Confidentiality Policy

Maintaining the confidentiality of ***confidential information*** of ***Encana*** Corporation and/or its ***subsidiaries*** (collectively, “Encana”) is essential for competitive, security and other business reasons, as well as to comply with applicable laws. Care must be taken to ensure that confidential information is provided only to Encana ***employees***, ***contractors*** or directors that require access to it to further business purposes of Encana and only on the basis that recipients maintain the confidentiality of such information.

This Confidentiality Policy is designed to protect confidential information and to assist employees, contractors and directors in complying with their confidentiality obligations.

Restrictions on Access

Access to confidential information shall be limited to individuals who have a “need to know” such information and such persons will be advised that the information is to be kept confidential. Such information shall not be discussed with any person who does not need to know such information for purposes of conducting Encana’s business. Family members and friends are among the persons with whom confidential information shall not be discussed.

Employees, contractors and directors shall use reasonable precautions to restrict access to confidential information in accordance with this Policy and applicable laws. Employees, contractors and directors must also consult the Information Management Policy, the Acceptable Use of Information Systems Practice, Information Security Classification Practice, Information Security Practice and the Information Security website for further guidance related to the classification, handling and use of ***corporate information***.

The following general precautions shall be observed, where practicable, by employees, contractors and directors who are in receipt of confidential information:

- documents and files containing confidential information should be kept in a secure place to which access is restricted to individuals who “need to know” that information in the necessary course of business. Project code names should be used if necessary.
- documents and files containing confidential information should be identified as such.
- confidential information should not be discussed in places where the discussion may be overheard or in areas that are not secured, such as elevators, hallways, restaurants, airplanes, taxis, online discussion forums or internet chat rooms.
- confidential information should not be discussed on wireless or cordless telephones or other wireless devices. Confidential information should not be read or displayed in public places and should not be discarded where others can retrieve it.
- employees, contractors and directors must ensure they maintain the confidentiality of confidential information in their possession both inside and outside the office.

- unnecessary copying of confidential information should be avoided and documents containing confidential information should be promptly removed from the conference rooms and work areas after meetings have concluded. Extra copies of confidential information should be shredded or otherwise destroyed.
- access to confidential information in electronic format should be restricted through the use of passwords and secure/specially created storage areas on Encana's computer system.

Restrictions on Transmission

Employees, contractors and directors privy to confidential information are prohibited from communicating such information to anyone else, unless it is necessary to do so in the course of business. Efforts will be made to limit access to such confidential information to only those who "need to know" the information and such persons will be advised that the information is to be kept confidential.

Encana may also require such persons to confirm their commitment to non-disclosure of such confidential information in the form of a written confidentiality agreement or written acknowledgement.

Transmission of documents by electronic means should be made only where it is reasonable to believe that the transmission can be made and received under secure conditions. Communication by email leaves a physical track of its passage that may be subject to later decryption attempts.

Confidential information being transmitted over the internet should be secured by encryption and validation where possible.

Violations of the Confidentiality Policy

Violations of this Policy or relevant laws may result in disciplinary action up to and including termination of employment or contract, as applicable. Encana may refer violations of this Policy or relevant laws to the appropriate regulatory authorities.

The confidentiality obligations set out in this Policy remain in effect beyond termination of employment, service agreements or Board of Directors' appointments with Encana.

Actions that violate or appear to violate this Policy must be reported in accordance with the Investigations Practice.

Further Information

Employees, contractors and directors should refer to the Disclosure Policy for information on the treatment and disclosure of ***material information***.

Employees, contractors and directors should also refer to the Securities Trading and Insider Reporting Policy for information on ***securities*** trading, trading prohibitions on Encana's securities or securities of any publicly-traded party (where the context demands) while in possession of ***undisclosed material information***, and applicable blackout periods.

Employees, contractors and directors who are unsure whether they possess confidential information should not disseminate such information to anyone outside Encana until consulting with the Corporate Secretary (or their delegate).

Any other questions regarding this Policy should also be directed to the Corporate Secretary (or their delegate).

Effective: March 27, 2013

**Terms bolded and italicized in a policy or practice are defined in the Policies & Practices Glossary and such definitions are incorporated by reference into such policy or practice to the extent used therein.*