BRITISH COLUMBIA **ENERGY REGULATOR**

Security Management Regulation Guideline

DRAFT - Version 1.0
August 2023

About the BC Energy Regulator

The BC Energy Regulator (BCER, formerly the BC Oil & Gas Commission) is the single-window regulatory agency with responsibilities for regulating energy resource activities in British Columbia, including:

- oil and gas exploration, development, pipeline transportation, and reclamation
- geothermal projects
- carbon capture and storage
- hydrogen methanol and ammonia production

The BCER's core roles include reviewing and assessing applications for industry activity, consulting with Indigenous nations, ensuring industry complies with provincial legislation and cooperating with partner agencies. The public interest is protected by ensuring public safety, protecting the environment, conserving petroleum resources and ensuring equitable participation in production.

Vision

Safe and responsible energy resource development for British Columbia.

Mission

We provide British Columbia with regulatory excellence in responsible energy resource development by:

- Protecting public safety,
- Safeguarding the environment, and
- Respecting those individuals and communities who are affected.

Values

- Transparency
  Is our commitment to be open and provide clear information on decisions, operations and actions.
- Innovation
  Is our commitment to learn, adapt, act and grow.
- Integrity
  Is our commitment to the principles of fairness, trust and accountability.
- Respect
  Is our commitment to listen, accept and value diverse perspectives.
- Responsiveness
  Is our commitment to listening and timely and meaningful action.

Preface

1.1. About This Guideline

The Security Management Regulation Guideline (the guideline) is intended to provide guidance on the BC Energy Regulator's expectations and requirements for complying with the BC Security Management Regulation. Effective June 1, 2023, the BC Security Management Regulation and the incorporated CSA Standard, Z246.1 is applicable to all permit holders under the Energy Resource Activities Act (ERAA, formerly the Oil and Gas Activities Act[1]). The guideline includes additional insight for permit holders on how to meet the requirements of the Security Management Regulation:

- Preparing and maintaining a Security Management Program
- Security incident reporting and evaluations
- Submission requirements
- Reports and record keeping requirements

1.2. Guideline Scope

The guideline is limited in scope to the BC Energy Regulator's authorities and requirements established within the Energy Resource Activities Act. Permit holders may be subject to requirements from other regulators or have obligations under other statutes, it is the permit holder's responsibility to know and uphold all their legal obligations.

1.3. Compliance and Enforcement

This document does not replace legislation or affect legislative requirements. All permit holders are ultimately responsible for ensuring they understand and meet all requirements of ERAA and their permits. If a person does not comply with ERAA, the BC Energy Regulator may take compliance and enforcement actions.

For more information regarding the BCER's Compliance and Enforcement processes, please refer to the Compliance and Enforcement Manual.

Throughout the guideline there are references to guides, forms, tables, and definitions to assist in creating and submitting all required information.

1.4. Additional Resources

Additional resources on the BC Energy Regulator's website include:

- Glossary and acronym listing
- Documentation and guidelines
- Frequently asked questions
- Advisories, Technical Updates, reports and directives
- Regulations and Acts

[1]This guideline refers to ERAA and "energy resource" activities in anticipation of the pending amendments detailed in Bill 37-2022. At the time of writing, the changes have not yet been brought into force by regulation.

Table of Contents

Guideline Revisions

The BCER is committed to the continuous improvement of its documentation. Revisions to the documentation are highlighted in this section and are posted to the Documentation Section of the BCER's website. Stakeholders are invited to provide input or feedback on BCER documentation to by using the contact form.

Version Number	Posted Date	Effective Date	Chapter Section	Summary of Revision(s)
DRAFT - 1.0	August 23, 2023	August 23, 2023	All	This is a new document. Users are encouraged to review in full.

1. Introduction

All permit holders carrying out energy resource activities as defined in the Energy Resource Activities Act are subject to the Security Management Regulation and are required to have a Security Management Program (SMP). This includes permitted activities under the following regulations:

- Drilling and Production Regulation
- Pipeline Regulation
- Liquefied Natural Gas Facility Regulation
- Oil and Gas Processing Facility Regulation

The objective of the Security Management Regulation (the Regulation) is to ensure that permit holders have appropriate measures in place to identify and minimize the security risks (both physical and cyber) to infrastructure which could jeopardize the province's safe, secure, and reliable energy supply. The Regulation, which incorporates the CSA Standard *CSA Z246.1* Security Management for Petroleum and Natural Gas Industry Systems (the Standard), provides a risk-based framework for companies to evaluate and respond appropriately to security threats for the protection of public safety, the environment, and critical energy infrastructure.

The requirements for SMPs are outlined in the standard and follow a management system-based approach. SMPs must be documented and must include policies, processes, and procedures to:

- Define roles, responsibilities and accountability for implementation and maintenance of the SMP.
- Proactively identify security threats to operations and ensure that associated risks are appropriately mitigated so that impacts to people, the environment, assets, and economic stability are minimized.
- Ensure personnel are trained and competent.
- Manage documentation, reporting, evaluation and continual improvement.

The purpose of this document is to provide permit holders with guidance for compliance with the Regulation. The Regulation applies to all permit holders carrying out energy resource activities including:

- Wells
- Facilities including production facilities, processing facilities, and LNG facilities
- Pipelines
- Oil and Gas roads
- Geophysical activities

The Regulation does not presently apply to a permit issued by the BCER under other Acts such as the Geothermal Resources Act.

2. Regulations, Standards and Other References

Security Management Regulation (B.C. Reg. 181/2022).

Canadian Standards Association
CSA Z246.1 Security Management for Petroleum and Natural Gas Industry Systems

National Institute of Standards and Technology
Framework for Improving Critical Infrastructure Cybersecurity
Cybersecurity Framework

Energy Resource Activities Act (repealed and substituted the Oil and Gas Activities Act under Bill 37 -2022)

The Security Management Regulation is applicable to all Energy Resource Activities under the Energy Resource Activities Act, including permits issued under the following regulations:

Drilling and Production Regulation (B.C. Reg. 282/2010)

Pipeline Regulation (B.C. Reg. 281/2010)

Liquefied Natural Gas Facility Regulation (B.C. Reg. 146/2014)

Oil and Gas Processing Facility Regulation (B.C. Reg. 48/2021)

Emergency Management Regulation (B.C. Reg 217/2017)

Freedom of Information and Protection of Privacy Act (RSBC 1996, c. 165)

Public Safety Canada
Critical Infrastructure Resources

Canadian Centre for Cyber Security
Self Assessment Tools and Resources

Cybersecurity and Infrastructure Security Agency (USA)
Cyber Security Evaluation Tool

3. Terminology and Application of CSA Z246.1

Guidance documents are generally non-mandatory but often reference mandatory requirements contained within regulatory and associated standards. Within this document, “shall” and “must” express mandatory requirements such as references to requirements within the Regulation or the Standard.

The Regulation requires compliance with CSA Z246.1 with the following modifications:

- All references to “operator” or “owner” in the Standard are to be read as “permit holder”.
- All references to “should” in the Standard are to be read as “must”.

While a permit holder may contract third parties to undertake certain security management tasks on their behalf, the permit holder remains accountable for ensuring compliance with the requirements of the Regulation.

4. Security Management Program

The Regulation requires every permit holder to have a documented Security Management Program (SMP) that complies with the CSA Z246.1. An SMP follows a Plan-Do-Check-Act cycle which includes several processes to identify and manage security threats and associated risks. SMPs determine security mitigation measures and response procedures to minimize the impact of a security incident.

Permit holders must have an SMP in place for all infrastructure and assets regulated by the BCER. Aspects of an SMP may be generally applied across multiple assets where suitable while other aspects of an SMP may be site-specific.

Where a permit holder has contracted operation of some infrastructure to a third party, the permit holder must clarify who is administering and implementing the SMP. Permit holders may choose to rely on a third party's SMP; however, the permit holder maintains responsibility to ensure that an effective SMP is in place.

Permit holders must be able to:

- Identify security risks including physical and cybersecurity risks.
- Develop and implement strategies to address security risks.
- Develop and implement a security training program.
- Respond to and report security incidents.

4.1. Scalability

SMPs are intended to be scalable for permit holders and assets of varying size and scope. Effective SMPs are 'fit for purpose' to appropriately address permit holder's security risks. It is expected that permit holders will consider the scale and scope of their operations as well as potential security threats and impacts of a security incident when developing their SMP to ensure it is effective.

All permit holders must develop a documented SMP which contains all required processes and components as defined in CSA Z246.1, however the content of the SMP documentation may be appropriately scaled for the assets covered under the SMP. Similarly, any systems or processes developed for an SMP may be scaled to be suitable for the assets covered under the SMP.

While implementing an SMP, permit holders can consider the type, size, location, and criticality of an asset to evaluate security threat levels and determine appropriate security measures. Permit holders must ensure the SMP and associated security measures are effective at managing and responding to security risks.

When determining the criticality of an asset, permit holders must develop and implement a documented evaluation process which considers the impacts that loss of, or damage to the asset would create.

External impacts can include the potential for harms, such as the effects that loss of service of the asset could have on other companies or consumers.

4.2. Components

The required components of an SMP are defined in CSA Z246.1. The Standard includes requirements for the following:

- Policy, Management Commitment and Accountability
- SMP Roles and Responsibilities
- Security Risk Management Process
- Information Security Management Process
- Cybersecurity Measures and Considerations
- Personnel Security Process
- Security Training and Awareness Process
- Physical Security Measures and Considerations
- Security Incident Management Process
- SMP Monitoring, Review, and Updates

This document includes additional details on expectations pertaining to some of the required SMP components contained within CSA Z246.1, however it does not address all requirements. Permit holders are responsible to ensure their SMP meets the requirements of CSA Z246.1 and the Security Management Regulation. Any questions on the BCER's expectations and requirements may be submitted to securitymanagement@bc-er.ca.

4.3. Information Security Management

An SMP must include an information security management procedure prepared and maintained in accordance with the Standard (Clause 6, CSA Z246.1). An information security management process consists of policies and procedures for protecting information from creation to final disposition.

Examples of information which may require protection under an information security management process include:

- Personnel records
- Security sensitive information
  (site access codes, any information detrimental to the security of assets.)
- Confidential information

CSA Z246.1 Clause 6 outlines the components of an information security management process:

- A system for classifying information
- Communication procedures
- Handling and storage procedures
- Security clearance to classified information for authorized personnel
- Record retention and destruction procedures

Permit holders shall establish security measures and procedures for classifying, communicating, handling, and storing protected or sensitive information. The information security management process

requirements must address the physical handling and storing of documentation as well as the electronic storage and transmission of information.

Permit holders must develop a classification system for protected information. For example: "unclassified", "restricted", "confidential" or the "Traffic Light Protocol" (TLP) in common use within many agencies. The security measures in place for protecting classified information must be appropriate based on the sensitivity or classification level of the information. Permit holders shall consider implementing security clearance requirements to limit access and protect classified information. The record retention and destruction requirements for protected information must be defined.

Permit holders must ensure its employees who have authorized access to protected information are trained on the information security management process. The information security management process is applicable to protected information associated with permitted activities / sites (e.g. wells, pipelines, facilities), including protected information which may be stored offsite.

4.4. Cybersecurity Measures

An SMP must include cybersecurity measures prepared, implemented, and maintained in accordance with the Standard (Clause 7, CSA Z246.1). As part of the security risk management process required by the Standard (Clause 5, CSA Z246.1), permit holders must assess security threats, vulnerabilities, and risks; including cybersecurity. The Standard includes several cybersecurity risk mitigation measures which shall be considered by permit holders to address associated cybersecurity risks. Permit holders may choose whether to implement a cybersecurity measure listed in the Standard, however this decision and the associated rationale must be documented. Like other types of security measures, the evaluation of cybersecurity measures shall take into consideration the threat level and characteristics of the asset being protected.

Cybersecurity risk management, may include:

- Cybersecurity supply chain management, which includes the ability to track and confirm the authenticity of items such as essential parts, the integrity of formatted devices (such as smart switches and controllers) from manufacturer to receipt, and service companies, such as contractors and managed service providers. Counterfeit electronic equipment may contain malicious modifications which allow attackers to access the equipment or associated networks.
- Insider risks and threats. An insider is someone who currently has or previously had authorized access to security sensitive information which may be used in an attack. For example, a disgruntled employee which tries to harm their employer.

Implemented cybersecurity measure must meet the objectives of the Framework for Improving Critical Infrastructure Cybersecurity as published by the National Institute of Standards and Technology (NIST) or a comparable standard if approved by the BCER. The BCER has not identified and approved a comparable standard to date. If a permit holder has identified a comparable standard, the permit holder may submit a request to the BCER to use the standard. Requests must include an explanation of why the use of the alternative standard is appropriate and documentation which demonstrates how the alternative standard is comparable or equivalent to the NIST Framework. Such requests will be considered by the BCER.

The Framework for Improving Critical Infrastructure Cybersecurity details a "Framework Core" (see Appendix A of the document) which separates cybersecurity measures by their function: Identify, Protect, Detect, Respond, or Recover. Each cybersecurity function is further divided into Categories and Subcategories which define the outcomes and objectives of various cybersecurity measures. NIST also provides additional online resources and guides for developing and improving cybersecurity framework.

Public Safety Canada offers virtual cybersecurity self-assessment tools, which may be beneficial to permit holders who own or operate critical infrastructure. There are two tools, a basic version (CCST) and a more detailed version (CCST 2.0) which provides direct mapping to the NIST cybersecurity framework.

Protection against cybersecurity threats requires cooperation and collaboration amongst industry and regulators. Permit holders are encouraged to communicate any identified or suspected threats with the Canadian Centre for Cyber Security (Tel: 1-833-CYBER-88 email contact@cyber.gc.ca) in addition to any reporting required by BCER regulations.

4.5. Training Plan

An SMP must include a training plan prepared and maintained in accordance with the Standard (Clause 8.3, CSA Z246.1). A training plan is equivalent to a security training and awareness process as described in the Standard. Permit holders must assess which security training and awareness requirements are applicable based on the type, size, location, and criticality of an asset. Some aspects of security training and awareness may be generally applied across multiple assets while other aspects may be site-specific.

CSA Z246.1 Clause 8.3 details the following security training and awareness requirements (read as "must" as per Section 2(3) of the Regulation).

Security training and awareness must:

- Be provided to all employees and on-site personnel
- Be conducted as part of new employee orientation
- Be provided on a regular basis (at least once every 24 months)
- Include development of security messages for internal communication that will promote a security culture and support the intent of the Standard
- Incorporate the following, as applicable:
    - Operational security, including
        - Threat environment
        - Surveillance techniques
        - Identifying suspicious activities
    - Threat-level response measures and policies
    - Physical security measures, including access controls and security badges
    - Confrontation and communication training
    - Personal protection training
    - Recognition and reporting of security-related threats/incidents or information that might help detect security threats
    - Information and cybersecurity

- Include a component that tests and assesses knowledge and understanding in applying the security awareness content specific to operational requirements
- Include a relevant security stakeholder component to enhance community awareness through various communication methods
- Maintain procedures to protect the integrity of training records in accordance with the organization's record retention policy

Training Records

The Regulation requires permit holders maintain a written record of participants for training that is completed in accordance with the SMP training plan.

On completing training in accordance with the training plan, a permit holder must prepare an evaluation and improvement report that:

- States whether the training objectives were met
- Makes recommendations for improvement including improvement to the training plan, and
- Includes a strategy to implement any recommendations.

Permit holders who are developing and implementing a new SMP and security training plan must prepare the training evaluation and improvement report within an appropriate timeframe after training has been provided for all applicable employees.

Permit holders who already have an existing SMP and provide security training on a regular basis (at least once every 24 months per CSA Z246.1) must prepare an evaluation and improvement report within an appropriate timeframe after conducting the regularly scheduled training sessions.

4.6. Physical Security

Physical security includes the protection of facilities as well as key supporting resources, critical spares, and equipment caches such as those pre-positioned for spill response.

Physical security for a fixed asset shall be considered as part of the design process. Existing facilities will need to be risk assessed to identify potential vulnerabilities and any appropriate mitigation measures.

Physical security encompasses deterrence, detection, and defence, and applies to the protection of people and property through the use of mitigations that can include signage, fencing and access controls to the extent the risk assessment indicates is necessary.

4.7. Incident Management

An SMP must include a security incident management process in accordance with the Standard (Clause 10, CSA Z246.1) which specifies how a permit holder will respond to, communicate, document, recover from, and de-escalate security-related threats and incidents. Security incidents include, but are not limited to, the following:

- Theft
- Vandalism
- Unauthorized entry

- Terrorism / bomb threats
- Suspicious packages / activities
- Control systems or information technology attacks (e.g. cybersecurity / cyberattacks)
    - Including the identification of malicious modifications made to installed or purchased critical components (supply chain management)

Please refer to Section 5.2 of this document which includes details on reporting requirements for security incidents.

Security Incident Response – Evaluation Report

In the event of a security incident, a permit holder must prepare a report of the results of an evaluation to a response to a security incident. Refer to Section 5.2 for security incident reporting.

An evaluation report must be completed once an incident has concluded and is under control, it may be incorporated into an incident investigation report.

The evaluation report must include the following four items:

1. A description of the incident including the cause or suspected cause
    a. Provide location and list associated permits
    b. Identify both causes and root causes
    c. Identify the consequences of the incident
2. A description of the incident response
    a. Provide a timeline of the incident and response
    b. Details on if the emergency response plan activated
3. Measures taken to reduce the risk of similar incidents occurring
    a. Provide corrective actions to repair and damages caused by the incident
    b. Provide preventative actions which address the root cause(s) of the incident
4. An assessment of the permit holder's response
    a. May be performed internally or by a third party
    b. Questions to consider:
        i. Were the appropriate internal staff notified within expected timelines?
        ii. Were the appropriate external parties notified within expected timelines?
        iii. Was the chain of communication efficient and logged?
        iv. Did the response effectively mitigate the impacts of the incident?
        v. What could have been done better?

The security incident response evaluation report must be maintained by the permit holder until the associated permit for the energy resource activity is cancelled or declared spent by the BCER. The BCER may request a copy of the incident response evaluation report while reviewing reportable incidents.

Security Exercises and Drills

CSA Z246.1, Clause 10.3 requires permit holders to evaluate the effectiveness of the security incident response process using exercises, drills and lessons learned from actual incidents. An exercise or drill plan must be developed and implemented.

Permit holders may consider opportunities to include a security component into emergency response exercises to satisfy this requirement. Please note that the requirements for emergency management can be found within the Emergency Management Regulation.

4.8. Monitoring, Review and Update

Permit holders are required to review and periodically update their SMP. A permit holder must review and, if necessary, update their SMP:

- At least once every three (3) years.
- After a significant change occurs in the types of threats, risks or vulnerabilities associated with a permit holder's activities that are subject to the SMP, and
- Any time the permit holder becomes aware of a deficiency in the program that risks the safety of
    - the public
    - the permit holder's employees
    - permitted activities

A significant change in the types of threats, risks or vulnerabilities may include:

- A permit holder becomes aware of new information on specific security threats and vulnerabilities that are not adequately addressed by their SMP.
- A significant change occurs to a permit holder's operations. This could include changes such as
    - A significant purchase or divestment.
    - The construction of a major new facility or pipeline that is significantly different or larger from the permit holder's existing activities.
    - Beginning energy resource activities in a new geographic area where the permit holder has not previously operated.
- A significant organizational change such as a new IT service provider or third party operator.

Clause 11 of CSA Z246.1 includes additional requirements for monitoring and review of SMPs such as:

- Establishing performance indicators (e.g. KPIs) for reporting to appropriate levels of management
- Conducting a management review of SMP suitability, adequacy, and effectiveness at least once per calendar year
- Implement a documented Management of Change (MOC) process which is applied to security / security management

5. Information Submission and Reporting Requirements

5.1. Security Management Program Contact Information

Within 14 days after preparing an SMP, a permit holder must submit the name and contact information of the person responsible for implementation of the program to the BCER. Permit holders with an existing SMP (prior to the introduction of the Regulation) must also provide the name and contact information of the person responsible for implementation of the program to the BCER.

Within 7 days of a change in the name or contact information of the person responsible for implementation of the program, a permit holder must submit the updated information to the BCER.

The submissions must be made to securitymanagement@bc-er.ca.

5.2. Reporting Security Incidents

Security incidents are classified and reported to the BCER in accordance with the Emergency Management Regulation. Security incidents that are classified as Minor, Level 1, Level 2 or Level 3 incidents in accordance with the incident classification matrix (Schedule D of the Emergency Management Regulation) are reportable to the BCER.

Vandalism, theft, malicious equipment damage or tampering, and other types of security incidents are reportable. Refer to Section 4.7 of this document for more examples of security incidents.

An information attack on a permit holder, which has not resulted in a reportable spill or release, is reportable to the BCER if it impacts:

- Sensitive information related to permitted activities,
- The permit holders ability to safely operate or control a permitted asset,

The Emergency Management Manual contains detailed guidance on the incident reporting process and requirements. The process for reporting security incidents is the same as for other reportable incidents. When reporting incidents, permit holders can indicate the incident type as "Security" for any security related incidents. It is important to specify which permitted activities (e.g. facilities, pipelines, etc.) were impacted by the incident and provide details on the type of security incident (theft, threat, sabotage, terrorism, etc.).

Incident reporting instructions and guidelines are located here:

Incident Reporting Instructions and Guidelines | BC Energy Regulator (BCER) (bc-er.ca)

5.3. Other Submissions

All communications with the BCER that are related to the administration of the Security Management Regulation must be made to securitymanagement@bc-er.ca.

5.4. Freedom of Information and Protection of Privacy Act

As a public body, the BCER is subject to the Freedom of Information and Protection of Privacy Act (FOIPPA), which makes public bodies accountable by providing the public with a legislated right of access

to government records. Under FOIPPA, an organization or member of the public can make a request for access to information possessed by public bodies.

The legislation contains certain exemptions to FOIPPA requests for disclosure. Information provided to the BCER is subject to the protection and security requirements in FOIPPA.

6. Required Records and Reports

The Regulation prescribes the following plans, records, or documentation as a prescribed record which must be prepared and maintained for compliance with Section 38(1)(a) of ERAA:

- Security Management Programs (see Section 4 of this document.)
- Documented considerations and decisions with respect to the implementation of cybersecurity measures (see Section 4.4 of this document)
- Training Plan (see Section 4.5 of this document), including:
    - Records of participants for training that is completed in accordance with the training plan
    - Training evaluation and improvement reports
- Security incident response – evaluation reports (see Section 4.7 of this document)
- Any other reports or records required under the regulation or CSA Z246.1

Information required under the Regulation and Standard must be kept in writing (electronic or paper form).

The reports and records prepared and maintained under the Regulation must be made available to the BCER at the permit holder's principal place of business in British Columbia upon request.

7. Third Party Review

At the request of the BCER, a permit holder must engage a third party to review their SMP to verify that it meets the objectives of CSA Z246.1 and submit the results to the BCER. The purpose of third party reviews is to evaluate compliance of the SMP with the requirements of the Security Management Regulation and CSA Z246.1. The BCER would likely request a third party review when additional expertise is needed to conduct a detailed review of an SMP for compliance.

The third party reviewer must be accepted by the BCER. The third party must have demonstrated experience with:

- The requirements of CSA Z246.1.
- Oil and gas sector security, including cybersecurity.
- Auditing SMPs.

If accepted by the BCER, permit holders may propose to use multiple third parties to conduct a review of an SMP. This may be necessary if an individual third party is lacking demonstrated experience in specific areas of CSA Z246.1 (e.g. cybersecurity).

Permit holders will be required to cooperate with third party reviewers, providing any requested information, participating in discussions, and arranging interviews with personnel as needed.

8. Exemptions

An official may exempt a permit holder from one or more provisions of the Security Management Regulation or one or more requirements of CSA Z246.1 if the official is satisfied that:

- Compliance with the provision or requirement is not reasonably practicable, or
- The exemption is in the public interest.

In granting an exemption, an official may impose conditions on the exemption.

All requests for an exemption must be made in writing and be signed by the permit holder's representative. Any exemption issued by an official will be in writing.

Exemption requests must include:

- Specific regulatory provision requiring an exemption;
- Rationale for exemption (explanation of why an exemption is required);
- Proposed plan which demonstrates equivalency or outlines mitigation strategies to reduce impacts (if required)