


Title:	Information Security Policy			
Type:	Corporate Policy	Version:	10/1/2024 (v.4)	
Function:	General	Last Reviewed:	10/1/2024	
Dissemination:	Internal only	Original Issuance:	7/18/2018 (v.1)	
Owner:	General Counsel			

1. PURPOSE

To provide a framework for securing Company data and maintaining Company Records, including but not limited to, the creation, retention, and disposition of Records; the protection of Confidential Information; and the identification, definition, and classification of certain data maintained, in any format, by Expand Energy Corporation and its subsidiaries and affiliates (the “Company”). Records are defined as, and include, all forms of recorded information (hard copy and digital) created or received during the course of Company business or the execution of job duties.

2. SCOPE

This policy applies to all Company data containing Confidential Information as defined herein and the Company employees and contractors (“Company personnel”) who access the data.

3. POLICY

3.1 Confidential Information

Company personnel may have access to Confidential Information concerning the Company or a third party. Confidential Information, as used in this policy, is generally described as information or its activities that is non-public, regardless of format. All personnel must conduct their business and personal activities in a way that does not compromise Confidential Information of the Company, its business partners, or potential business partner, or its employees.

Information is not considered confidential if it is disclosed through a designated employee, an officer, or a director; it is received from a third party, and not subject to a legal obligation of confidentiality or non-disclosure; or it is readily available to the public at large. All other records considered Confidential Information.

3.1.1 Third-Party Confidential Information

When the Company has the right to use or access proprietary or Confidential Information belonging to third parties, we must comply with any applicable confidentiality and non-disclosure agreements, unless otherwise prohibited by law. Competitors may not be asked to reveal proprietary or Confidential Information. Likewise, Company personnel should never divulge proprietary or Confidential Information about third parties or from their former employers to the Company. The records we maintain on our business partners may only be used for Company business purposes and may only be released with appropriate authorization from the third party and be accompanied by a legitimate business purpose.

Company Personnel are not allowed to obtain or attempt to obtain competitive or Confidential Information belonging to a competitor or business partner through improper means. Personnel are strictly prohibited from obtaining competitor information under false pretenses or engaging in any form of theft, illegal entry, black market purchases, blackmail, electronic eavesdropping, threats, and other improper methods of

This document is uncontrolled when downloaded or printed.
Users must verify this document against the latest controlled version available.

collecting information. If you suspect that information about a competitor or business partner has been obtained improperly or received in error, you must not use this information and must report it to the Legal Department.

3.2 Protecting Confidential Information

All Personnel must actively protect Confidential Information from improper or inadvertent disclosure. If a third-party Company questions you about Confidential Information or requests Confidential Information that you are not authorized to distribute, immediately refer the request to your supervisor or contact the Legal Department. Confidential Information is requested by someone inside the Company and you are concerned about the appropriateness of the information request or are unauthorized to share the requested information, immediately refer the request to your supervisor or contact the Legal Department.

3.3 Disclosing Confidential Information

As a matter of course, and with appropriate approval and confidentiality protections, such as a non-disclosure agreement, the Company's Confidential Information may be disclosed to third-party business partners, suppliers, and other third parties on a need-to-know basis in the furtherance of the Company's business strategies and objectives.

Non-routine requests to disclose Confidential Information to a third party must be submitted to the VP of the requesting employee and the Legal Department. Non-routine requests are defined as disclosures of information that do not directly support the Company's business strategies or are not subject to a non-disclosure or confidentiality agreement as a matter of due course. Non-routine disclosures of Confidential Information may only occur if:

- i) the applicable VP has pre-approved the disclosure; and
- ii) the Legal Department has approved the disclosure and ensured that a Non-Disclosure Agreement or other protective measure has been executed by the Company and any applicable third parties.

Confidential Information may be disclosed as required by a court order or during litigation, but only at the direction of the Legal Department (except as set forth below). To the extent possible, Confidential Information should only be disclosed under a protective order.

Notwithstanding the above, Company personnel may disclose Confidential Information in confidence, either directly or indirectly, to a federal, state, or local government official, or to an attorney, solely for the purpose of reporting or investigating a suspected violation of law, or in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal. Additionally, personnel who file retaliation lawsuits for reporting a suspected violation of law may disclose related Confidential Information to their attorney and use them in related court proceedings as long as the individual files documents containing the Confidential Information under seal and does not otherwise disclose the Confidential Information except pursuant to a court order.

Similarly, nothing in this policy prohibits any individual from reporting possible violations of federal law or regulation to any governmental agency or entity, including but not limited to the Department of Justice, the Securities and Exchange Commission, Congress, and any agency Inspector General, or making other disclosures that are protected under the whistleblower provisions of federal or state law or regulation. It

This document is uncontrolled when downloaded or printed.
Users must verify this document against the latest controlled version available.

is unnecessary to obtain the Company's prior authorization when making any such reports or disclosures, and an individual is not required to notify the Company of any such reports or disclosures.

3.3.1 Reporting Disclosure of Confidential Information

If you accidentally disclose or distribute Confidential Information, you are required to notify your supervisor and contact the Legal Department immediately.

3.4 Data Classification

The Company maintains two levels of data classification: (1) Confidential or Internal; (2) Non-confidential or Public. Information is considered Non-confidential or Public if it is disclosed by the Company through a designated employee, an officer, or a director; received from a third party and not subject to a legal obligation of confidentiality or non-disclosure; or readily available to the public at large. All other records are considered Confidential Information or Internal. Marking documents as Confidential or Internal is not required, as documents should be assumed confidential until determined otherwise. The Company provides marking capabilities to facilitate visual awareness that data is confidential or public. Company Personnel, however, are responsible for knowing data confidentiality regardless of marking.

3.4.1 Personally Identifiable Information ("PII")

Where the Company is in possession of PII, special consideration must be used in how this documentation is stored, accessed, and used. Only Company personnel with an explicit need-to-know reason should have access to PII. The strictest approach must be used when handling PII to ensure protection of the data. PII includes non-public information that can be used, either alone or in combination with other PII, to uniquely identify an individual. Examples include, but are not limited to, social security numbers, credit card numbers, banking information, driver's license numbers, and medical or health information.

3.4.2 Data Owners

The Company will identify Data Owners in appropriate functional areas. Data Owners are leaders within the business who are accountable for and understand the key business processes impacting their data family. Data Owners must:

- establish, monitor and update classification levels of their data;
- work with IT and Corporate Security to establish, monitor and update data protection requirements;
- manage access control; and
- promote data resource management for the good of the Company.

3.5 Minimum Protection Standards

All Confidential Information, regardless of format, must be identified, categorized, and secured according to the associated [Minimum Protection Standard](#).

This document is uncontrolled when downloaded or printed.
Users must verify this document against the latest controlled version available.

3.6 Record Retention

The Company owns all Records created, received, or used in the course of conducting business, regardless of location or form. Company personnel must retain Records in accordance [Records Retention Schedule](#). The Schedule sets forth requirements that meet at least minimum legal or regulatory compliance obligations.

3.7 Legal Hold

The Records Retention Schedule may be suspended during certain circumstances including litigation, regulatory inspections, government investigations, audits, or other actions that require the preservation of Records otherwise eligible for disposition. A legal hold supersedes the scheduled retention and destruction of Records. Employees must abide by and follow all applicable legal holds. The authority to issue or release legal holds is granted by the General Counsel.

3.7 Cybersecurity

Cyber incidents identified through the Company's monitoring process are properly logged, investigated, and responded to accordingly. Cyber incidents are to be assigned a tier based on an evaluation of the materiality of the loss. The Company maintains a [Cybersecurity Material Incident Assessment Procedure](#) for evaluating incidents to determine if they should be disclosed. Cyber incidents that result in a significant loss to the Company are presented to the Cyber disclosure committee. The Cyber disclosure committee will evaluate the loss and determine if a formal SEC disclosure or an insider trading blackout period is required.

3.7.1 Annual Cyber Risk Assessment

The Company will perform an annual risk assessment over the Cybersecurity function. This assessment may be performed by either an internal or external party for any area within the Cybersecurity function. Management will evaluate the results of the risk assessment, determine issues that need to be addressed, and create or revise policies or procedures to formally respond.

3.8 Policy Violations

Failure to comply with this policy can damage the Company's reputation and expose the Company to legal penalties. Violations may also lead to criminal and civil charges being filed against violating employees. In addition to the penalties that may be imposed by law, any employee who violates this policy, orders another to violate this policy, or knowingly permits a subordinate to violate this policy will be subject to disciplinary action, up to and including termination.

If you are aware of any violations or potential violations of this policy, you must report all information concerning the violation using one of the following methods:

- speaking with your supervisor or manager;
- consulting the [Legal Department](#);

This document is uncontrolled when downloaded or printed.
Users must verify this document against the latest controlled version available.

- consulting the Compliance Department; or
- file a report using the Company's Ethics and Integrity Helpline by calling 866-291-3401,

3.9 Additional Guidance

The following examples illustrate steps that all employees must take to guard against improper disclosure of Confidential Information. All Company Personnel must:

- conduct Company business in a manner that does not compromise the confidentiality of Company Confidential Information;
- keep electronic and paper documents and files containing Confidential Information in a secure location, or a location that meets the minimum protection standards associated with each classification level;
- exercise caution when discussing confidential business matters;
- use passwords, when appropriate, to restrict access to electronic devices or files containing Confidential Information;
- lock computers when away or when not in use;
- avoid leaving computers or other electronic devices in unsecured locations;
- transmit documents containing Confidential Information by electronic devices, such as by fax or e-mail, only when it is reasonable to believe this can be done under secure conditions;
- avoid unnecessary copying of documents containing Confidential Information;
- return any of the Company's Confidential Information created or moved outside of the Company's possession, custody or control;
- upon request, destroy or return any of the Company's Confidential Information that has been copied, printed or otherwise obtained from a Company IT resource or physical location;
- provide any Confidential Information to other employees on a strictly need-to-know basis;
- refrain from discussing or communicating any Confidential Information with anyone, including fellow employees, if they do not have a legitimate business need to know the information;
- to the extent possible, use programs that create audit trails that record who accessed information, at what times information was accessed, and for how long; and
- designate information as "Confidential" when communicating externally. Standard language can be used. Please contact the Legal Department if you need assistance.

If you have questions about the interpretation of this policy, contact the Legal Department.

4. DEFINITIONS

- **Confidential Information**, as used in the Policy, includes, but is not limited to, any of the following:
 - all trade secrets;
 - all proprietary information, defined as any valuable commercial information that is not public knowledge, developed or used by the Company to further its business strategies;
 - all non-public information about the Company's business partners;
 - all non-public classified data as defined in section 3.4;
 - customer contacts;

This document is uncontrolled when downloaded or printed.
Users must verify this document against the latest controlled version available.

- any information provided to the Company by a third party under restrictions against disclosure, including but not limited to proprietary information belonging to a third party, intellectual property, such as trade secrets, reports, know-how, inventions, discoveries, improvements, ideas, computer programs, patents, copyrights, trademarks, leases, and related documentation belonging to a third party;
- any other information subject to a confidentiality or non-disclosure agreement between The Company and a third party;
- all employee or third-party information that is maintained as confidential by the Company (such as social security numbers, tax identification numbers, protected health information, or bank account information) and of which an employee, temporary worker, contractor or subcontractor has been given special custody to use in the performance of job duties; and
- all non-public financial information, including non-public information regarding corporate expenditures, future business performance, business plans, lease bonuses, well results, leasing activities, acquisition targets or geological prospects; and statements about an upcoming quarter, future periods, or information about business partners including conversations with analysts, press, or other third parties.

5. RELATED DOCUMENTS

[Cybersecurity Material Incident Assessment Procedure](#)

[Insider Trading Policy](#)

[IT Acceptable Use Policy](#)

[Minimum Protection Standard](#)

[Protection of Expand Energy Assets Policy](#)

[Record Retention Schedule](#)

[Social Media and External Communications Policy](#)

This document is uncontrolled when downloaded or printed.
Users must verify this document against the latest controlled version available.