


Title:	<b>Information Security Policy</b>			
Type:	Corporate Policy	Version:	7/18/2018 (v.1)	
Function:	General	Last Reviewed:	7/18/2018	
Dissemination:	Internal only	Original Issuance:	7/18/2018 (v.1)	
Owner:	General Counsel			
				<b>LGL-22</b>

**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 Chesapeake Energy Corporation and its subsidiaries and affiliates (“Chesapeake” or the “Company”).

**Table of Contents**

1. PURPOSE..... 1

2. SCOPE ..... 2

3. POLICY ..... 2

    3.1 Confidential Information ..... 2

        3.1.1 Third-Party Confidential Information ..... 3

    3.2 Data Classification ..... 3

        3.2.1 Minimum Protection Standards ..... 4

        3.2.2 Data Classification Roles and Responsibilities ..... 4

        A. Data Owners ..... 4

        B. Information Security..... 5

        C. Corporate Security ..... 5

        D. Data Consumers ..... 5

        E. Data Producers ..... 5

    3.3 Protecting Confidential Information..... 5

        3.3.1 Requests to Disclose Confidential Information ..... 6

        3.3.2 Reporting Disclosure of Confidential Information..... 7

    3.4 Record Retention ..... 7

        3.4.1 Ownership of Company Records ..... 7

        3.4.2 Management of Company Records..... 7

        3.4.3 Records Retention Schedule ..... 7

        3.4.4 Legal Hold ..... 8

        3.4.5 Disposition of Records..... 8

    3.5 Disclosure of Cyber Incidents ..... 8

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

3.5.1 Cyber Incident Monitoring Process..... 8

3.6 Annual Cyber Risk Assessment..... 8

3.7 Policy Exceptions ..... 9

3.8 Policy Violations ..... 9

3.9 Additional Guidance ..... 9

4. RELATED DOCUMENTS ..... 9

**2. SCOPE**

This policy applies to:

- all employees, temporary workers, contractors;
- all Company Records as defined by section 3.3 of this policy; and
- all Company data listed in the [Data in Scope Document](#) located on the Data Classification information web page.

**3. POLICY**

**3.1 Confidential Information**

During the course of job duties, Chesapeake employees, temporary workers, contractors and subcontractors may have access to Confidential Information concerning Chesapeake and third parties. Confidential Information is generally described as non-public information, regardless of format. All employees, temporary workers, contractors and subcontractors must conduct their business and personal activities in a way that does not compromise Confidential Information of Chesapeake or its business partners or employees.

Confidential Information can include, but is not limited to any of the following:

- trade secrets;
- proprietary information, defined as any valuable commercial information that is not public knowledge, developed or used by the Company to further its business strategies;
- non-public information about the Company’s business partners;
- all levels of non-public classified data as defined in section 3.2;
- customer contacts;
- 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;
- other information subject to a confidentiality or non-disclosure agreement between Chesapeake and a third party;

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

- 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
- 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.

Information is not considered confidential if it is officially 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.

### 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 comply with any applicable confidentiality and non-disclosure agreements, unless otherwise prohibited by law. Employees of competitors may not be asked to reveal proprietary or Confidential Information. Likewise, our employees, temporary workers, contractors or subcontractors should never divulge proprietary or Confidential Information about third parties or from their former employers to the Company. The Records we maintain on our customers and suppliers may only be used for Chesapeake business purposes and may only be released with proper authorization and a legitimate business purpose.

Employees, temporary workers, contractors and subcontractors are not allowed to obtain or attempt to obtain competitive or Confidential Information belonging to a competitor or business partner through improper means. Employees, temporary workers, contractors and subcontractors 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 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 at [Legal@chk.com](mailto:Legal@chk.com).

## 3.2 Data Classification

To further protect, control and secure its information, Chesapeake uses a data classification scheme to assign varying confidentiality levels to certain types of confidential data. According to the Company's data classification scheme, data listed in the [Data in Scope Document](#) must be classified as either Restricted, Sensitive, or Internal as it is created, amended, enhanced, stored, processed or transmitted. The classification level is an indication of value, confidentiality, or importance of the data to the enterprise. Chesapeake uses the following four classifications of data.

### **RESTRICTED:**

Data should be classified as Restricted if it is highly confidential and/or proprietary to Chesapeake or its business partners and is only known by a discrete set of individual employees, each with an explicit need-to-know requisite. The unauthorized public or internal disclosure of such data could have a severe or catastrophic adverse effect on company operations, company assets or individuals.

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

**SENSITIVE:**

Non-Restricted data should be classified as Sensitive if the information is accessible to predefined groups of employees but not freely shared publicly or across and among all business units and departments within the company.

**INTERNAL:**

Non-Restricted, Non-Sensitive data that can freely flow across the company should be classified as Internal. It may be generally used or accessed by any employee, designated temporary worker, contractor or third party with a legitimate Chesapeake business purpose. By default, all Company data that is not explicitly classified as Restricted, Sensitive or Public should be treated as Internal.

**PUBLIC:**

Data should be classified as Public if it is officially disclosed by the Company, a director, officer or designated employee.

**3.2.1 Minimum Protection Standards**

The [Minimum Protection Standards](#) specify the level of security protection that is required for each data classification scheme. These standards provide the minimum requirements for handling and storing physical Records and the minimum security standards required for the storage of and access to electronic data.

**3.2.2 Data Classification Roles and Responsibilities**

Data security measures must be implemented commensurate with the classification of the data and the risk to Chesapeake if the data is compromised. No employee, temporary worker, contractor or third party may take actions to circumvent data classification or data security controls. Employees, temporary workers, contractors and subcontractors performing key data classification roles must comply with their responsibilities and duties. A detailed explanation of the key data classification roles and responsibilities is below.

**A. Data Owners**

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 Data Strategy and Governance, IT Security and Corporate Security to establish, monitor and update data protection requirements;
- manage access control;
- require and facilitate proper training of Data Producers and Data Consumers; and
- promote data resource management for the good of the Company.

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

The Company will identify Data Owners in appropriate functional areas.

### **B. Information Security**

Information Security is responsible for working with all roles defined in this policy to identify and implement technical controls for protecting data appropriately and within reasonable costs to the Company based on the data's classification level. Each data classification level will have a defined minimum protection standard that must be met.

### **C. Corporate Security**

Corporate Security is responsible for working with all roles defined in this policy to identify and implement physical controls for protecting data appropriately and within reasonable costs to the Company based on the data's classification level. Each data classification level will have a defined minimum protection standard that must be met.

### **D. Data Consumers**

Data Consumers are individuals who use Company data to report or analyze as part of their daily job. Data Consumers who are given access to Restricted, Sensitive, or Internal data have a position of special trust and are responsible for protecting the security and integrity of that data.

### **E. Data Producers**

Data Producers are the Company's employees, temporary workers, contractors and third parties who generate data in any format. Data Producers may generate data directly or indirectly through the use of applications or systems that generate or compile data from other sources. Data Producers have the same responsibilities as Data Consumers, as well as the responsibility of working with IT & Corporate Security to make sure they are aware of the data being produced so that it can be classified and handled appropriately.

## **3.3 Protecting Confidential Information**

Company data listed in the [Data in Scope Document](#), regardless of format, must be identified, categorized, and secured according to the associated [Minimum Protection Standards](#). Additionally, every employee must actively protect all Confidential Information, regardless of whether or not it is classified under the Company's Data Classification Scheme or listed in the [Data in Scope Document](#). The following examples illustrate steps that all employees must take to guard against improper disclosure. All employees 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;
- not discuss Confidential Information in public places where it could be overheard, such as elevators, hallways, restaurants, airplanes, and taxis;

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

- exercise caution when discussing confidential business matters on wireless telephones or other wireless devices;
- 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 Confidential Information to other employees on a strictly need-to-know basis;
- refrain from discussing or communicating 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;
- mark applicable documents as directed by the [Marking Classified Documents Procedure](#); and
- designate information as "Confidential" when communicating externally. Standard language can be used. Please contact the Legal Department if you need assistance at [Legal@chk.com](mailto:Legal@chk.com).

If an external third party outside of the 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 at [Legal@chk.com](mailto:Legal@chk.com).

If 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 at [Legal@chk.com](mailto:Legal@chk.com).

### 3.3.1 Requests to Disclose Confidential Information

As a matter of course, and with appropriate approval and confidentiality protections, 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 Chesapeake's business strategies and objectives. Non-routine requests to disclose confidential and/or classified data to a third party must be submitted to the EVP of the requesting employee and [Legal@chk.com](mailto:Legal@chk.com). Non-routine requests are defined as disclosures of information that do not directly support Chesapeake's business strategies and/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 EVP 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.

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

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, employees may disclose trade secrets 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, employees who file retaliation lawsuits for reporting a suspected violation of law may disclose related trade secrets to their attorney and use them in related court proceedings as long as the individual files documents containing the trade secrets under seal and does not otherwise disclose the trade secrets 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 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.

### **3.3.2 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 at [Legal@chk.com](mailto:Legal@chk.com).

## **3.4 Record Retention**

Chesapeake and its employees must retain Records in accordance with all applicable recordkeeping requirements and compliance obligations, to include legal, regulatory, or operational reasons. Records are defined as, and include, all forms of recorded information (hard copy and electronic) created or received during the course of Company business or the execution of job duties. Information created or received by the Company's IT systems are also considered Company Records. The Company's [Records Retention Schedule](#) identifies Record classes and states how long each class should be retained. All Company Records must be managed in accordance with the [Records Retention Schedule](#).

### **3.4.1 Ownership of Company Records**

Chesapeake owns all Records created, received and/or used in the course of conducting business, regardless of location or form.

### **3.4.2 Management of Company Records**

It is the responsibility of each department to manage Company Records. Departments shall maintain and dispose of all Company Records in accordance with the [Records Retention Schedule](#).

### **3.4.3 Records Retention Schedule**

The [Records Retention Schedule](#) identifies record classifications and states how long each class should be retained. All Company Records created or received by employees or contractors in the course of business must be managed in accordance with the [Records Retention Schedule](#).

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

### 3.4.4 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.

### 3.4.5 Disposition of Records

Disposition is the process of taking a final action with regard to Records, which in most cases means destruction. However, in some cases, it can also mean permanent preservation for historical purposes or transfer to another organization, as in the case of a divestiture.

Records that are beyond the [Records Retention Schedule](#) requirements and are not subject to any legal holds must be destroyed.

Duplicates or draft documents must not be retained longer than original Records. When official Records are beyond the retention period and not subject to legal hold, all copies in the possession of employees in all media and formats must also be destroyed. This includes, but is not limited to photocopies, microfilm copies, and electronic files stored on removable media, hard disks, file servers, magnetic tape, or other storage devices, subject to the limitations of specific software applications.

Destruction of Records still within the retention period is expressly prohibited.

## 3.5 Disclosure of Cyber Incidents

Known incidents that are perpetrated by an insider (i.e., perpetrated by either an employee, temporary worker or a contractor) or an external party (i.e., perpetrated by an entity outside of the Company) are logged, reviewed, and responded to accordingly. The Company has designed a process for evaluating incidents to determine if they should be disclosed.

### 3.5.1 Cyber Incident Monitoring Process

Cyber incidents identified through the Company's monitoring process are properly logged and investigated. Cyber incidents are assigned a tier based on an evaluation of the materiality of the loss. 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 and/or an insider trading blackout period is required.

## 3.6 Annual Cyber Risk Assessment

In addition to Enterprise Risk Management activities, the Company will perform an annual risk assessment over the Cyber Function, which is comprised of Information Security and Forensic Services. This assessment will be performed by either an internal or external party for any area within the Cyber Function. Management will evaluate the results of the risk assessment, determine issues that need to be addressed, and create or revise policies and/or procedures to formally respond.

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



### 3.7 Policy Exceptions

Requests for exceptions to this policy must be submitted, in writing, to the Company's General Counsel at [Legal@chk.com](mailto:Legal@chk.com) and [DataGovernance@chk.com](mailto:DataGovernance@chk.com). Exceptions to the classification of data outlined by this policy may only be granted in cases where risk is mitigated by other factors. Examples of these factors can include, but are not limited to:

- where security risks are low and can be documented as such; or
- where adherence with the minimum protection standards would interfere with legitimate business needs.

The General Counsel and the Chief Digital Officer or their appointed designees will review exceptions annually to ensure ongoing legitimacy for any policy exception.

### 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 at [Legal@chk.com](mailto:Legal@chk.com);
- consulting the Compliance Department at [Compliance@chk.com](mailto:Compliance@chk.com);
- file a report using the Chesapeake Ethics and Integrity Helpline by calling 877-245-8007 or visiting [chkethics.com](http://chkethics.com); or
- register your concern by contacting our Board of Directors via the Director Access Line (866-291-3401) or by written communication as described on [chk.com/about/governance/pages/contact.aspx](http://chk.com/about/governance/pages/contact.aspx).

### 3.9 Additional Guidance

If you have questions about the interpretation of this policy, contact the Legal Department at [Legal@chk.com](mailto:Legal@chk.com). Questions on Data Classification may be directed to [DataGovernance@chk.com](mailto:DataGovernance@chk.com).

## 4. RELATED DOCUMENTS

[Protection of Chesapeake Assets Policy](#)

[IT Acceptable Use Policy](#)

[Social Media and External Communications Policy](#)

[Insider Trading Policy](#)

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

[Minimum Protection Standards](#)

[Marking Classified Documents Procedure](#)

[Data in Scope Document](#)

[Record Retention Schedule](#)

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