❍ Human Resources Policy; and
- ❍ Compensation Policy.

2. EMPLOYEE'S REPRESENTATIONS: The employee represents that:

(a) He has had sufficient time to read and has actually read the Code, each of the above-mentioned policies and directive (collectively, the "**Policies**") in their entirety;

(b) An authorized representative of NAPEC Inc. offered to provide him, if he should so desire, with information and explanations needed to understand the Policies;

(c) Each and every one of the provisions of the Policies are readable;

(d) The employee understands the nature and significance of the Policies;

(e) The Policies are reasonable, justified and in the interest of the NAPEC Inc., its subsidiaries, its employees, its suppliers and its customers; and

(f) An authorized representative of NAPEC Inc. provided him with a copy of the above mentioned Policies or indicated how to consult them on NAPEC Inc. website (www.napec.ca).

3. EMPLOYEE ACKNOWLEDGMENT AND COMMITMENTS

The employee acknowledges having received the Policies mentioned above, and agrees and undertakes that he will respect each and every one of the provisions therein.

SIGNED AT _____(city), _____ (state or province), _____ (country), this _____ day of the month of _____ 20 ___.

THE EMPLOYEE

_____ _____

Employee name (printed) Employee signature

Subsidiary: _____

Updated as at March 24, 2016

CODE OF PROFESSIONAL ETHICS AND BUSINESS CONDUCT

APPROVED BY THE CORPORATE GOVERNANCE COMMITTEE ON NOVEMBER 2, 2015
APPROVED BY THE BOARD OF DIRECTORS ON NOVEMBER 6, 2015

CODE OF PROFESSIONAL ETHICS AND BUSINESS CONDUCT

1. Purpose and Scope

The purpose of the existing Code of Professional Ethics and Business Conduct (the "Code") is to establish guidelines such that all employees (the "employees") of NAPEC Inc., its subsidiaries (collectively referring to as the "Corporation") and all its consultants, suppliers and other people who work with the Corporation or on its behalf respect the Corporation's commitment to show respect, integrity, honesty and transparency during the course of business and in all its relationships. The employees shall ensure that the consultants, suppliers and other people who work with the Corporation or on its behalf know and comply with the content of the Code.

The existing policy also applies to the members of the Board of Directors of the Corporation and the term "employees", when used herein, shall, as the case may be, also apply to such members of the Board of Directors.

2. Details

General

2.1 The Corporation has always been aware that its success is based on its values that are, integrity, honesty, responsibility, transparency and team work. The Corporation pledges to abide by applicable laws in conducting its business and expects its employees, consultants, suppliers and other people who work with the Corporation or on its behalf to do the same. Moreover, the business relationships the employees enjoy in the course of their work and with shareholders, customers, suppliers, community organizations, governments and regulatory bodies, shall be based on the highest ethical standards. The purpose of the Code is to ensure that all employees have a good understanding of the conduct they are expected to have.

2.2 **The Code is not meant to be a comprehensive Code of Professional Ethics and Business Conduct that covers all eventualities.** As such, if an employee finds himself in a situation that requires further advice, the issue should be discussed with his/her department manager, or the Human Resources Department, or the Legal Department or the Corporation's Senior Management. An employee can, at any time, discuss ethical issues with his/her colleagues or his/her superiors and ask for help. The Corporation acknowledges its obligation to support its employees when ethical issues arise.

2.3 Abiding by the Code is essential to bring into focus and protect the Corporation's reputation as a firm that is aware of its responsibilities as a corporate citizen. Violating the Code is a very serious offence.

Employee Conduct and Behaviour

2.4 It is the responsibility of each employee to observe the rules of conduct generally accepted as standard in a business concern.

2.5 The managers have major responsibilities under the Code. They must understand the Code, ask for advice as needed and report any alleged violation. They most promote the Code and ensure its dissemination among the employees. It is the manager's responsibility to inform the employees as quickly as possible when their conduct or behaviour is not aligned with the Code. If a manager knows that an employee committed or intends to commit something that is contrary to the Code and omits to stop him/her, he/she bears the same liability as the employee.

2.6 The Corporation agrees to maintain a work environment that is free of illegal drugs, alcohol, firearms or anything inappropriate. Possessing, exchanging, selling or using any of these on Corporation premises is strictly forbidden. Violation of the existing policy shall give rise to disciplinary action that could lead to a dismissal without prior notice or compensation in lieu of notice.

Professional Ethics Guidelines for the Employees

2.7 The employees' conduct and behaviour must comply with the professional ethics guidelines details below:

2.7.1 Respect: The employees consider the needs and wishes of others. They acknowledge the skills and knowledge of others. They appreciate cultural diversity and differences.

2.7.2 Civility: The employees make reasonable efforts in order to maintain a harmonious and pleasing work environment. They treat others with courtesy and politeness. They refrain from any form of harassment, direct or indirect.

2.7.3 Integrity: In their decisions and actions, the employees give precedence to ethical principles and obligations. They respect all the ethical obligations that stem from applicable laws and regulations. They do not tolerate unethical conduct.

2.7.4 Loyalty: The employees must act with loyalty, to protect and promote the Corporation's good reputation and interests. They must commit to fulfilling their duties, to maintaining their knowledge current, to working in achieving Corporation's objectives and to demonstrating quality and rigor in discharging their duties.

The employees may take part, in his/her personal capacity, in non-professional activities of their choice to the extent that such participation does not go against this Code, compliance with the terms of employment or contract and is not detrimental to reputation or the interests of the Corporation. No employees may express political opinions on behalf of the Corporation.

2.7.5 Honesty: The employees are sincere in their decisions and their actions. They use resources judiciously and in the best interest of the Corporation's mission, principles and guidelines.

2.7.6 Fairness: The employees are just and fair in their decisions and their actions.

2.7.7 Responsibility: The employees fulfill their tasks using competence, diligence and devotion. They give clear and concise directives.

Conflicts of Interest

2.8 A conflict of interest occurs when an individual's private or personal interest interferes, or may appear to interfere, with the interests of the Corporation. It also occurs when an employee takes actions or has interests that may make it difficult to perform his/her Corporation work objectively and effectively.

2.9 The Corporation expects and requires that the employees have no interest or relationship that might be counter-productive or damaging to the interests of the Corporation.

2.10 This section of the Code is intended to advise employees so that they can avoid situations which could be perceived or likely to be in conflict with their responsibilities. As a general rule, the following situations amount to a conflict of interest:

i) When an employee has an interest that significantly infringes on the time and attention he/she should be devoting to the Corporation's business, or puts effort into something that will prevent him/her from concentrating fully on his/her work;

ii) When an employee or, to the best of his knowledge, one of his/her relatives holds a direct or indirect interest or have a connection with a customer, representative, competitor, or another person who is related to the Corporation's business and might reasonably:

a) result in personal gain for the employee involved or for one of his relatives;

b) make the employee biased, to detriment of the interests of the Corporation; or

c) place the employee or the Corporation in an ethically embarrassing or doubtful position in the eyes of the public or any supervisory agency.

iii) When an employee or, to the best of his/her knowledge, one of his/her relatives uses information that is exclusive, internal, privileged or confidential, or information obtained in conduction Corporation business, to his own advantage or to the advantage of a third party.

2.11 When an employee finds himself/herself in a situation which could be perceived to be in conflict with his/her responsibilities or has a question about the interpretation or the

application of the concept of conflict of interests, he/she has an obligation to discuss it with his/her immediate supervisor or with the Legal Department of the Corporation.

Gifts, Rewards and Entertainment

2.12 All the employees must lead their business to avoid affecting their judgement unfavourably or the Corporation's reputation. In the course of their work and unless upon prior approval by the President and Chief Executive Officer or the appointed Vice-President, the employees, either directly or indirectly, must not accepts gifts, rebates, valuables or favours from companies, organizations, representatives, employees or other people who do business or might do business with the Corporation.

Under no circumstances, the Corporation will agree to receive or that one of its employees receives cash, a commission or a loan from companies, organizations, representatives, employees or other people who do business or might do business with the Corporation.

Issues related to Competition

2.13 The Corporation shall act independently and in its own interest in all business situations that have an impact on the business's competitive conditions and avoid practices that restrict competition.

2.14 It is the responsibility of each manager to respect the spirit and letter of all laws regarding competition that apply to the Corporation. In case of doubt, issues affecting competition should be brought to the attention of the Corporation's Legal Department.

2.15 It is proper to gather information about the Corporation's business, including information about its competitors and their products and services. But it must always be done appropriately. Illegal or unethical means such as theft, spying, bribery, or in breach of a nondisclosure agreement must never be used to obtain such information.

Bribery

2.16 The Corporation attaches great importance to its reputation and it is vital to maintain it. The Corporation has a "zero tolerance" approach towards bribery. This commitment implies that no employees can offer or give an arbitrary form of bribe or dividend to any third party to ensure a preferential treatment in connection with the Corporation's businesses.

Confidential Information and Intellectual Property

2.17 Confidential information includes, among others, technical information on products and processes; lists of suppliers and purchase prices; strategies related to costs, pricing, marketing or services; results of development projects, technical knowledge and computer software, non-public financial information reports. Also, how the Corporation gathers public information can be considered to be a secret.

2.18 Intellectual property includes, among others, patents, royalties, trademarks, trade secrets and engineering drawings.

2.19 Confidential information, especially information related to intellectual property, is considered to be an asset. Employees shall take care not to disclose such information to unauthorized persons. In this regard, the employees must refer to the guidelines provided in the Information Communication Policy and Procedure and in the Confidentiality and Non-Solicitation Agreement.

Relationships with Third Parties

2.20 An employee must refuse to receive any unsolicited third-party information that is exclusive, internal, privileged or confidential in nature. If an employee inadvertently receives such information, he/she must refrain from disseminating it and immediately notify his/her immediate superior and the Legal Department of the Corporation.

2.21 An employee must not use, for any purpose whatsoever, information provided by a third party that is exclusive, internal, privileged or confidential in nature in conducting Corporation business or to the advantage of the Corporation business.

2.22 Any information determined to be exclusive, internal, privileged or confidential in nature must be returned to such third party.

2.23 Should there be any doubt as to the exclusive, internal, privileged or confidential in nature of the information received or the manner in which it was collected, the employee, consultant or other person who works with the Corporation must consult his/her immediate superior as well as the Legal Department of the Corporation.

Laws and Regulations

2.24 The Corporation must observe the laws and regulations that govern the activities it exercises in the territories in which it carries out its business. The employees shall not only respect these laws and regulations, but also report any worrisome situation to the Legal Department of the Corporation.

2.25 The provisions of the Code are not intended to provide legal advice on the laws and regulations that affect the Corporation's activities. Specialized resources are available for this purpose within the Corporation. However, there are several laws that should be specifically noted. These are presented below:

2.25.1 Laws regarding Health and Safety: The Corporation pledges to create and maintain a healthy and safe work environment for its employees. As such, the employees shall not only respect the laws and regulations regarding safety, but shall report any worrisome situation to their superior.

2.25.2 Laws regarding human/civil rights: Everyone has the right to be treated fairly on the job and to a work environment that is free of harassment, where there is no discrimination on the basis of race, ancestry, place of origin, citizenship, religion, sex, sexual orientation, age, record of offences, marital status, family circumstances or handicap. The Corporation does not tolerate discrimination, harassment or violence of any kind in the work place. Employees must report such behaviour or problems, especially those that affect their personal safety or that of their colleagues.

2.25.3 Laws regarding securities and insider trading: The employees shall refrain from buying or selling Corporation securities and property when they are aware of important non-public information about the Corporation, and they shall refrain from disclosing such information to other people, especially their families and their friends. "Important non-public information" refers to information that is sufficiently important that, if it were disclosed to the public, would, in all likelihood, impact the price of the Corporation's securities (for example, shares or bonds). The Corporation's guidelines regarding insider trading are provided in the Policy on Insider Trading. Examples of potentially price sensitive information include, among others:

- Board of Directors appointments or departures;
- share dealings by directors, senior officers and major shareholders;
- major acquisitions and disposals;
- regulatory or legal rulings;
- the winning or loss of a large contract; and
- a major internal restructuring.

Books and Registers

2.26 When working on business registers, it is of the utmost importance to be precise and dependable/reliable in making decisions and in properly carrying out financial and legal obligations and in reporting financial information. The business registers, expense accounts, invoices, payroll journals and personnel files, as well as all other reports, shall be prepared carefully and honestly.

2.27 All financial operations shall be correctly entered in the book of accounts and accounting methods supported by the necessary internal controls. All books and registers of the Corporation shall be accessible for audit purposes.

2.28 As regards to the books and registers of the Corporation, the employees:

i) Shall not intentionally do anything that would render the Corporation's documents inexact in any way;

ii) Shall not produce or participate in producing registers that conceal anything that is inexact;

iii) Shall correctly enter all disbursements without delay;

iv) Shall cooperate with the external auditors and to those authorized under applicable law;

v) Shall report any false or inexact information or register or any transaction that does not seem to be in line with a legitimate business objective; and

vi) Shall not make any unusual financial arrangements with a customer or a supplier for example, overcharging or undercharging.

2.29 Alleged violations of the financial policy shall be reported to the Chairman of the Audit Committee, the Chairman of the Board of Directors or to the Chairman of the Corporate Governance Committee in accordance with the Corporation' Whistle Blowing Policy.

Relations with Shareholders, Investors and the Media

2.30 Requests from investors or shareholders for information regarding the Corporation and its business must be referred to the President and Chief Executive Officer or the Chief Financial Officer.

2.31 All spokespersons, or anyone who deals with the shareholders, investors and media, shall demonstrate a high degree of integrity and transparency, while refraining from having any exclusive or non-public communication. The Corporation's guidelines regarding relations with the shareholders, investors and the media can also be found in the Corporation's Information Communication Policy and Procedure.

2.32 The employees should ensure that these spokespersons are aware of any relevant issue of local or national interest that deals with the business of the Corporation and of which they might not be aware.

Abiding by the Code

2.33 The employees shall immediately report any real or alleged violation of the Code to one of the following persons:

- an immediate superior;
- a person in charge of a department or function;
- the Legal Department;
- the Human Resource Department;
- the Corporation's President and Chief Executive Officer; or
- any other person designated by the Corporation.

2.34 All information shall be treated as confidential. No reprisal shall be exercised against anyone who reports a violation in good faith. However, anyone who takes part in a forbidden activity may have disciplinary measures taken against him/her, even if he/she reports the activity. If disciplinary measures are contemplated, an employee's decision to report a violation shall be considered in all cases.

2.35 Any employee who does not comply with the Code, or who holds back information during an investigation regarding a possible violation of the Code, may have disciplinary measures taken against him/her, or even dismissed without prior notice nor compensation in lieu of notice. Depending on the nature of the violation, the Corporation may be legally forced to report the violation to the appropriate authorities.

2.36 Any consultant or supplier who does not comply with the Code, or who holds back information during an investigation regarding a possible violation of the Code, may have his contract terminated or not renewed. Depending on the nature of the violation, the Corporation may be legally forced to report the violation to the appropriate authorities.

2.37 Every time there is a violation of the Code, the Corporation shall make an attempt to impose disciplinary measures that take into account the nature of the violation and the specific facts surrounding it. Such disciplinary measures can include, without restrictions, warnings, reprimands, probation periods or suspension without pay, demotion, salary reduction or dismissal. Moreover, any superior who directs or approves any type of violation of this Code, or who is informed of such a conduct and does not report it, can also be subjected to the disciplinary measures up to and including dismissal.

2.38 The Corporation reserves the right to change or void the Code at any time and for any reason whatsoever.

INSIDER TRADING POLICY

APPROVED BY THE GOVERNANCE AND NOMINATING COMMITTEE ON APRIL 25TH, 2013
APPROVED BY THE BOARD OF DIRECTORS ON MAY 2ND, 2013

INSIDER TRADING POLICY

1. PURPOSE OF THE POLICY

Insider trading is a priority of market monitoring agencies. The fundamental rule is based on the fact that insiders may neither buy nor sell securities or related financial instruments when they have information on material facts that are unknown to the public at large and, if they were known, could affect the decision of reasonable investors to buy or sell securities. The main safeguard against insider trading is the insider reporting requirement, which has two goals. First, it provides the market with information on the trading activities of those who manage or control reporting issuers. Second, it serves to prevent insider trading based on confidential information, given that insiders must report all their transactions to the public.

The rules and procedures below were approved by the Governance and Nominating Committee and the Board of Directors of NAPEC Inc. (the "**Corporation**") to prevent illegal insider trading and ensure that the Corporation's directors, officers, and employees and any affiliated individuals or corporations or those that they control act, and are perceived to act, in accordance with applicable laws, the highest ethical standards, and professional behavior beyond reproach.

2. INSIDERS

Insiders of the Corporation include its directors and officers, the directors and officers of its subsidiaries, any individual or corporation that exercises control or direction over more than 10% of the voting rights attached to the Corporation's outstanding voting securities, and any other employees of the Corporation who have knowledge of privileged information (as defined below).

3. RESTRICTIONS ON THE USE AND DISCLOSURE OF PRIVILEGED INFORMATION

Insiders may not, for their own purposes or the purposes of others, use or disclose any material information, i.e., any information not disclosed to the public relating to the business and activities of the Corporation or its subsidiaries that is likely to affect the decisions of reasonable investors or that results, or would be reasonably be expected to result, in a significant change in the market price or value of the Corporation's securities. Material information consists of material facts and changes. Examples of material information are provided in Appendix A of this policy. Material information, changes, and facts are herein collectively referred to as "**privileged information.**"

4. SECURITIES TRADING RESTRICTIONS

Insiders and anyone entitled to act on their behalf are prohibited from buying or selling the Corporation's securities or related financial instruments[1] if privileged information is brought to their knowledge. This restriction also applies to anyone who obtains privileged information from an insider of the Corporation and anyone with whom the Corporation or any of the abovementioned individuals is associated under applicable securities laws.

---

1. *Related financial instrument:*
   - Any instrument, agreement, or security whose value, market price, or payment obligations are based on the value, market price, or payment obligations of a security
   - Any other instrument, agreement, or arrangement that indirectly affects an individual's financial interest in a security

   Examples: Share- or option-based instruments, derivatives, forward contracts, share purchase contracts, and linked notes.

5. INSIDER TRADING REPORTS AND OTHER REPORTS

a. Initial reports

All reporting insiders[2] (under *Regulation 55-104 respecting Insider Reporting Requirements and Exemptions*) must register as insiders and file an initial report no later than ten calendar days after becoming reporting insiders of the Corporation. The report must contain the following information:

a) The reporting insider's beneficial ownership of, or control or direction over, directly or indirectly, securities of the Corporation

b) The reporting insider's interest in, or rights or obligations associated with, any related financial instrument

The Canadian Securities Administrators have implemented the System for Electronic Disclosure by Insiders ("**SEDI**"), which all reporting insiders must use to file insider reports (www.sedi.ca).

b. Transactions covered

Reporting insiders have five calendar days following the date of a trade to report any trade associated with:

a) the purchase of the Corporation's shares, on the market or otherwise (including by means of an account managed on a discretionary basis);

b) the sale of the Corporation's shares;

c) the sale of shares following the exercise of stock options ("**options**");

d) the granting of options;

e) the exercise, divestiture, or transmission of options following a discretionary decision made by the reporting insider;

f) or any change in the reporting insider's interest in, or rights or obligations associated with, any related financial instrument.

c. Early warning reports

A reporting obligation is triggered under the *Securities Act* (Quebec) and under the securities laws of other Canadian provinces when an investor acquires beneficial ownership of 10% or more of the Corporation's common shares, taking into account securities convertible into securities on the date of the report, or when said investor has control of or direction over such securities.

---

2. *The insiders who are required to file insider reports on SEDI under* Regulation 55-104 respecting Insider Reporting Requirements and Exemptions *are the directors of the Corporation or one of its major subsidiaries, the President and Chief Executive Officer and the Chief Financial Officer of the Corporation or one of its major subsidiaries, anyone responsible for one of the main operating units, divisions, or offices of the Corporation, and any other officer of the Corporation or subsidiary of the Corporation who meets the following conditions: i) he or she receives, during the normal course of his or her duties, information or access to information on material facts or changes concerning the reporting issuer before it is made public and ii) directly or indirectly exercises, or has the ability to exercise, significant power or influence over the business, operations, capital, or development of the reporting issuer.*

Directors, officers, or employees who intend to buy shares that will exceed the abovementioned limit must therefore consult the Chief Financial Officer or the Corporate Secretary of the Corporation to determine the nature of their reporting obligations under applicable Canadian securities laws.

6. BLACKOUT PERIODS

a. Routine blackout periods

The Corporation's insiders must refrain from buying or selling securities or related financial instruments for a specified period, starting 30 days before and ending 24 hours after the Corporation's interim or annual financial statements are published (unless such individuals have access to privileged information).

b. Temporary blackouts

The Chair of the Board of Directors or the President and Chief Executive Officer may, from time to time, announce the dates of any blackout periods that coincide with the emergence of new, unexpected facts affecting the Corporation, the availability of new privileged information or other undisclosed material information, or details of a possible trade.

Anyone who is aware of special circumstances or new facts affecting the Corporation is subject to a blackout. This may include external advisors such as the Corporation's legal and financial advisors. The length of the blackout and waiting period between the publication of material information and the resumption of insider trading rights will be determined by the Chair of the Board of Directors and the President and Chief Executive Officer and communicated to officers, directors, employees, and other affected individuals when deemed appropriate under the circumstances.

Officers, directors, employees, and anyone else affected by a trade blackout will be notified by the Chair of the Board of Directors, the President and Chief Executive Officer, or the Corporate Secretary. If a trade is initiated prior to the notice but is not concluded at the time the blackout comes into effect, such a trade may be executed. However, no new trade may be undertaken. Anyone affected by a blackout who is in the process of a trade must notify the Chair of the Board of Directors or the President and Chief Executive Officer.

The purpose of the abovementioned rules is to help the Corporation's insiders ensure that they and third parties execute trades on the Corporation's securities or related financial instruments only when it is reasonable for them to believe that any privileged information regarding the Corporation has been communicated to the public.

7. TRADING RESTRICTIONS

a. New business facts and material information

Insiders may not trade the Corporation's securities or related financial instruments (exercise options) between the date on which it is reasonably expected that a new, material business fact (not known to the public) is likely to occur and the day after information on such fact is published. New business facts include the acquisition or divestiture of shares or assets, the formation of joint ventures, the Corporation's investment in another corporation, the procurement contracts of

a major client, the loss of a major client, or the expected loss of business due to an unexpected event.

b. Financial instruments

Directors, officers, and employees may not buy financial instruments, particularly variable prepaid forward contracts, equity swaps, collars, or shares of listed funds designed to protect against decreases in the market value of equity securities that are granted as compensation or held, directly or indirectly, by a director, officer, or employee.

c. Miscellaneous

It is inappropriate for any director, officer, or employee of the Corporation or any other individual or corporation to which the policy applies, acting alone or with another individual or corporation, to directly or indirectly undertake any activity that (i) is or appears to be against the interests of the Corporation or its success, (ii) creates or may create a false or misleading appearance of trading activity on the Corporation's shares, (iii) has a direct or indirect effect of establishing an artificial price for such shares, or (iv) otherwise interferes with the free determination by the market of the market price of such shares. Although it is impossible to list all the activities prohibited by this policy, the activities described below are typically activities that are prohibited and should therefore not be pursued:

- Selling short shares of the Corporation (e.g., sell shares not held by the seller in anticipation of a drop in the market price of the Corporation's shares)
- Buying or selling shares or other securities of the Corporation primarily to influence the market price or the trading volume of such shares or other securities
- Being both a buyer and seller (directly or indirectly) of shares or other securities of the Corporation at or about the same time
- Retaining or having retained, in a personal capacity and not on behalf of the Corporation, the services of an individual or corporation to promote the Corporation's shares or other securities

8. RESPONSIBILITIES OF INSIDERS

Reporting insiders are required to submit reports regarding their situation.

Insiders are individually responsible for the information in their reports and for transmitting their reports to the regulatory authorities within the prescribed time limit following a trade in the Corporation's securities or related financial instruments.

All insiders and reporting insiders must comply with this policy. Any failure to comply may constitute a violation of applicable laws, result in sanctions, and have serious consequences for the Corporation.

9. QUARTERLY REPORT

All reporting insiders of the Corporation must each submit to the Corporation's management a quarterly report (Appendix B) confirming that all their trading in the Corporation's securities or related financial instruments was reported in accordance with applicable securities laws.

10. COMMUNICATION

New directors, officers, and employees must be informed of their obligations under this policy, and this policy must be brought to the attention of all employees of the Corporation.

11. QUESTIONS

Any questions regarding this policy should be submitted to the Corporate Secretary or Chief Financial Officer of the Corporation.

APPENDIX A

MATERIAL INFORMATION

National Policy 51-201: Disclosure Standards is used to determine material information.

Examples of potentially material information

The following examples are types of events or information that may be material. This list is not exhaustive, and any questions regarding materiality should be submitted to the Corporate Secretary or Chief Financial Officer of the Corporation.

Changes in the structure of the business or capital

- Changes in shareholding that may affect control of the Corporation
- Major restructurings, amalgamations, or mergers
- Takeover bids, issuer bids, or a takeover bid made by an insider
- Public or private sale of additional securities
- Scheduled redemptions of securities
- Scheduled divisions of common shares or investments in warrants or rights to buy shares
- Any share, share exchange, or share dividend consolidations
- Changes in the Corporation's dividend payments or policies
- Possible initiation of a proxy fight
- Major amendments to shareholder rights

Changes affecting financial performance

- Increase or decrease in expected profits
- Unexpected changes in financial performance for any period
- Changes in financial situation, such as cash flow reductions, write-offs, or depreciations of major assets
- Changes in the value or composition of the Corporation's assets
- Any major changes in the Corporation's accounting policies

Changes affecting business and operations

- A major change in the Corporation's capital spending plans or objectives
- Major labor disputes or disputes with major contractors or suppliers
- Major new contracts or major contract or business losses
- Major discoveries
- Changes to senior management or the Board of Directors, including the departure of the Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, or President (or individuals occupying similar positions)
- Institution of major legal or regulatory procedures or the emergence of new related facts
- Any notice that previous use of an audit is no longer permitted
- Delisting of the Corporation's securities or their transfer from a rating system to another system, or from one stock exchange to another

Acquisitions and divestitures

- Major acquisitions or divestitures of assets, property, or interests in joint ventures

- Acquisitions of other corporations, including a takeover bid from another corporation or a merger with another corporation

Changes in credit agreements

- Borrowing or lending of major sums of money
- Subjecting of the Corporation's assets to a mortgage or charge
- Breach of the terms of debt securities, debt restructuring agreements, or enforcement procedures provided for by a bank or other creditor
- Major new credit agreements

APPENDIX B

QUARTERLY REPORT OF REPORTING INSIDERS

I hereby confirm that I have reported, via the System for Electronic Disclosure by Insiders ("SEDI"), all trades in the securities or related financial instruments of NAPEC Inc. in accordance with applicable securities laws for the quarter ended ●.

Name	Signature	Date

WHISTLEBLOWER POLICY

APPROVED BY THE GOVERNANCE AND NOMINATING COMMITTEE ON DECEMBER 11, 2013
APPROVED BY THE AUDIT COMMITTEE ON MARCH 25, 2014
APPROVED BY THE BOARD OF DIRECTORS ON MARCH 26, 2014

WHISTLEBLOWER POLICY

1. GENERAL

NAPEC Inc., including its subsidiaries (the "**corporation**"), seeks to maintain the highest professional ethical standards and comply with all applicable laws and government rules and regulations, accounting controls, and audit practices.

The corporation has created a work environment based on trust and respect so that all employees can work without fear and free from intimidation, harassment, and discrimination. One component of this commitment consists of fostering an atmosphere of openness and honesty, where any problem, concern, or complaint about wrongdoing can be raised in good faith without fear of any retaliation whatsoever.

2. POLICY STATEMENT

This policy provides for the possibility for corporation employees and officers, including temporary staff and consultants, to communicate the existence of a problem or serious concern in good faith regarding wrongdoing that may occur in the corporation. It does not intend to call into question financial or business decisions made by the corporation.

At the same time, this policy provides for confidential and anonymous reporting.

3. RESPONSIBILITY FOR THE POLICY

In accordance with its mission and applicable securities regulations, the Audit Committee of the corporation's board of directors (the "**board**") is responsible for ensuring that a confidential and anonymous reporting process is in place so that individuals can report any wrongdoing associated with the corporation.

Under the direction of the Audit Committee, the Audit Committee chair is entrusted with the responsibility of applying this policy and ensuring that the corporation complies with it.

4. RELATED DOCUMENTS

This policy must be read in conjunction with the corporation's Professional Code of Ethics and Business Conduct.

5. WRONGDOING

For the purposes of this policy, the concept of wrongdoing is broad and extensive. It includes any act that, in the whistleblower's opinion, is illegal, unethical, contrary to the corporation's policies, or reprehensible or inappropriate in any other manner, particularly:

a) Violation of applicable laws, rules, or regulations that relate to the corporation's reporting

b) Fraud or deliberate errors in the preparation, assessment, examination, or audit of the corporation's financial statements

c) Fraud or deliberate errors in the entries in or the maintenance of the corporation's financial records

d) Deficiencies in the corporation's policies and internal controls or failure to comply with such policies and controls

e) False declarations made by or to a director, officer, or employee of the company or one of its subsidiaries regarding items in the financial records and reports or audit reports

f) Failure to present a complete and accurate report of the corporation's consolidated financial position

g) Misappropriation of the corporation's funds

h) Acts committed to conceal any of the abovementioned acts

(collectively "**wrongdoing**")

6. COMMUNICATION OF THE POLICY

Through the corporation's management, the board ensures that all of the corporation's employees, including temporary staff and consultants, are familiar with the policy.

They are provided with a copy of the policy and informed that it is available for consultation on the corporation's website. They are also informed of any major changes made to the policy.

New directors, officers, and employees, including temporary staff and consultants, receive a copy of the policy and are made aware of its importance.

7. REPORTING AN ALLEGED BREACH OR MAKING A COMPLAINT

Anyone wishing to report a concern regarding alleged wrongdoing may submit it to the chair of the corporation's Audit Committee, either:

a) in a sealed envelope addressed to the attention of the Audit Committee chair and marked "Confidential: To be opened by the Audit Committee chair only" to the following address:

1975 rue Jean-Berchmans-Michaud, Drummondville, Quebec J2C 0H2;

or

b) by email to auditcommittee@napec.ca.

Concerns should be expressed in writing. Disclosures of wrongdoing must include relevant, accurate, and sufficient information on dates, individuals, locations, witnesses, figures, etc. so that a reasonable investigation can be conducted.

8. ANONYMITY AND CONFIDENTIALITY

The corporation undertakes to maintain adequate procedures for the anonymous and confidential reporting of complaints. The identity of whistleblowers is not disclosed unless they expressly authorize the disclosure of their names, or such disclosure is required by law.

Anonymous and confidential reports are sent only to individuals who must be informed of them so that alleged wrongdoing can be investigated.

9. NO NEGATIVE REPERCUSSIONS

No member of the corporation's staff who raises a concern in good faith or reports alleged wrongdoing will be subject to harassment, retaliation, or adverse employment action.

Any staff member or representative of the corporation who retaliates against someone who has reported a concern in good faith regarding alleged wrongdoing commits a serious breach of this policy and is subject to disciplinary action up to and including dismissal.

The protection provided for extends to anyone who provides information related to an investigation, including an internal investigation.

The corporation's staff must refrain from confronting a person under investigation or conducting independent investigations. In the event that an investigation reveals criminal activity, the appropriate law enforcement agency will be informed.

10. PROCESSING DISCLOSURES OF WRONGDOING

Upon receipt of a disclosure or report of wrongdoing, the Audit Committee chair acknowledges its receipt to the extent possible.

The chair opens a file that is kept in a secure location to protect the confidentiality of information on the whistleblower.

It is then determined whether:

(i) The disclosure of wrongdoing actually deals with a subject covered by this policy

(ii) The alleged breach is serious

(iii) The disclosure of wrongdoing appears to be based on credible allegations and information

If the Audit Committee chair believes that the complaint meets the criteria in the preceding paragraph, he/she must refer to the Audit Committee so that it can conduct an investigation. To do this, the Audit Committee may use internal or external legal or accounting resources or anyone else if necessary.

During the investigation, the Audit Committee must have access to all of the corporation's books and records. The corporation's directors and employees must cooperate fully with the investigation.

In the conduct of its investigation, the Audit Committee must make reasonable efforts to protect the confidentiality of information on the whistleblower.

Investigations must take place as quickly as possible, depending on the nature and complexity of disclosures of wrongdoing and the questions that are often raised.

11. RECORD KEEPING

The Audit Committee chair must keep a file on all reports, complaints, questions, and related documents for at least three years.

12. AUDIT COMMITTEE'S REPORT

The Audit Committee chair keeps a record of all complaints to track their receipt, investigation, and resolution and prepares a periodic summary report of such reports for the Audit Committee.

Notwithstanding the foregoing, the Audit Committee chair must report to the Audit Committee immediately regarding any complaint that may have serious consequences for the corporation.

Appropriate corrective measures may be taken immediately based on the Audit Committee's recommendations.

13. EXAMINATION OF THE WHISTLEBLOWER POLICY

The effectiveness of this policy is monitored by the Audit Committee.

The Audit Committee, together with the board's Governance and Nominating Committee, assesses this policy annually to determine whether it provides an effective confidential and anonymous procedure for disclosing wrongdoing.

INFORMATION DISCLOSURE POLICY AND PROCEDURE

APPROVED BY THE GOVERNANCE AND NOMINATING COMMITTEE ON SEPTEMBER 6, 2013
APPROVED BY THE BOARD OF DIRECTORS ON NOVEMBER 12, 2013

TABLE OF CONTENTS

1. OBJECTIVE AND SCOPE

The objective of this information disclosure policy and procedure (the "Policy") is to ensure that:

1.1 Disclosures intended for the public (investors, the media, analysts, the general public, etc.) from the board of directors and the executive committees of NAPEC Inc. ("NAPEC" or the "Corporation") are conveyed in a timely fashion, are accurate and factual, and are issued in accordance with applicable legal and regulatory requirements;

1.2 This disclosure policy applies to all employees of NAPEC and its subsidiaries, its board of directors, and anyone who speaks on its behalf;

1.3 It concerns information disclosed in documents submitted to securities regulatory authorities and written statements made in NAPEC annual and quarterly reports, news releases, letters to shareholders, presentations made by senior management, information contained on the NAPEC website, and other electronic communications, as well as in oral statements made during meetings and phone conversations with analysts and investors, interviews with the media, speeches, press conferences, and conference calls.

2. DISCLOSURE RESPONSIBILITY

2.1 The president and chief executive officer of NAPEC and/or the chair of the board of directors and/or the chief financial officer determine whether the public disclosure of new facts is justified, and if deemed necessary, the board members are consulted.

3. PRINCIPLES OF DISCLOSING MATERIAL INFORMATION

3.1 Material information is generally defined as any information relating to NAPEC that results in or could reasonably be expected to result in a significant change in the value of NAPEC securities, or that could reasonably be expected to have a significant influence on a reasonable investor's investment decisions regarding such securities. The term "material information" should be interpreted in the wide sense. In complying with the requirement to disclose forthwith all material information under applicable laws and stock exchange rules, NAPEC adheres to the following basic disclosure principles:

a) Material information is published through news releases as soon as management is made aware of it or, if management is already aware of it, as soon as it becomes clear that it is material information.

b) In certain circumstances, such disclosure may be unduly detrimental to NAPEC (e.g., information that may prejudice negotiations in a corporate transaction), in which case such information is kept confidential until it is appropriate to publicly disclose it.

c) Disclosure must include any information that, if not disclosed, would make the rest of the message misleading.

d) Unfavorable material information must be disclosed as promptly and completely as favorable information.

e) Communicating material information not yet disclosed to the public may not be selective.

f) Previously undisclosed material information must not be disclosed to selected individuals (e.g., in an interview with an analyst or in a telephone conversation with an investor). If previously undisclosed material information has been inadvertently disclosed to an analyst or any other person not bound by an express confidentiality obligation, such information must be broadly disclosed immediately via a news release.

g) Disclosure of material information is monitored to establish whether previously disclosed material information has become false or misleading in the advent of some event, in which case the disclosed information must be corrected immediately.

h) Posting information on the websites of NAPEC and its subsidiaries does not alone constitute adequate disclosure of material information.

4. MAINTAINING CONFIDENTIALITY

4.1 Any employee, director, officer, or insider privy to confidential information is prohibited from communicating such information to anyone else, unless it is necessary to do so in the course of business. Efforts are made to limit access to confidential information and undisclosed material information only to those who need to know the information, and such persons are advised that the information is to be kept confidential.

4.2 Outside parties privy to undisclosed material information concerning NAPEC are advised that they must not divulge such information to anyone else, other than in the necessary course of business, and that they may not trade in NAPEC's securities until the information is publicly disclosed.

4.3 In order to prevent the misuse or inadvertent disclosure of material information, the procedures set forth below must be observed to the extent possible:

a) Documents and files containing undisclosed material information must be kept in a safe place to which access is restricted to individuals who need to know the information in the normal course of business.

b) Confidential matters must not be discussed in places where the discussion may be overheard.

c) Confidential documents must not be read or displayed in public places and should not be discarded where others can retrieve them.

d) NAPEC directors, management, and employees must ensure they maintain the confidentiality of information in their possession both inside and outside the workplace.

e) Transmission of documents by electronic means, such as by fax or directly from one computer to another, must be made with caution and only where it is reasonable to believe that confidentiality will be maintained.

f) Unnecessary copying of confidential documents and documents containing undisclosed material information must be avoided; they must be promptly removed from conference rooms and work areas after meetings have concluded.

5. DESIGNATED SPOKESPERSONS

5.1 To minimize the risk of selective disclosure and ensure that clear messages are communicated to the public, NAPEC designates a limited number of spokespersons responsible for regular communication with the investment community, the media, and the public. Only the following individuals may answer questions dealing with NAPEC's financial situation or financial results, as the case may be:

- President and chief executive officer
- Chair of the board of directors
- Chief financial officer

(hereinafter referred to as "Spokespersons")

These individuals may occasionally designate other members of the Corporation to take their place, if required, or to respond to specific inquiries.

Similarly, any approach to the media concerning these topics may be made only by the abovementioned individuals. In all cases, Spokespersons must express the point of view of NAPEC and not their own opinions.

6. NEWS RELEASES

6.1 Once the president and chief executive officer of NAPEC and/or the chair of the board of directors and/or the chief financial officer determine that new facts are material, they authorize the issuance of a news release unless such new facts must remain confidential for the time being.

6.2 If a material statement is made inadvertently in a selective forum, NAPEC immediately issues a news release in order to fully disclose such information.

6.3 If the stock exchanges where shares of NAPEC are listed are open for trading at the time of a proposed announcement, prior notice of a news release announcing material information must be provided to the Market Surveillance Department to enable a trading halt, if deemed necessary by the stock exchanges. If a news release announcing material information is issued outside of trading hours, the Market Surveillance Department must be notified before the market opens.

6.4 Annual and quarterly financial results are publicly released immediately following approval by the board.

6.5 News releases are disseminated through an approved news wire service that provides simultaneous national and/or international distribution. News releases are transmitted to all relevant regulatory bodies, major business wires, and national financial media.

6.6 News releases are posted on NAPEC's website immediately after release over the news wire.

7. RUMORS

a. NAPEC must not comment, affirmatively or negatively, on any rumors whatsoever, including rumors on the Internet; it must respond by saying that it is NAPEC's policy not to comment on industry or market rumors or speculation. If a stock exchange requests that NAPEC make a definitive statement in response to a market rumor that is causing significant volatility in the stock, the president and chief executive officer of NAPEC and/or the chair of the board of directors and/or the chief financial officer and, if deemed necessary, the members of the board of directors consider the matter and decide whether to make a policy exception. If the rumor is true in whole or in part, NAPEC immediately issues a news release disclosing the relevant material information, subject to the principles of disclosure of material information provided herein, which state that unduly detrimental material information may be kept confidential.

8. CONTACTS WITH ANALYSTS, INVESTORS, AND THE MEDIA

8.1 NAPEC recognizes that meetings with analysts, significant investors, and the media are a key part of its external outreach program. NAPEC may meet with them on an individual or small group basis as needed and contacts them or responds to their calls in a timely manner in accordance with this Policy.

8.2 Information communicated in individual or group meetings does not constitute sufficient disclosure of information deemed material and undisclosed. If NAPEC intends to announce material information at an analyst or shareholder meeting or a press conference, the announcement must be preceded by a news release.

8.3 During such meetings, authorized NAPEC spokespersons disclose only information that is known to the public or nonmaterial. They do not alter the materiality of information by breaking down the information into smaller, nonmaterial components. They must also ensure that no material information is selectively disclosed. If NAPEC management deems that this is not the case, all measures are taken to ensure that such material information is immediately disclosed to the public.

9. FORWARD-LOOKING INFORMATION

9.1 Financial guidelines and any other forward-looking information may be disclosed to a range of audiences to better evaluate NAPEC's future. The following principles must be observed when disclosing such information:

a) NAPEC's board of directors must approve, whenever possible, financial guidelines disclosed to the public.

b) If the information is deemed material, it is released through a news release, in accordance with this Policy.

c) The information is clearly identified as being forward-looking.

d) Depending on how the information is reported, an oral or written statement identifies the assumptions, risks, and uncertainties likely to cause the actual results to differ substantially from the results provided in the forward-looking information. Such statement also indicates that the information is valid as at a specific date.

e) Forward-looking information is prefaced by a statement that disclaims NAPEC's intention to update or revise the forward-looking information, whether as a result of new information, future events, or otherwise. Notwithstanding this disclaimer, if subsequent events prove previous forward-looking information to be substantially off target, NAPEC may choose to issue a news release updating such information or explaining the reasons for the difference.

10. DISCLOSURE RECORD PERIODS

10.1 The corporate secretary of NAPEC maintains a five-year file containing all public information about NAPEC, including continuous disclosure documents and news releases.

11. QUIET PERIODS

11.1 In order to avoid the potential for selective disclosure, NAPEC observes a quarterly quiet period, during which NAPEC does not comment on current performance other than responding to inquiries concerning factual matters. The quiet period in any fiscal quarter commences 30 days prior to the scheduled release of quarterly or annual results and ends 24 hours after a news release disclosing quarterly or annual results is issued.

11.2 During a quiet period NAPEC may, however, hold discussions and take part in meetings, investor conferences, telephone conversations regarding information not related to benefits, and unsolicited requests dealing with factual questions with analysts, the media, or investors, provided that only public or nonmaterial information is involved.

12. RESPONSIBILITY FOR ELECTRONIC COMMUNICATIONS

12.1 This Policy also applies to electronic communications. Accordingly, the Spokespersons are also responsible for electronic communications.

12.2 The chief financial officer is responsible for updating the investor relations section on the NAPEC website and, along with the corporate secretary, for monitoring all NAPEC information posted on the website to ensure that it is accurate, complete, up-to-date, and in compliance with relevant securities laws.

12.3 The chief financial officer is also responsible for responses to electronic inquiries. Only public information or information that could otherwise be disclosed in accordance with this Policy is used to respond to electronic inquiries.

12.4 The NAPEC website does not generally contain links to third party websites. The few exceptions to this rule must be approved by the president and chief executive officer. Any such links include a notice that advises the reader that he or she is leaving the NAPEC website and that NAPEC is not responsible for the content of the other site. For example, such a notice might read, "You are now leaving the NAPEC website. NAPEC undertakes no obligation whatsoever to review, update, or ensure the accuracy of information on other websites. NAPEC assumes no liability whatsoever for the legality and copyright compliance of documents on other websites."

12.5 Investor relations documents appear in a separate section of the NAPEC website. All data posted on the website, including textual and audiovisual material, must show the date such material was issued. Any material changes in information must be updated immediately.

12.6 In order to ensure that no undisclosed material information is inadvertently disclosed, employees are prohibited from participating in online chat rooms or newsgroup discussions on matters pertaining to NAPEC's activities or securities. Employees who encounter a discussion pertaining to NAPEC must advise the chief financial officer and the corporate secretary immediately, so that the discussion can be monitored.

13. COMMUNICATION OF THE POLICY

13.1 All employees, directors, and authorized Spokespersons of NAPEC are informed of this Policy and its importance. The Policy must be posted on the NAPEC website and copies are provided to the directors, executive committee members, and other employees of NAPEC likely to be called upon to make decisions regarding the disclosure of information under the terms of this Policy. These same individuals must understand this Policy and its relevance so as to ensure its compliance with applicable laws.

13.2 Any employee who violates this Policy may face disciplinary action up to and including termination of his or her employment with NAPEC. A violation of this Policy may also constitute a violation of certain securities laws. NAPEC may refer the matter to the appropriate regulatory authorities, which could impose penalties.

14. FINAL PROVISIONS

14.1 The NAPEC board of directors is responsible for monitoring implementation of this Policy and ensuring that it complies with applicable laws and is communicated to its directors and officers. All directors, officers, and employees of NAPEC are responsible for acting in accordance with NAPEC's policies. The board of directors may review and amend this Policy from time to time if it deems it appropriate.

NAPEC

INFORMATION TECHNOLOGY POLICY

APPROVED BY THE CORPORATE GOVERNANCE AND NOMINATING COMMITTEE ON JANUARY 12, 2016

APPROVED BY THE BOARD OF DIRECTORS ON JANUARY 13, 2016

INFORMATION TECHNOLOGY POLICY

1. PURPOSE

NAPEC is committed to have adequate and end user friendly information technology deployed allowing employees and interested third parties to work in a compelling information technology environment. This will be balanced between functionality, business requirements, and cost.

All existing NAPEC policies also apply to employee conduct and use of Information technology resources, including the Code of Professional Ethics and Business Conduct.

2. SCOPE

Within its strategic plan, information technology is a core component to enable NAPEC to achieve its vision. Information technology will be leveraged to increase efficiencies, increase collaboration, assist our employees to be effective, and assist on contributing to commercial success.

Information technology resources (i.e. pc's, smart phones, etc.) will be provided by NAPEC to employees to assist them in achieving their obligations and responsibilities for results.

For the above stated subject, without being limitative, the Vice President Information Technology recommends to the NAPEC Executive Committee the directives, guidelines, processes, procedures, programs, tools, hardware and software to enable employees in their job function, the management of technology resources, and the management of information data assets.

3. RESPONSIBILITIES

Each manager has the responsibility to communicate and ensure compliance of the Information Technology Policy along with its directives, guidelines, processes, procedures, and programs. The manager has a duty of accountability toward the employee and the business.

The President and Chief Executive Officer ensures that NAPEC has the essential resources to provide information technology solutions to enable employees to carry out their job function in the most efficient and cost effective manner. On an annual basis the Board of Directors through the Corporate Governance and Nominating Committee, receive from the President and Chief Executive Officer and/or the Vice-President Information Technology the information on application of the Policy.

4. QUESTIONS

Any question related to this Policy must be submitted to the Vice-President, Information Technology or to the General Counsel and Corporate Secretary.

NAPEC

Corporate Directive
Information Technology Employee Guidelines

Vice-President, Information Technology
January 29th, 2016

Table of Contents

EMPLOYEE GUIDELINES

Introduction

The "Corporate Directive: Information Technology Employee Guidelines" expresses the NAPEC (NAPEC and/or subsidiaries) Strategic Guidance and its business units in terms of Information Technology. Any reference to NAPEC throughout this document also covers any and all subsidiaries of NAPEC unless expressed otherwise. It aims to set priorities, to document, and to establish the parameters regarding Information Technology. It includes guiding principles, roles and responsibilities of interested persons, and prescribe the behavior to be adopted considering the obligations of legal and the administrative nature of NAPEC. It aims to:

- Protect NAPEC information data assets regarding the use and handling of data, electronic exchanges, use of information technology, telecommunications, and computer systems;
- Establish the rules, expectations, processes, and the requirements of the management team needed to operate safely and reliably the information data assets of NAPEC.
- Ensure adequate protection of information data assets held by physical and electronic security perimeters (e.g. buildings, rooms, type of access, etc.). In addition, ensure that access to these areas is reserved for individuals and entities authorized and that the access to information data assets is closely monitored to detect any use or access not authorized.
- Ensure that each employee understands what are their responsibilities, their role, and the consequences of their decisions on the security of information data assets.
- Educate employees in the importance that information security has to protect the business.

1. Scope

Covered assets: this directive applies to the following information data assets: those belonging to NAPEC (or subsidiaries) and utilized by it or by a service provider or a third party.

Interested persons: this directive applies to any person performing work or providing services to NAPEC (or subsidiaries), on a permanent or temporary basis and responding in all or in part to the following definitions:

- **Employee**: Any employee of NAPEC that uses and accesses NAPEC information systems in the exercise of their function.

- **Non- Employee**: Any individual or legal entity and having been duly authorized by NAPEC to access the information data asset, which is not under the direction or control of NAPEC in the exercise of its functions, has the same employee obligations.

Activities: all activities related to access and use of all forms of information data assets of NAPEC, that these are conducted on its premises, and/or in another location or remotely.

Exclusions: This guideline applies in all cases, except in the circumstances when a specific guideline may be in force in certain situations only, or when the owner of the guideline found that, in a particular case, a control is not necessary and that the decision has been documented. This will require the approval of the NAPEC EXCOM.

2. Definitions

Information Data Assets - A repository or collection of electronic information, a system or media, documentation, information technology, an installation or a set of these items, acquired or formed by an organization. This could be in the form of email, scanned documents, documents in various formats (i.e. PDF, MS Word, MS Excel, etc), texts, instant messages, social media, shared network storage, or any other type of data.

Data - Representation of information encoded in a format for processing by a computer system. Data can be classified as ***Confidential, Sensitive***, or ***Public***.

- **Confidential Data** - Defined as whose disclosure, alteration, loss or destruction might jeopardize NAPEC and/or their customers and, as such, NAPEC becomes vulnerable. The disclosure of this type of Corporate and/or Customer data could put the organization at significant financial or legal risk. Examples would be employee social security numbers, employee banking information, access to corporate banking/funding operations, customer data in which NAPEC has signed a Non-Disclosure Agreement.

- **Sensitive Data** - Defined as whose disclosure, alteration, loss or destruction may have a negative impact to operations and internal data that is not meant for public disclosure. Examples would be contracts with third party suppliers, employee performance reviews, organizational charts, project bid details, project bidding processes.

- **Public Data** - Defined as whose disclosure, alteration, loss or destruction would not jeopardize NAPEC and/or their customers

Security Incident - Defined as an event (either proactively detected or detected after the fact) either actively or potentially having endangered or is likely to compromise the security of information assets.

Information - Defined as an element of knowledge (voice, data, image) which may be stored, processed or transmitted using a computer, printer, or other electronic device.

Information System - Defined as a computer system or set of components/hardware/processes for collecting, creating, storing, processing,

updating, reproducing, and distributing information, typically including hardware, software, system users, and the data itself.

Information Technology **-** Any software, software or electronic equipment, computer and telecommunications, fixed or portable equipment, and any combination of these elements that are used to create, collect, store, process, communicate, protect or have the information in any form.

User **-** Anyone who has a logical or physical access to information data assets.

Owner **-** Defined as a service or an administrative unit which is the main user of an application or information data asset, which is ultimately responsible for its classification, use, protection, review to confirm access, and the treatment of the form of the information data asset.

3. Guideline Statements

This Information Technology Guideline is based on the following principles:

Guidelines

- Information Data Assets remain at all times the property of NAPEC, regardless of where they are located, how they are stored, and the format. NAPEC has a right to access and review the use of any Information Data Assets by any users.

- Information Data Assets are essential to the day-to-day operations and must undergo a classification process, an assignment of ownership, an organizational review, and have adequate protection. All efforts will be made to protect Information Data Assets against any unauthorized access or illicit use.

- Any Information Data Asset in any format that is being stored (shared network storage), or residing (email), or being transmitted through the NAPEC network (web browsing history) is and will remain the sole property of NAPEC. Examples are emails sent to a work email address that may be personal in nature, pictures or other files that may be personal in nature that are contained in an email or stored on the NAPEC network, any and all voice mails stored on a voice mail system.

- It is understood that NAPEC has not obligation to store, retain, or reproduce any type of Information Data Asset that may be considered personal. This would include but no limited to pictures, files, voice mails, email distribution lists, or contact information. These are and will remain the sole property of NAPEC.

- NAPEC reserves its right to do surveillance, to access, to recuperate and to read any communications that the employees have created, sent, received or memorized on the Corporation's Electronic Communication Systems and this, without prior notice to the employee(s) which is(are) the author(s) of these communications. In addition, the Corporation reserves its rights to investigate and to do a follow-up with respect to any irregularity and to divulge, if necessary,

any communication to any official authority and/or organization or to any interested third party.

- The protection of Information Data Assets is based on the principle that users have access only to information systems and data that are necessary and permitted in the exercise of their functions. NAPEC will follow the concept of "least privileged access" when grating access to NAPEC systems.

- NAPEC must ensure protection of information data assets against any unauthorized access by implementing controls ensuring authentication, accountability, and traceability of actions.

- NAPEC must ensure adequate protection of information data assets against corruption, disclosure or loss at the time of data entry, loss during transmission, and against loss of storage.

- The use of the information data assets of NAPEC is a privilege. This privilege may be revoked at any time, to any user who does not comply with the Information Technology Guideline.

- Agreements and contracts in connection with Information Data Assets must ensure respect for the security and protection of the requirements detailed in the Information Technology Guideline.

- Anyone that has been granted access to Information Data Assets accepts the responsibility for the security and is accountable for the protection of Information Data Assets. This includes password protection and not sharing user accounts.

- NAPEC must take the necessary steps to ensure that third parties and suppliers are made aware of the policy and be required to comply with the policy.

- NAPEC must fulfil its responsibilities to the customer and third parties by taking the necessary measures to prevent any disclosure of proprietary information belonging to them and implementing methods that can respond quickly to security incidents.

- NAPEC must support compliance as well as the promotion of the rules, laws, and regulations governing the confidentiality, integrity and availability of information data assets as it applies in the country, province, or state.

- NAPEC undertakes to exercise its activities so as to ensure an adequate level of security to protect its information data assets. These information data assets are secured based on definitions of classification; confidential, sensitive, and public. NAPEC also undertakes activities to ensure integrity and availability to information data assets to limit to an acceptable level, risks to information data assets.

- ***Integrity*** - Integrity is defined as information data assets that during their treatment or their transmission, does not undergo any alteration or destruction of unauthorized manner (malicious or accidental) and remain in a format allowing their use in being protected against failures, assaults and attacks.
- ***Availability*** - Availability is defined as the ability to have the information data assets be accessible and usable in due time and in the manner required by a user.

4. Incident Reporting

A person who has knowledge of an act, an irregular situation, or behavior that could constitute among others:

- A violation of the Information Technology Employee Guidelines, its guidelines, its standards, its procedures and its computer security measures;
- An attempt of unauthorized access to NAPEC information systems or computer systems;
- Any act that can compromise safety and cause deliberate damage such as theft, the intrusion and misuse of information systems, fraud, etc..

Must inform the CITVP or IT Manager expeditiously or may inform their immediate supervisor.

5. Awareness and Training

NAPEC must have a program to provide awareness and training of users to the security of information data assets, to the consequences of a breach of security, as well as the roles and obligations of the persons concerned in the process of protection of these information data assets.

Awareness of the policy will be made:

- At the hiring of any new employee; and
- An annual basis to all employees of NAPEC.
- As needed based on an increase in detected activities (i.e. email phishing)

6. Guideline Management

In order to ensure compliance to the Information Technology Employee Guidelines, employees must be made aware of its existence, it must be clearly communicated, published, and available to all NAPEC employees. The Information Technology Employee Guidelines and the standards must be accessible and available at all times..

7. Approval of the Information Technology Employee Guidelines

The implementation of the Information Techonology Employee Guidelines, standards, procedures and processes coincides with their approval by the NAPEC Executive Committee. They replace all information technology guidelines, standards, methods and the earlier proceedings specific to employees.

8. Distribution

This directive is published and distributed for the information and guidance of users. This distribution serves as communication and dissemination.

9. Respect

Processes, standards, and procedures put in place to support the Information Technology Employee Guidelines represent the foundation on which checks and conformity assessments are carried out. It is the responsibility of users to comply and they must answer for their conduct under the policies, guidelines, standards and procedures of NAPEC.

10. Sanctions

Any user who violates the Information Technology Employee Guidelines is subject to disciplinary action which could lead to dismissal and legal or criminal proceedings. The Manager of the user, Vice President of Human Resources, and the Vice President of IT will determine disciplinary measures to be taken.

11. Roles and Responsibilities

Executive Committee

The Executive Committee (SC) is responsible for:

- Review and to distribute the Information Technology Employee Guidelines and standards supporting it and must provide and coordinate the efforts necessary to achieving the objectives;
- To approve the initiatives put forward for enhancing the security of information data assets before their implementation;
- To ensure adequate supervision of projects and safety initiatives. It ensures that executives, corporate IT, and subsidiaries have in hand all the tools and all the knowledge and skills necessary to perform their work.

Vice-President, Information Technology

CITVP is responsible for:

- To develop the strategic plan, the vision and direction of the Information Technology Employee Guidelines;

- Identification and the overall assessment of risks to Confidential and Sensitive data and ensure data integrity and availability of data;
- The identification of the owner of information data assets within NAPEC;
- To develop and manage processes, standards, and safety procedures. The CITVP will ensure their compliance and will have the exclusive right to authorize any derogation or exception to these policies, standards and procedures for the security of information data assets;
- To ensure the governance of security suppliers, partners and business units;
- To determine the security requirements in accordance with legal and regulatory compliance obligations;
- To develop adequately equipped security systems as defined in the different standards and norms of NAPEC;
- Review and distribute the Information Technology Employee Guidelines and standards supporting it. The CITVP must coordinate the efforts necessary to achieving security objectives;
- To inform NAPEC of threats and vulnerabilities current and emerging, ensuring that the company is sufficiently aware of the risks faced by information data assets, and to set up sufficient measures to mitigate them;
- To examine security vulnerabilities, assess the threats and vulnerabilities, and recommend updates and upgrades;
- To assess the records of security incidents (frauds, attacks, etc.) and review reports, monitor and adjust any violation of security and abnormal activities of confidentiality, integrity and availability of systems and data. Issue safety recommendations/requirements;
- To ensure adequate supervision of projects and safety initiatives that have IT components. It ensures that IT Managers of subsidiaries have all the tools and all the knowledge and skills necessary to perform their work;
- To participate in the investigation requests related to security, at the request of the Vice President, Human Resources, Finance, and Legal;
- Audit periodically all computing environments hosting the information data assets of NAPEC and test practices and safety procedures to ensure that all conform to the standards established. Make the necessary recommendations for patch management;
- To ensure by various means (training, documentation, etc.) that users and IT Managers of subsidiaries understand and apply practices, procedures and safety standards;
- Coordinate the activities of the External Audit for areas related to IT.

IT Manager of Subsidiaries

IT Managers are responsible for:

- To provide awareness to employees of the subsidiary they support to the issues related to the security of information data assets;
- The identification of the owner of information data assets within the subsidiaries;
- To ensure that information data assets are used in accordance with security standards, guidelines, processes, and procedures;

- To act as soon as possible when an incident occurs to protect information data assets, report to the CITVP when incidents occur, when necessary reviews event logs to identify potential areas of security weakness, reviews documentation aimed at the protection of information data assets;
- Participate in the development of policies ensuring compliance with the requirements for security and protection of information data assets included in contracts and agreements with suppliers;
- To facilitate the implementation of emergency measures to ensure delivery of the computer systems and retrieve critical data deemed force majeure.

Owner of Information Data Assets

The Owner of an Information Data Asset is responsible for:

- To ensure that the information data assets they own are classified accurately and protected adequately;
- To understand the risk associated with the breach of confidential or sensitive information data assets and the impact to the loss of data integrity, and loss of access to information data assets;
- To ensure that the necessary measures are put in place to minimize any risks that have been identified;
- To allow the use and access to information data assets that they own;
- Adhering to the Information Technology Employee Guidelines and ensuring that their staff act so as to protect the information data assets of NAPEC;
- To inform immediately the CITVP any deviations or any violation of the policies, standards and security procedures.

The Administrator of the Information Data Assets

The IT Managers are responsible for granting access to information data assets after the appropriate authorization has been provided by the owner of the information data asset.

The User

It is the responsibility of users to preserve all information data assets entrusted to them. They must understand and conform to policy, standards and security procedures of NAPEC.

They are invited to discuss any potential problems of security with their immediate supervisor or to share any concerns that they have with the CITVP.

12. Directive Changes

Revision

Any revisions and changes will be documented on the last page on this document by date and by version control.

Approval

This Corporate Directive and Information Technology Employee Guidelines is approved by the Executive Committee on January 29, 2016.

This page is purposely left blank

Internet Acceptable Use Guideline
Guideline for use of the Internet when accessing the NAPEC network

1. Objective.

The objective of this guideline is intended to regulate the access and use of the internet in the NAPEC network. The internet should be used in the context of an employee's function and role at NAPEC. Given the non-restrictive nature and scope of the Internet, the user must be aware that visiting certain sites is not acceptable. NAPEC information systems can track the sites visited by each user and can be reviewed at any time without consent of the employee.

2. Scope

This guideline governs and applies to all NAPEC and subsidiary employees, contractors, consultants, and other individuals who utilize either a company owned or personally owned mobile device to access, retrieve, copy, read, store, backup any data residing on the NAPEC network. The guideline also applies to all NAPEC and subsidiary employees, contractors, consultants, and other individuals operating a company owned/leased/rented vehicle at any time. This guideline also covers but not limited to laptops, notebooks, tablets, mobile phones, smart phones, and PDA's either company owned or personally owned.

3. Guidelines

Some examples (but not limited to) the type of sites and activities which are not acceptable:

- Internet sites that may be deemed as pornographic, obscene, hateful, which promote drugs and violence
- The use of an Internet Service Provider while in a NAPEC facility or site other than the service that has been contracted by NAPEC
- Bypassing security protection protocols and control measures
- Disseminate information that may cause harm to NAPEC either financial or reputation
- Accessing the internet from another NAPEC users account
- The use of the internet to make phone or voice calls over the internet (i.e. VoIP, Skype, etc) unless reviewed and approved by the CITVP. This practice can have a negative impact to the performance of the network and could cause a breach of security protocols.
- Download and/or distribute pirated content or software
- Download and/or distribute unlicensed software
- Download for personal purposes, files and videos, live stream radio, live stream video, or other such activity that could have a negative impact to the performance of the network.

NAPEC tolerates that Internet service is used for personal purposes provided that this does not negatively impact productivity and performance of the network. The activities listed above that are not acceptable must be respected and the use of the Internet for personal purposes must be limited to the strict minimum. It is the responsibility of the users to respect all the guidelines at all time and internet usage not be detrimental to the performance of the employee.

It is the responsibility of the CITVP to ensure by various means (training, documentation, etc) that employees understand and apply the rules detailed in this guideline.

4. Definitions, abbreviations.

Pirated Software – Software that has been copied, distributed, used, or modified in an illegal manner which the copyrighted owner or contractual would have a right to pursue legal or civil action. Examples would be downloading software (i.e. Adobe, Microsoft Office, etc) and using it in a manner that circumvents a standard licensing agreement.

Pirated Content – Content (video, audio, or other electronic format) that has been copied, distributed, used, or modified in an illegal manner which the copyrighted owner or contractual owner would have a right to pursue legal or civil action. Examples would be the copy and distribution of movies, music, and videos which authorization to do so does not exist.

Abbreviations

CITVP	Corporate Information Technology Vice President
VoIP	Voice over Internet Protocol

Social Media Acceptable Use Guideline

Guideline for use of Social Media when accessing the NAPEC network or as a NAPEC employee

1. Objective.

The objective of this guideline is intended to provide guidelines when accessing Social Media or representing NAPEC and/or subsidiaries of NAPEC.

Merriam-Webster defines Social Media as: ***"forms of electronic communication (as Web sites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos)".***

Social Media can be a valuable means in which NAPEC and/or the subsidiaries utilize to create awareness with current and future customers. It can be used to promote our brand, our capabilities, and promote our success stories. It can also be used in a manner that creates unintended consequences that could harm our brand, reputation, and place in the market.

NAPEC information systems can track the sites visited by each user and can be reviewed at any time without consent of the employee.

2. Scope

This guideline governs and applies to all NAPEC and subsidiary employees, contractors, consultants, and other individuals who utilize NAPEC resources to access Social Media or represent themselves as employees of NAPEC and/or all subsidiaries on Social Media. This guideline also covers but not limited to how employees can access Social Media through laptops, notebooks, tablets, mobile phones, smart phones, and PDA's either company owned or personally owned devices.

3. Guidelines

In general, what you do outside of work through Social Media is your own business. However, although not intentional, your actions or behavior in Social Media may have a negative impact to NAPEC and/or subsidiaries.

- Accessing Social Media sites that may be deemed as pornographic, obscene, hateful, which promote drugs and violence **is not acceptable**.
- Bypassing security protection protocols and control measures to access Social Media sites **is not acceptable**.
- Disseminate information that may cause harm to NAPEC either financial or reputation **is not acceptable.**

- Posts or Blogs. When making a post of comment in a blog about NAPEC, its subsidiaries, or customers, you should point out and state that you are not an official spokesman for NAPEC, its subsidiaries, or customers. Add a disclaimer such as "The opinions and positions expressed are my own and don't necessarily reflect those of NAPEC".
- Respect the company branding. Do not modify, change, distort, or otherwise depict any logos in a negative manner.
- Be Professional. Understand that if in any way your post is related to the company, how you do it and interact with others is a reflection of the company.
- Permanent Record. Remember that once you post something on Social Media, it is more than likely there forever. Do not post something which you may regret later.
- When in doubt, do not post or comment.

NAPEC tolerates that Internet service is used to access Social Media provided that this does not negatively impact productivity and performance of the network. The activities listed above that are not acceptable must be respected and the use of Social Media must be limited to the strict minimum. It is the responsibility of the users to respect all the guidelines at all times and Social Media usage not be detrimental to the performance of the employee.

NAPEC and/or subsidiaries retain the right to restrict access to Social Media at any time if it is deemed detrimental to the performance of the employee by their Manager.

It is the responsibility of the CITVP to ensure by various means (training, documentation, etc) that employees understand and apply the rules detailed in this guideline.

4. Definitions, abbreviations.

Social Media – Merriam-Webster defines Social Media as: ***"forms of electronic communication (as Web sites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos)".***

Abbreviations

CITVP	Corporate Information Technology Vice President

Email Acceptable Use Guideline
Guideline for use of NAPEC Email and systems

1. Objective.

The objective of this guideline is intended to regulate the access and use of NAPEC Email (and subsidiaries) and systems supporting email. NAPEC email should be used in the context of an employee's function and role at NAPEC. NAPEC email, the storage of, and documents attached to NAPEC emails are the property of NAPEC. Due to the nature of our business and security management of email systems, email (received and sent) is scanned and may be blocked by filters.

2. Scope

This guideline governs and applies to all NAPEC and subsidiary employees, contractors, consultants, and other individuals who utilize NAPEC email. This guideline also covers but not limited to laptops, notebooks, tablets, mobile phones, smart phones, and PDA's either company owned or personally owned.

3. Guidelines

Some examples (but not limited to) the type of activities which are not acceptable:

- Confidential information or confidential information about our customers should not be shared via email outside of NAPEC without authorization at any time.
- Personal business. Personal business over email should be kept at a minimum and should not interfere with the job function of the employee.
- "Chain Letters" and other type of email "spamming" are not permitted through company email.
- Forwarding or sending pornography, pornographic jokes or stories, or any activity that could be considered sexual harassment.
- Any email or content of an email that discriminates against any protected classification including but not limited to race, religion, sex, ethnicity, age, disability, etc.
- Disseminate information that may cause harm to NAPEC either financial or reputation
- Accessing another employee's account unless provided an approval from their immediate Manager and the VP of HR. An example when this would be allowed due to business continuity is when an employee has left NAPEC or is on long term leave. This should then be restricted to the Manager of the former employee or HR.
- Forwarding or sending pirated content or software
- Forwarding or sending unlicensed software
- Download through an email link for personal purposes, files and videos, live stream radio, live stream video, or other such activity that could have a negative impact to the performance of the network.

NAPEC tolerates that the use of NAPEC email used for personal purposes provided that this does not negatively impact productivity and performance of the network. The activities listed above that are not acceptable must be respected and the use of email for personal purposes must be limited to the strict minimum.

NAPEC owns any communication sent via NAPEC email and any documents that may be attached or embedded in NAPEC email. NAPEC reserves the right to allow Management and other authorized staff to have access to any material on a NAPEC employees email at any time whether it is stored on the computer or server. Employees need to consider that any electronic communication received via NAPEC email or stored on NAPEC servers is not private.

NAPEC is also not responsible during or after employment for the storage of or to retain personal data in the form of emails, documents, pictures, or in any other electronic/digital format. In the event that any personal data is deleted, NAPEC is not responsible to restore or retrieve any personal data and will not be held liable for its loss.

It is the responsibility of the CITVP to ensure by various means (training, documentation, etc) that employees understand and apply the rules detailed in this guideline.

4. Definitions, abbreviations.

Pirated Software – Software that has been copied, distributed, used, or modified in an illegal manner which the copyrighted owner or contractual would have a right to pursue legal or civil action. Examples would be downloading software (i.e. Adobe, Microsoft Office, etc) and using it in a manner that circumvents a standard licensing agreement.

Pirated Content – Content (video, audio, or other electronic format) that has been copied, distributed, used, or modified in an illegal manner which the copyrighted owner or contractual owner would have a right to pursue legal or civil action. Examples would be the copy and distribution of movies, music, and videos which authorization to do so does not exist.

Abbreviations

CITVP	Corporate Information Technology Vice President
PDA	Personal Digital Assistant

PC Acceptable Use Guideline
Guideline for use of a NAPEC PC

1. Objective.

The objective of this guideline is intended to establish guidelines as to what is acceptable use of pc's and what is unacceptable use of pc's. The use of NAPEC (and subsidiaries) pc's should be used in the context of an employee's function and role at NAPEC. NAPEC provides pc's to employees to assist them to meet company goals, initiatives, and other company directed activities. It is the responsibility of the employee when using a NAPEC pc to do so in an ethical and lawful manner that maintains confidentiality, security of the network, adherence to policies and guidelines, and in a manner that protects the company against any potential legal issues.

2. Scope

This guideline governs and applies to all NAPEC and subsidiary employees, contractors, consultants, and other individuals who utilize a NAPEC pc. This guideline also covers but not limited to laptops, notebooks, tablets, and other computer devices provided by NAPEC

3. Guidelines

- The employee is responsible at all times for the care and security of the pc. The pc will be assigned to the employee as an asset. The employee must protect their pc against theft, loss, or damage.
- The employee is responsible for protecting and preventing the unapproved distribution of any intellectual property, proprietary information, private information, and confidential information that is stored on the pc.
- Only employees authorized by NAPEC and issued a pc are authorized to use the pc. Members of their family and friends are not authorized to use a NAPEC issued pc.
- All pc's will have password authentication for access to the NAPEC network enabled. Disabling password requirements is prohibited.
- Use of the pc for unlawful, unethical, or other activities against company policies or guidelines is prohibited
- Use of the pc to discriminate, harass, defame, abuse, or otherwise harm another person is prohibited.
- Use of the pc to engage in "hacking" activities, exchange pirated software, or any other illegal computer activity.
- NAPEC reserves the right to assign authorized personnel to audit and monitor pc's for security, compliance, maintenance, and unauthorized access at any time.
- Employees are prohibited from disabling or interfering with any corporate device management system, and end point security system, any malware software, or any other type of antivirus software.

- The pc as well as all of the content residing on it, are and remain the property of NAPEC
- Data that is stored on the pc and belonging to NAPEC must be saved on the shared network. Data stored on the shared network is backed up so in the event of a loss of data, it can be recovered. Data stored on a pc hard drive that is lost or can no longer be accessed on the pc hard drive, may not have the ability to be recovered.
- The pc must be connected to the NAPEC network at least every two weeks to allow for updates to corporate software, patches, or security updates.
- Employees are prohibited against accessing another employee's account unless provided an approval from their immediate Manager, the VP of HR, and the VP of IT. An example when this would be allowed due to business continuity is when an employee has left NAPEC or is on long term leave. This should then be restricted to the Manager of the former employee or HR.

NAPEC is also not responsible during or after employment for the storage of or to retain personal data in the form of emails, documents, pictures, or in any other electronic/digital format. In the event that any personal data is deleted, NAPEC is not responsible to restore or retrieve any personal data and will not be held liable for its loss.

It is the responsibility of the CITVPto ensure by various means (training, documentation, etc) that employees understand and apply the rules detailed in this guideline.

4. Definitions, abbreviations.

Abbreviations

CITVP	Corporate Information Technology Vice President

Mobile Device Acceptable Use Guideline

Guideline for use of Mobile Devices to ensure safety for employees, security of the NAPEC network, and guidance for usage

1. Objective.

The overall objective of this guideline is to promote a safe work environment where safety is first, to protect the integrity of the private and confidential information that resides on the NAPEC network, and ensure that the usage of mobile devices does not violate any law, creates non-compliance to licensing of software, and does not infringe on copyright laws.

Employee Safety – It is the responsibility of any employee of NAPEC and subsidiaries to work in a safe manner at all times and follow all safety protocols and procedures. With this guideline, NAPEC and all subsidiaries will have strict guidelines prohibiting the use of electronic devices while driving in order to protect NAPEC and subsidiary employees from injury or death, to protect other pedestrians and drivers from being injured or killed, and to protect NAPEC and subsidiaries from any liabilities inherent to these type of activities. It is the responsibility of any employee of NAPEC and subsidiaries to follow all safety guidelines and guidelines at a job site.

Information and Network Security - It is the responsibility of any employee of NAPEC and subsidiaries who uses any mobile device that has access to the corporate network and resources to ensure that all security processes and protocols are used in order to protect the NAPEC network. Only those devices approved by the CITVP may be used to access the NAPEC and subsidiaries network. The goal is to address threats of loss, theft, copyright infringement, malware, and non-compliance.

Guidance on Mobile Device Usage – It is the responsibility of any employee of NAPEC and subsidiaries to use any mobile device that conforms to established country, state, provincial, or other local laws. License non- compliance (i.e. pirated software) and copyright infringement (i.e. un-authorized use of music, videos, or applications) is prohibited. Mobile Devices issued by NAPEC and on a NAPEC Corporate Liable Account are not to be "tethered" (Tethering is when you turn you smartphone into a mobile Wi-Fi hotspot and share your phones 3G/4G data connection) or otherwise connected to an unsecure network or used to download non-work related information, applications, or software.

2. Scope

This guideline governs and applies to all NAPEC and subsidiary employees, contractors, consultants, and other individuals who utilize either a company owned or personally owned mobile device to access, retrieve, copy, read, store, backup any data residing on the NAPEC network. The guideline also applies to all NAPEC and subsidiary employees, contractors, consultants, and other individuals operating a company owned/leased/rented vehicle at any time. This guideline also covers but not

limited to laptops, notebooks, tablets, mobile phones, smart phones, and PDA's either company owned or personally owned.

3. Guidelines

Employee Safety

The following activities are prohibited at all times:

- Sending or reading text messages or emails when driving a company owned/leased/ rented vehicle or personal vehicle when conducting company business.
- Speaking on a hand held mobile device while driving a company owned/leased/rented vehicle or personal vehicle when conducting company business.
- Entering information into a GPS device (included GPS enabled smart phones and mobile phones) when driving a company owned/leased/rented vehicle or personal vehicle when conducting company business.
- Using a smart phone, cell phone, mobile phone, laptop, notebook, or any other computer device while driving a company owned/leased/rented vehicle or personal vehicle when conducting company business.
- Using a smart phone, cell phone, mobile phone, laptop, notebook, or any other computer device when refuelling a company owned/leased/rented vehicle or personal vehicle when conducting company business.
- Any other type of electronic device that requires user input while driving a company owned/leased/rented vehicle or personal vehicle when conducting company business.
- For vehicles with installed hand held radios (i.e. "CB's"), when the vehicle is in operation, the passenger and not the driver should be the person responding on the radio. Once the vehicle is parked in a safe and secure area, then the driver can use their discretion to use the installed hand held radio.

Safety considerations:

- Drivers will always stop the vehicle at the earliest convenient time in a safe area before making or receiving calls when "hand's free" devices are not being used.
- A "hand's free" device can be used to make and receive calls as long as safety is not being compromised.

Job Sites:

Due to the nature of our industry, working in proximity to energized equipment, potentially working in extreme terrain, and potentially working in extreme weather conditions, extra precautions must be taken and adhered to at all times.

- Use of any type of mobile device at a job site is prohibited unless otherwise noted or approved by the Supervisor. All safety procedures must be followed. This could include but not limited to proximity to exposed energized or potentially energized equipment.
- If approved at the job site, mobile devices can be used during breaks or during vehicle travel between job sites provided the person using the mobile device is not driving the vehicle.

- Mobile devices shall not be used by anyone while within the established proximity underground or overhead energized conductor(s); 3 meters in Canada, 30 feet in the US from the work zone.
- The use of any type of mobile device while working or riding in an elevated aerial lift device such as a bucket truck is prohibited unless approved being used as a two-way means of communication specific job tasks and if outside of the established proximity distance to exposed energized or potentially energized equipment.
- Personal mobile phone devices should not be carried on an employee's person during work time at a job site. The General Foreman or Management Representative at a job site will determine who the emergency contact person at the job site is and all employees will provide family members and friends the name and number to contact in the event of an emergency.
- All visitors to a job site must comply with all safety rules regarding the use of a mobile device.
- Prior to using a mobile device at a job site, all employees should move to a designated safe area. Once in a designated safe area for using a mobile device, employees should remain stationary when using a mobile device to avoid any chance of tripping, slipping, or injuring themselves.
- For vehicles with installed hand held radios, when the vehicle is in operation, the passenger and not the driver should be the person responding on the radio. Once the vehicle is parked in a safe and secure area, then the driver can use their discretion to use the installed hand held radio.

Information and Network Security
It is the responsibility of any employee of NAPEC and subsidiaries who uses any mobile device that has access to the corporate network and resources to ensure that all security processes and protocols are used in order to protect the NAPEC network. Only those mobile devices approved by the VP of IT may be used to access the NAPEC and subsidiaries network. The goal is to address threats of loss, theft, copyright infringement, malware, and non-compliance.

Guidance on Mobile Device Usage
Employees need to have an awareness of the costs associated with a mobile device. Streaming of audio, video, or other media that is not business related over a 3G or 4G network can substantially increase costs NAPEC and subsidiaries and is prohibited.

It is the responsibility of any employee of NAPEC and subsidiaries to use any mobile device that conforms to established laws. License non - compliance (i.e. pirated software) and copyright infringement (i.e. un-authorized use of music, videos, or applications) is prohibited.

A mobile device can be used as a "hot spot" to provide connectivity to the NAPEC network from a job site. This should be done when no other solutions exist or can be implemented. This should only be done over a secure network

Failure to follow this Guideline detailing Employee Safety, Information and Network Security, and Guidance on Mobile Device Usage can result in disciplinary action up to and including termination of employment.

4. Definitions, abbreviations.

Definitions

Mobile Device – Any type of electronic device that can receive and transmit data through WIFI, cellular, 3G, or 4G. Examples of some mobile devices are: laptops, notebooks, tablets, mobile phones, smart phones, and PDA's either company owned or personally owned.

3G - Short for third generation, is the third generation of mobile telecommunications technology. 3G allows for wireless voice telephony, mobile internet access, and video calls.

4G - Short for fourth generation, is the fourth generation of mobile telecommunications technology. 4G allows for mobile web access, IP telephony, video conferencing, and cloud computing.

Abbreviations

CITVP	Corporate Information Technology Vice President

NAPEC

HUMAN RESOURCES POLICY

APPROVED BY THE HUMAN RESOURCES AND COMPENSATION COMMITTEE ON MARCH 24, 2015
APPROVED BY THE BOARD OF DIRECTORS ON MARCH 25, 2015

HUMAN RESOURCES POLICY

1. PURPOSE

This Policy is NAPEC Inc.'s ("NAPEC") commitment towards its employees. NAPEC is respectful of the individual and interested in having an organizational capacity that will enable it to meet its business objectives. The employee contributes to the business results of NAPEC.

2. SCOPE

Within its strategic plan, NAPEC considers the employees as being essential to achieve its vision. The health & safety, the competency evolution, the engagement, the working conditions and the performance are factors contributing directly to the success of NAPEC. The employee assumes its obligations and responsibilities of results.

For the above stated subject, without being limitative, the Vice President Human Resources recommends to NAPEC Executive Committee the directives, programs and procedures to govern and materialize the instructions in connection with the management of the human capital.

3. RESPONSIBILITIES

Each manager has the responsibility to communicate and ensure compliance of the Human Resources Policy along with its directives, programs and procedures. The manager has a duty of accountability toward the employee and the business.

The President and Chief Executive Officer ensures that NAPEC has the essential elements to foster a healthy management of employees. On an annual basis the Board of Directors and, as the case may be, its committees, receive from the President and Chief Executive Officer and/or the Vice President Human Resources the information on the current status and topics of this Policy.

4. QUESTIONS

Any question related to this Policy must be submitted to the Vice President Human Resources or to the General Counsel and Corporate Secretary.

NAPEC

COMPENSATION POLICY

APPROVED BY THE HUMAN RESOURCES AND COMPENSATION COMMITTEE ON APRIL 23, 2015
APPROVED BY THE BOARD OF DIRECTORS ON MAY 4, 2015

COMPENSATION POLICY

1. PURPOSE

This policy is NAPEC Inc.'s ("NAPEC") commitment to have a competitive compensation policy within its financial capacity and the applicable legal requirements. The employee must act at all times in accordance with the values and rules of NAPEC.

2. SCOPE

To achieve its strategic plan, NAPEC considers that for retaining and attracting talent, motivate and mobilize its employees, to create value and have working conditions adapted to its environment and market, a compensation policy is necessary. Various compensation programs arise from this policy taking into consideration the levels of organizational responsibilities. While respecting the authority grid, it is important to have several compensation components enabling to reach and exceed the profitability targets within a culture where each one understands its role and expected contribution.

Compensation must be at all-time directly link to performance improvements and recognition of value added while supporting talent retention and attraction. More precisely:

Direct Compensation:

- Competitiveness and fairness of base pay taking into consideration the activity sector, seize of the business unit and the geographical area;
- Annual bonus based on individual and team objectives. Objectives must be measurable, quantified and contributive to performance and added value;
- Stock purchase option plan limited to higher management positions and linked to creation of added value;
- Long term incentive program linked to business projects for designated management employees not entitled to stock purchase option plan, based on base pay or a lump sum.

Indirect Compensation:

- Pension plan;
- Group insurance;
- Support professional membership requirements;
- Other benefits, e.g. vacation, car allocation, etc.

With integrity, loyalty and diligence, the employee, by its presence, his accountable for the quality of work, the quantity of work and the results.

For the above topics, without being exhaustive, the Vice President of Human Resources recommends to NAPEC's management committee the directives, programs and procedures deemed necessary to manage the activities and formalize the instructions linked to global compensation.

3. RESPONSIBILITIES

The management committee has the responsibility to approve and to ensure the application of the Compensation Policy through its directives, programs and procedures.

The President and Chief Executive Officer ensures that NAPEC has the essential compensation elements to foster a healthy management of employees. On an annual basis the Board of Directors and, as the case may be, its committees, receive from the President and Chief Executive Officer and/or the Vice President Human Resources the information on the current status and topics of this Policy.

4. QUESTIONS

Any question related to this Policy must be submitted to the Vice President Human Resources or the Chief Financial Officer of NAPEC.

Riggs Distler & Company, Inc.
4 Esterbrook Lane
Cherry Hill, NJ 08003-4002
Phone 856/433-6000 Fax 856/433-6035

New Hire Drug Screening Test Administration Affirmation

A drug screening test was administered for the newly-hired employee:

NAME: _____

This record is only for informational purposes and will be kept on file with the employees records in the Human Resources Department.

_____
Tester Signature

_____
Tester Name

_____
DATE

CONFIDENTIALITY AND NON-SOLICITATION AGREEMENT

Mr._____, domiciled and residing at _____, acknowledges and commits, during the entire term of his employment with Riggs Distler & Co., Inc., a subsidiary of CVTech Group, and thereafter, without limit as to time:

a) Not to help anyone meet the clients of the Company or one of its subsidiaries and not to disclose or reveal their names and addresses and, especially, without limiting the generality of the foregoing, not to make any attempt to take advantage, to the detriment of the Company or one of its subsidiaries or any other business associated with the Company, if such exists, of contracts entered into with any client of the Company or one of its subsidiaries while he/she is in the service of the Company;

b) To surrender and transfer to the Company all his rights and interests in any inventions, techniques, drawings and processes he may have imagined, designed or created and in all discoveries he may have made since he has been in the Company's employ, and all rights and interests in any inventions, techniques, drawings and processes he may imagine, design or create and that are related to the activities of the Company, and in all discoveries he may make during the term of his employment, whether or not these inventions, techniques, drawings or processes were or are imagined, designed or created or these discoveries were or are made, directly or indirectly, by him alone or jointly with others, by or for the Company, all such rights and interests being, under the terms and conditions of this Agreement, surrendered and transferred to the Company, and all royalties, compensation or retribution payable for such inventions, processes or discoveries belonging and being payable to the Company;

c) Never to disclose or reveal the affairs, inventions, techniques, drawing or processes of the Company or one of its subsidiaries or any other business associated with the Company, or any secrets of the Company or one of its subsidiaries or any other business associated with the Company, if such exists, nor to use, for his own purposes or for purposes other than those of the Company or to the detriment of the Company, any information, inventions, techniques, drawings or processes related to the affairs of the Company or one of its subsidiaries or any other business associated with the Company, if such exists;

d) To respect the confidentiality of any information disclosed by the Company with respect to products, projects, plans or business opportunities, or relative to the finances, research, development, know-how or personnel of the Company, as well as confidential information disclosed by a third party to the Company and information relative to other products, strategies and secrets ("Confidential Information");

Initials _____

e) To maintain the secrecy of the Confidential Information and prevent unauthorized publishing or broadcasting of same. It is however understood that this Agreement does not in any way require the Employee to maintain the secrecy of confidential information 1) that is publicly known or that becomes so through no fault of his, 2) that he himself or an affiliate is aware of before obtaining it from the Company, 3) that he himself or an affiliate may obtain independently of the Company, 4) that he himself or an affiliate legitimately obtains from a third party, 5) that is disclosed by court order or other legal obligation;

f) Not to manufacture, for his own account or that of a third party, parts or components that deal with the Confidential Information, unless he has received written authorization from the Company to do so. The Employee also agrees not to use the Confidential Information for purposes other than the possibility of entering into business relations with the Company.

The Employee acknowledges that the preceding clauses are perfectly reasonable given the Company's specific situation. However, should a court decide that a subsection or part of a subsection is unreasonable, given the specific circumstances, it is agreed that the court shall reduce the scope of such part of the subsection to render it reasonable.

It is agreed that all Confidential Information shall remain the property of the Company and no other right or authorization regarding such Confidential Information shall be granted under the terms and conditions of this Agreement. The Employee also agrees to return to the Company, upon its written request, any confidential information of which he disposes, including, but not limited to, all computer programs, documents, notes, plans, drawings and related copies.

The Employee acknowledges, by virtue of this Agreement, that any unauthorized disclosure or use of the Confidential Information could cause the Company major, even irreparable, harm that might be difficult to assess precisely. As a result, the Employee acknowledges that the Company has the right to request and take out, without delay, an injunction in the event the terms and conditions of this Agreement are not observed, and to exercise any other right or recourse it may have at its disposal.

SIGNED in _____, on this _____ day of the month of _____, 20__.

Signature: _____

New Hire Video Acknowledgement

I verify that I have watched Riggs Distler's new hire videos, have asked questions about any piece of information I do not understand, and have had those questions answered to my satisfaction.

I have watched:

_____ The human resources video

_____ The general safety video

_____ The video for my specific discipline

Circle one: Overhead Lines Underground Lines Mechanical Electrical

In addition, I understand that some information in the video has changed. In particular, I understand:

_____ I will be informed if the host utility for my project does not require insulated buckets to be grounded

_____ Because of a change to OSHA language effective July 10, 2014, employees working on or near energized electrical equipment must wear work boots with an electrical hazard rating

_____ Because of a change to OSHA language effective April 15, 2015, the height at which fall protection is required during construction work has changed from six feet to four feet

_____
Print name

_____
Signature

_____
Date