PIERIDAE
ENERGY

2.1.5.2
CORPORATE SECURITY PLAN

June 2021

24 Hour Emergency Number

1-866-267-5298

Pieridae Alberta Production Ltd., a wholly owned subsidiary of Pieridae Energy Limited

INTEGRATED MANAGEMENT SYSTEM
2.1.5.2 CORPORATE SECURITY PLAN

PREPARED BY: PIERIDAE ENERGY

Next Review Date: June 2022

Pieridae Energy Limited - Corporate Security Plan
Manual Receipt Form

Upon receipt of this Pieridae Energy Limited Corporate Security Plan, this Receipt Form must be completed and returned to the SVP Drilling, Completions & HSE in the Corporate Office. The Manual holder is responsible for ensuring that the Manual is kept current by inserting the latest revisions as they are issued.

Name (please print): ______________________________

Position: ______________________________

Date: ______________________________

Signed: ______________________________

Return signed copy to:

Pieridae Energy Limited
3100, 308 – 4th Avenue SW
Calgary, AB T2P 0H7

Phone: 403-351-5423
Fax: 403-261-5902
Email: yvonne.mcleod@pieridaeenergy.com

Attention:

Yvonne McLeod
VP Drilling, Completion & HSE

PROGRAM ADMINISTRATION

RESPONSIBILITY

The responsibility for maintaining this Corporate Security Plan ("The Plan") is three fold:

1. All manual recipients are responsible for ensuring that their assigned manuals are current.
2. Information in this plan will be verified and updated annually. The Corporate Security Manager is responsible for ensuring the Plan is reviewed by all personnel annually and immediately after any changes have been made to the manual.
3. The Corporate Security Manager, is responsible for updating the manual. Any requests for revisions to the Plan should be forwarded to the Corporate Security Manager or approval and implementation.
4. The only physical copy will be held by Corporate Security Manager, all other copies will be available digitally in the Integrated Management System (IMS) under 2.1.5.2 Corporate Security or via link in Operations Management System (OMS) SS 5.0 Security. All other recipients of digital copies will have annual review assignment through Learning Management System (LMS) Workhub identified learning profile requirements. Review sign off will be recorded in Workhub.

REVISION MATRIX

Site Specific Area: ____

Matrix Administrator:____

Plan Revision	Annually
Update Company Personnel Contact List	✓
Document and Map Updates’	✓
Confirm Response Agencies and Government Support	✓
Update Distribution List	✓
Conduct Response Training	✓

Note: Updates to the manual will be issued to all manual holders annually.

REVISION REQUEST FORM

Recommended By: ______________________________
(Signature)

____
(Name and title)

Date:______________________

Approved By: ______________________________

(Signature)

____
(Name and title)

Date: ______________________

Copies of revised pages attached: Yes □ No □

Section(s) and pages(s) amended or replaced:

Section	Page(s)

Section	Page(s)

Purpose / Comments:

____
____
____
____
____
____
____
____
____

Revision Log		
Revision #	**Date**	**Description**
1	April 2016	Create a Corporate Security Plan to satisfy Canada Energy Board requirements (OPR 99, PRC 2010-01 Pipeline Security Management Programs) and in accordance with CAN-CSA Z246.1-13.
2	August 2017	Revision only to Corporate Emergency Response Team
3	March 2018	Revision only to Corporate Emergency Response Team
4	February 2019	Revision to Corporate Emergency Response Team, Field Personnel and Other Consultant Revised Title on 4.3 Revision to Telephone Directory Revision to Emergency Contact Information Revision to Emergency Contact Information - Ojay CER Regulated Pipeline Revision to Specific Roles & Duties - Ojay CER Regulated Pipeline
5	August 2020	Revision to Company Name and Logo from Ikkuma to Pieridae Alberta Production Ltd. Revision to Distribution List.
6	February 2021	Revision adding New Pieridae Energy acquired assets information
7	June 2021	Revision to include Rail requirements defined by Transport Canada. Revision to integrate the Existing Pieridae Risk Matrix into security risk assessment process.

SECURITY MANAGEMENT PLAN

1.0 DISTRIBUTION LIST

The following individuals will have a copy of this Corporate Security Plan for use as a reference document in the event of a security incident.

CORPORATE EMERGENCY RESPONSE TEAM

Manual #	Name / Title	Company	Location	Plan Type
CSP 01	Darcy Reding Chief Operating Officer	Pieridae Energy Limited	Calgary	DC
CSP 02	Yvonne McLeod VP Drilling, Completions & HSE	Pieridae Energy Limited	Calgary	C
CSP 03	Carolyn Normand VP Engineering	Pieridae Energy Limited	Calgary	DC
CSP 04	Amanda Leam Manager Information and Technology	Pieridae Energy Limited	Calgary	DC
CSP 05	Ken Scheirer Development Engineering Manager	Pieridae Energy Limited	Calgary	DC
CSP 06	Jason Parise Technical Engineering Manager	Pieridae Energy Limited	Calgary	DC
CSP 07	TBD Operations Manager	Pieridae Energy Limited	Calgary	DC

FIELD PERSONNEL

Manual #	Name / Title	Company	Location	Plan Type
CSP 08	Mark Weiss Superintendent Caroline Plant	Pieridae Energy Limited	Caroline Plant	DC
CSP 09	John Fordham Caroline Plant Foreman	Pieridae Energy Limited	Caroline Plant	DC
CSP 10	Billy Joe Jensen Caroline Field Foreman	Pieridae Energy Limited	Caroline Plant	DC
CSP 11	Clair Crosby Caroline Maintenance Foreman	Pieridae Energy Limited	Caroline Plant	DC
CSP 12	Trevor Prenevost Central Alberta Field Foreman	Pieridae Energy Limited	Nordegg	DC
CSP 13	Paul Smith Shantz Foreman	Pieridae Energy Limited	Shantz Plant	DC
CSP 14	Conrad Kenny Superintendent Jumping Pound Plant	Pieridae Energy Limited	Jumping Pound Plant	DC
CSP 15	Dan Flynn Jumping Pound Plant Foreman	Pieridae Energy Limited	Jumping Pound Plant	DC

Manual #	Name / Title	Company	Location	Plan Type
CSP 16	Matt Gartner Jumping Pound Field Foreman	Pieridae Energy Limited	Jumping Pound Plant	DC
CSP 17	Mike Carr Jumping Pound Maintenance Foreman	Pieridae Energy Limited	Jumping Pound Plant	DC
CSP 18	Josh Storle Northern Foothills Foreman	Pieridae Energy Limited	Grande Prairie	DC
CSP 19	Darrell Archibald Superintendent Waterton Plant	Pieridae Energy Limited	Waterton Plant	DC
CSP 20	Randy Urlacher Waterton Plant Foreman	Pieridae Energy Limited	Waterton Plant	DC
CSP 21	Lorne Harty Waterton Field Foreman	Pieridae Energy Limited	Waterton Plant	DC
CSP 22	Jason Jacobs Waterton Maintenance Foreman	Pieridae Energy Limited	Waterton Plant	DC

OTHER CONSULTANTS

Manual #	Name / Title	Company	Location	Plan Type

****Plan Type Legend****

C	Corporate full paper copy
MS	Memory Stick
DC	Digital Copy
APP	Mobile Application

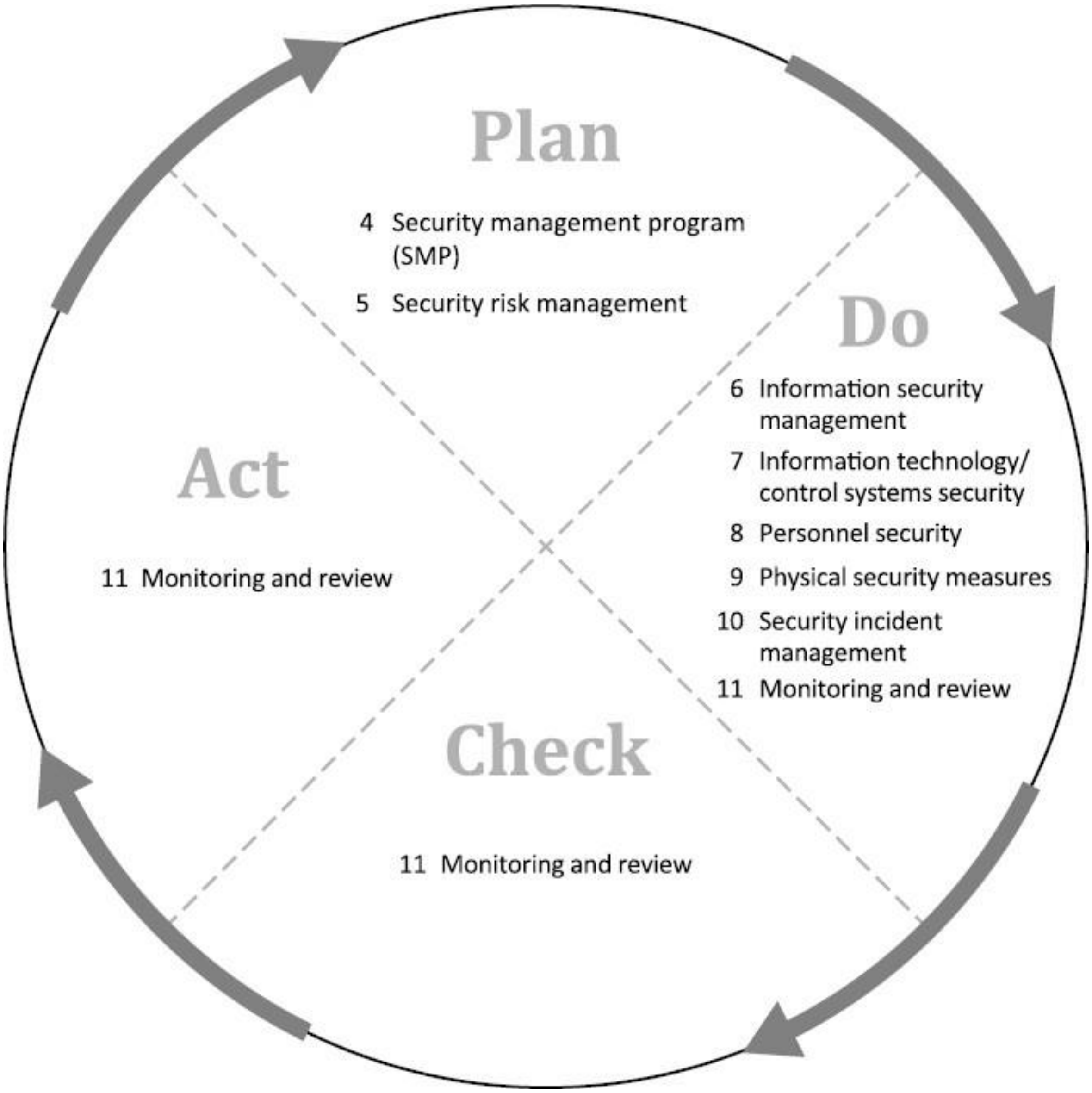
PIERIDAE SECURITY PLAN ROLES

Role	Name / Title	Company	Location	Plan Type
Corporate Security Manager	Yvonne McLeod VP Drilling, Completion & HSE	Pieridae Energy Limited	Calgary	C
Corporate Cyber Security Focal	Amanda Leam Manager, Information and Technology	Pieridae Energy Limited	Calgary	DC
Site Security Manager	Mark Weiss Superintendent Caroline Plant	Pieridae Energy Limited	Caroline Plant	DC
Site Security Manager	Conrad Kenny Superintendent Jumping Pound Plant	Pieridae Energy Limited	Jumping Pound Plant	DC
Site Security Manager	Darrell Archibald Superintendent Waterton Plant	Pieridae Energy Limited	Waterton	DC

Role	Name / Title	Company	Location	Plan Type
Physical and Personal Security Focal	Monica Rosevear HSE Coordinator Caroline Plant	Pieridae Energy Limited	Caroline Plant	DC
Physical and Personal Security Focal	Chris Clattenburg HSE Coordinator Jumping Pound Plant	Pieridae Energy Limited	Jumping Pound Plant	DC
Physical and Personal Security Focal	Maureen Pasion HSE Coordinator Waterton	Pieridae Energy Limited	Jumping Pound Plant	DC
Physical and Personal Security Focal	Paul Smith Shantz Foreman	Pieridae Energy Limited	Jumping Pound Plant	DC
Rail Security Focal	Brent Tannas Jumping Pound, Shantz and Waterton Rail Maintenance Foreman	Pieridae Energy Limited	Shantz Waterton, Jumping Pound Plants	DC
Remote Site Security Focal	Josh Storle Northern Foothills Foreman	Pieridae Energy Limited	Northern Alberta/BC	DC
Remote Site Security Focal	Trevor Prenevost Central Alberta Field Foreman	Pieridae Energy Limited	Central Alberta	DC
Remote Site Security Focal	Matt Gartner Jumping Pound Field Foreman	Pieridae Energy Limited	Jumping Pound Plant	DC
Remote Site Security Focal	Maureen Pasion HSE Coordinator Waterton	Pieridae Energy Limited	Waterton Plant	DC
Remote Site Security Focal	Billy Joe Jensen Caroline Field Foreman	Pieridae Energy Limited	Caroline Plant	DC
Site Cyber Security Focal	Lonny Mackenzie Controls and Automation Specialist Caroline Plant	Pieridae Energy Limited	Caroline Plant	DC
Site Cyber Security Focal	Gavin Bonertz Controls and Automation Specialist Waterton Plant	Pieridae Energy Limited	Waterton Plant	DC
Site Cyber Security Focal	Mark Kendrick Controls and Automation Specialist Jumping Pound Plant	Pieridae Energy Limited	Jumping Pound Plant	DC

2.0 INTRODUCTION

2.1 Introduction


Plan
4 Security management program (SMP)
5 Security risk management
Do
6 Information security management
7 Information technology/ control systems security
8 Personnel security
9 Physical security measures
10 Security incident management
11 Monitoring and review
Check
11 Monitoring and review
Act
11 Monitoring and review

Security Management Program Overview

*Obtained from CAN CSA Z246.1-13.

Pieridae Energy Limited (“Pieridae”) is committed to ensuring the safety and security of the public, personnel and facilities involved in its business operations and in doing so will also minimize any adverse impacts to the environment or economic conditions that might result from any security threat or incident.

Pieridae Alberta Production Ltd. (“PAPL”) is a wholly owned subsidiary of Pieridae Energy Limited and the operating assets in Alberta, British Columbia and Saskatchewan are governed by PAPL.

Accordingly, company personnel are required to understand how the security protocols and procedures outlined in this Corporate Security Plan apply to their respective areas of work and responsibility and to adhere to security procedures as required.

This Plan provides personnel at all levels with the corporate policies, necessary checklists and matrices to respond to security incidents and threats in a proactive manner, minimizing impact and mitigating risk where possible.

Security is everyone’s responsibility. Pieridae’s policies and personnel are the first line of defense against every threat, from minor accidents to simple criminal intent through terrorism and its resultant catastrophic impact.

Pieridae has a **Minimum Operating Security Standard** (MOSS) that defines the standard of security risk mitigation measures for operating in a no risk/low risk threat environment through to complete shut-down of operations where a specific target has been identified and the probability of attack is imminent.

2.2 Purpose

The Pieridae Corporate Security Plan establishes security policies and practices for mitigating security risks and for reducing the impact of threats or incidents on the facilities operated by the company. The Plan ensures uniformity in fundamental security practices and procedures. Utilizing the guidelines provided herein, Pieridae managers should review all facility-specific security measures that are appropriate for the type and location of the facility and report MOSS deficiencies immediately.

The Plan outlines the roles, responsibilities, reporting procedures, guidelines for protective measures against, and response procedures to threats posed by terrorists and criminals to Pieridae facilities. It is designed to comply and interact and be consistent with:

- Corporate Emergency Response Plan (ERP), Site Specific ERPs and Canada Energy Board (CER) Regulated ERPs.
- Pieridae Policies, Procedures and Practices.
- Pieridae Information Security Policies and Procedures.
- Pieridae Corporate Health and Safety Management System.
- Pieridae Human Resource Policies, where applicable.
- The Canada Energy Board (CER) PRC 2010-01.
- Transportation of Dangerous Goods by Rail Standard current to May 17, 2020
- The Alberta Counter Terrorism Crisis Management Plan (ACTCMP).
- RCMP Guide to Threat and Risk Assessment can be referenced.
- Canadian Standards Association Z246.1-13 dated March 2013.
- Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition – American Petroleum Institute.

2.3 Scope

The Plan applies to all Pieridae facilities including, but not limited to:

- Offices
- Facilities
- Pipelines
- Pipeline systems handling;
    - oil
    - gas
    - sulphur
    - oil-field water
    - liquid products
    - multi-phase fluids
    - slurries
    - system supports, including
        - meter stations
        - compressor station,
        - pump stations
        - tank farms, and
        - all assets that support the above.
- Rail loading facilities
    - Sulphur
    - Propane
    - Butane
    - Ethane
- Liquefied natural gas (LNG) production, storage and handling facilities (LPG etc...)
- Storage of hydrocarbons in underground formations
- Petrochemical installations, including:
    - Refineries
    - Gas processing plants
    - Synthetic natural gas plants
- Well sites, batteries, Steam Assisted Gravity Drainage (SAGD) facilities and gas plants in Canada.

The Plan has been structured with criticality, vulnerability, risk, likelihood and consequence of a threat taken into account in assessing each individual facility and incorporating commensurate security measures in accordance with the Minimum Operating Security Standards as set out in this Plan.

2.4 Security Policy

The **Minimum Operating Security Standards (MOSS)** details risk mitigation policies that form the centre of Pieridae security policies. The MOSS measures are defined in Section 6.0 for all Pieridae facilities.

2.5 Document Maintenance and Distribution Process

Plan Coordinator

- The Corporate Security Manager is responsible for development and administration of this Plan.

Update and Approval of Security Management Plan

The Corporate Security Manager will conduct an annual review of the Security Plan as a minimum, or more frequently if threat levels change, indicators are triggered, if a significant security incident takes place either within Pieridae's installations, or if there are significant changes to the Company's facilities.

- The Corporate Security Manager will be responsible to update all Corporate Security Plan information.
- The Corporate Security Manager, in the Operations Department will approve significant changes to the Corporate Security Plan in consultation with the COO.
- It is the responsibility of any persons referencing these documents to ensure they contain the most up to date information.

2.6 Training and Testing the Security Management Plan

Required field employees will undergo security awareness training on commencement of employment, periodically at minimum every three years, or as situations dictate. Training will be conducted in conjunction with Pieridae's various ERP training schedules and Learning Management System learning profiles, under the auspices of the Corporate Security Manager.

2.7 Security Vulnerability Assessment

Pieridae has conducted an SVA of its CER Regulated pipelines / facilities and critical infrastructure in April 2016. The process includes facilities and pipeline inspections completed in April 2016 and report submission. Capital budget inclusion for facility upgrades to meet Pieridae's Minimum Operational Security Standards (MOSS) will be submitted in fiscal year April 2016 for future security enhancement.

2.8 Audits and Security Plan Review

Management will identify facilities to be randomly audited annually to ensure compliance with the Corporate Security Plan. The results of the audit will be reported to the Corporate Security Manager for remediation.

2.9 Change Management, Evaluation and Improvement Process

Pieridae will develop and implement a security exercise and drill process to evaluate the effectiveness of the security incident response process. Security exercises and drills will be conducted on a regular basis as determined by Senior Management. Lessons learned will be identified and collated by the Corporate Security Manager and communicated to Senior Management. Evaluation results of the audit, combined with the lessons learned during the Plan exercises across Pieridae facilities will generate recommended amendments to the Plan for management review and implementation annually. See Section 11 for Change Management Process.

2.10 References

- Canada Energy Board (CER) Pipeline Security Management, 21 May 2004
- Canada Energy Board (CER) Proposed Regulatory Change (PRC) 2010-01
- Alberta Regulation 253/2007 – Security Management Regulation
- CSA Z246.1-13 Security Management for Petroleum and Natural Gas Industry Systems, March 2013
- Alberta Counter Terrorist Crisis Management Plan
- Transport Canada – Transportation of Dangerous Goods by Rail Security Regulations

3.0 GLOSSARY

The glossary of terms can also be found in *CAN/CSA Z246.1-13Security Management for Petroleum and Natural Gas Industry Systems*.

Access Control – The control of persons, vehicles and materials through entrances and exits of a protected area: *Access control is an aspect of security that often utilizes hardware systems and specialized procedures to control and monitor movement into, out of, and within a protected area. Access to various areas may be limited to place or time, or a combination of both.*

Adversary – any individual, group, organization or government that conducts activities, or has the intention and capability to conduct activities detrimental to an operator's critical assets. *An adversary can include intelligence services of host nations, or third party nations, political and terrorist groups, criminals, rogue employees and private interests; and adversary can also include site insiders, site outsiders, or the two acting in collusion*.

Alert Levels – describes a progressive, qualitative measure of the likelihood of terrorist actions, from negligible to imminent, based on government or company intelligence information. Different fixed or variable security measures may be implemented based on the level of threat to the facility.

Asset – any person, environment, facility, material, information, business reputation, or activity that has a positive value to an owner. Assets in the Security Vulnerability Assessment include the community and the environment surrounding the site.

Asset Attractiveness – An assessment of the perception of value of an asset from an adversary's perspective that influences the likelihood of a security incident, based on factors such as location, ease of access, size and vulnerability, with consideration being given to the threat environment.

Asset Characterization – The systematic identification and ranking of facility assets that, if destroyed or damaged due to criminal activity or other hazards, could potentially result in significant adverse consequences to the owner / operator. *Asset characterization can include surrounding and supporting infrastructure*. *This process will allow the operator to determine which assets require further evaluation under the security risk management process.*

Change Management – A systematic process used to ensure internal and external changes are continuously evaluated in order to assess the potential impact that change will have on the security management program (SMP).

Countermeasure – A temporary action or activity taken as a reaction to mitigate a specific security threat.

Critical Facilities – Systems and assets, whether physical or virtual, so vital to the company that the incapacity or destruction of such systems and assets would have a debilitating impact on people, the environment, property, or the economic viability of the company.

Critical Infrastructure – Systems and assets, whether physical or virtual, so vital to Canada that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters.

Cyber Security – Is the practice of protecting systems, networks, and programs from digital attack.

Intrusion Detection Systems – A system designed to detect the entry or attempted entry of a person or vehicle into an area.

Measure – An action or activity intended to improve one or more aspects of the security system to mitigate security risks/threats.

National Terrorism Advisory System (NTAS) – replaces the color-coded Homeland Security Advisory System (HSAS). NTAS will communicate information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports and other transportation hubs, and the private sector.

Operator – A person, including an owner or delegate who:

- Is in control of part or all of a petroleum and natural gas industry system and is accountable for its day-to-day operations.
- Has operational responsibility for any petroleum and natural gas industry system.
- Has direct operational control of part or all of a petroleum and natural gas industry system.

Owner - A person, other than a lien holder, who has an asset or title to a petroleum and natural gas industry system, facility, or equipment and is:

- Responsible for the ongoing operation of a petroleum and natural gas industry system.
- In charge of managing the operation of a petroleum and natural gas industry system, if all or part of the petroleum and natural gas industry system are owned jointly by different persons.

Perimeter – An outer limit or boundary that protects another area.

Physical Security – Security systems and architectural features that are intended to improve protection. *Examples include security officers, fencing, doors, gates, walls, turnstiles, locks, intrusion detection systems, vehicle barriers, and hardened glass*.

Policy – A high-level statement of the overall written intentions and directions of an organization.

Post Orders – Written directions informing uniformed security officers of what they are required to do in the event of a security-related incident or threat.

Railway Carrier – Means a person who has possession of dangerous goods for the purpose of transportation by railway vehicle on a main railway line, or for the purpose of storing them in the course of such transportation.

Railway Loader – (a) any person that operates a handling site, or (b) any manufacturer or producer of dangerous goods that has possession of dangerous at a handling site for the purpose of loading them prior to, or unloading them after, transportation by rail.

Restricted Area – An area containing systems or assets that, if compromised, would have a major adverse impact on people, the environment, assets and economic stability. **Note:** *Restricted areas include control centre operations, security departments, and certain information technology areas*.

Risk – The measure of potential for damage to or loss of an asset based on the probability of an undesired occurrence.

Risk Analysis – A detailed examination including risk assessment, risk evaluation, and risk management alternatives, performed to understand the nature of unwanted, negative consequences to human life, health, property, or the environment; an analytical process to provide information regarding undesirable events; the process of quantification of the probabilities and expected consequences for identified risks.

Security Incident – A security-related occurrence, threat or action that has led to, or could potentially lead to adversely affecting people, the environment, assets, and economic stability.

Security Management Program (SMP) – An on-going process to ensure security threats and associated risks are identified and managed with appropriate mitigation and response procedures to prevent and minimize the impact of security incidents adversely affecting people, the environment, assets, and economic stability.

Security of Information – Information obtained or developed in the conduct of security activities.

Security Partner – Parties who, through formal or informal agreements, establish relationships with each other, governments, regulators, enforcement, and public safety agencies and participate in security risk assessments and risk mitigation strategies, including the sharing of information and the securing of petroleum and natural gas industry systems against acts of vandalism, terrorism, or other security threats.

Security Stakeholder – Parties who have a direct or indirect vested interest in petroleum and natural gas industry systems infrastructure security. **Note:** *Examples include operators, government agencies, regulators, advocates*, *landowners, third parties and members of the general public*.

Security Risk Assessment (SRA) – A systematic, analytical process which identifies security threats, assesses, and implements key security controls in application. It also focuses on preventing application security defects and vulnerabilities.

Security Vulnerability Assessment (SVA) - A systematic, analytical process in which potential security threats and vulnerabilities to facility or system operations are identified and the probability and consequences of potential adverse events are determined.

Supervisory Control and Data Acquisition (SCADA) – A computer-based monitoring and control system that collects, displays, and stores information from remotely located data collection units and sensors to support the control of equipment, devices, and facilities.

Terrorism – In accordance with section 83.01 (1) (b) of the Anti-Terrorism Act of December 24, 2001, “terrorism” involves an actual or threatened.

> *“Act or omission, in or outside Canada, that is committed in whole or in part for a political, religious or ideological purpose, objective or cause, and ... with the intention of intimidating the public, ... with regard to its security, ... and ... that intentionally causes death or serious bodily harm ... by the use of violence, ... causes a serious risk to the health or safety of the public, ... substantial property damage ... or causes serious interference with ... an essential service, facility or system, ... other than as a result of advocacy, protest, dissent or stoppage of work...”*

Threat - The intention and capability of an adversary to undertake actions that will be detrimental to people, the environment, assets, and economic stability.

Threat Levels – A progressive, qualitative measure of the likelihood of adversarial actions, from negligible to imminent, based on government or company intelligence or information. **Note:** *Different fixed or variable security measures can be implemented based on the level of threat to the facility.*

Vulnerability - Any weakness that can be exploited by an adversary to gain access or cause damage to an asset. **Note:** *Vulnerabilities include asset characteristics, equipment properties, personnel behaviour, locations of people, equipment, buildings, and operational and personnel practices.*

4.0 SECURITY MANAGEMENT PROGRAM (SMP)

4.1 General

Governance of the Security Management Program (SMP) sets Pieridae policies and processes to define how the SMP will be integrated into the overall Pieridae Integrated Management System and further into the Operations Management System. Security governance includes management commitment and accountability as outlined in the ensuing sub-sections.

4.2 Management Commitment

The Corporate Security Plan (CSP) is integrated into the Company's overall security management program. Management at all levels are committed to and are accountable for security governance. The CSP provides clear direction, commitment, responsibility and oversight and defines Pieridae's security environment.

4.3 Chief Operating Officer

The COO will:

- Establish goals and expectations.
- Assign responsibility and accountabilityfor all levels of management and employees for implementing the security policies and procedures.
- Remain accountable for protecting the safety of the work force by promoting the security program.
- Encourage employee involvement in the security program bydemonstrating management commitment to security.

4.3.1 *Corporate Security Manager*

The Corporate Security Manager is responsible for implementing and managing Pieridae's corporate Security Management Program (SMP) and is the **primary corporate security focal point**. The Corporate Security Manager will coordinate among the company's entities to ensure compliance with applicable regulatory requirements. This office is responsible for disseminating Pieridae security policies, procedures and alerts and is designated as Pieridae's security incident and threat information manager. In the event of a security incident or threat, the Corporate Security Manager will recommend to the President/CEO the appropriate Pieridae response as required. The Corporate Security Manager, will:

- Ensure that implementation plans are prepared for all major facilities, CER regulated pipelines, and rail sites.
- Assist in the development, implementation, control, review, maintenance and continual improvement, and approval of the security management program.
- Ensure resources are in place for executing an effective security managementprogram.
- Develop Performance Management objectives for implementing the security management program.
- Encourage employee involvement in the security management programby demonstrating management commitment to security.
- Set expectations on the required performance tomeet the standards of the Company's security management program.
- Assess security incidents and threats and recommend appropriate responses.

4.3.2 *District / Area / Production Foreman and Superintendents (Site Security Manager)*

Pieridae District / Area / Production Foremen and Superintendents play a critical role in translating corporate security policies into functional security measures and procedures at individual field locations. District / Area / Production Foremen and Superintendents are also responsible for ensuring that procedures are in place for regular monitoring of facility location for any breaches in security or potential security threats.

All security incidents and threat information obtained in the field by company personnel should immediately be reported to the Corporate Security Manager and the appropriate District / Area / Production Foremen, Superintendents and Operations Manager. In addition, the District / Area / Production Foremen and Superintendents should maintain close coordination with the Corporate Security Manager to ensure that security measures at each facility are in compliance with current regulations and MOSS guidelines. District / Area / Production Foremen and Superintendents will:

- Prepare and communicate security implementation plans for all field and office groups.
- Incorporate requirements of security into daily work activities.
- Investigate incidents.
- Develop Performance Management objectives for implementing security.
- Report and investigate security incidents and implement corrective actions.
- Review the Company's security program with all new and transferring workers.
- Ensure workers understand the security program and their security responsibilities.
- Ensure security awareness orientations are conducted and recorded.

4.3.3 Site Security Focal

Pieridae Energy Site Security Focal's will play a critical role in the competency training and internal auditing of our security management plan. They are considered the Subject Matter Experts of the site security processes such as but not limited to, Physical Site security, Personal Security, IT/Technologies Security, Rail Security and Remote site security and will:

- *Conduct Yearly Security Self Assessments LOD audits.*
- *Participate in completion of Security Risk Assessment and scheduled update reviews.*
- *Assess competency of persons who is responsible for implementing the plan or a portion of it, within the Pieridae Learning Management System.*

4.3.3 *Site Liaison Officer*

The Site Liaison Officer will ensure government and regulatory agencies are contacted and provided with any necessary communications related to a security threat or incident.

4.3.4 *Pieridae Corporate EOC*

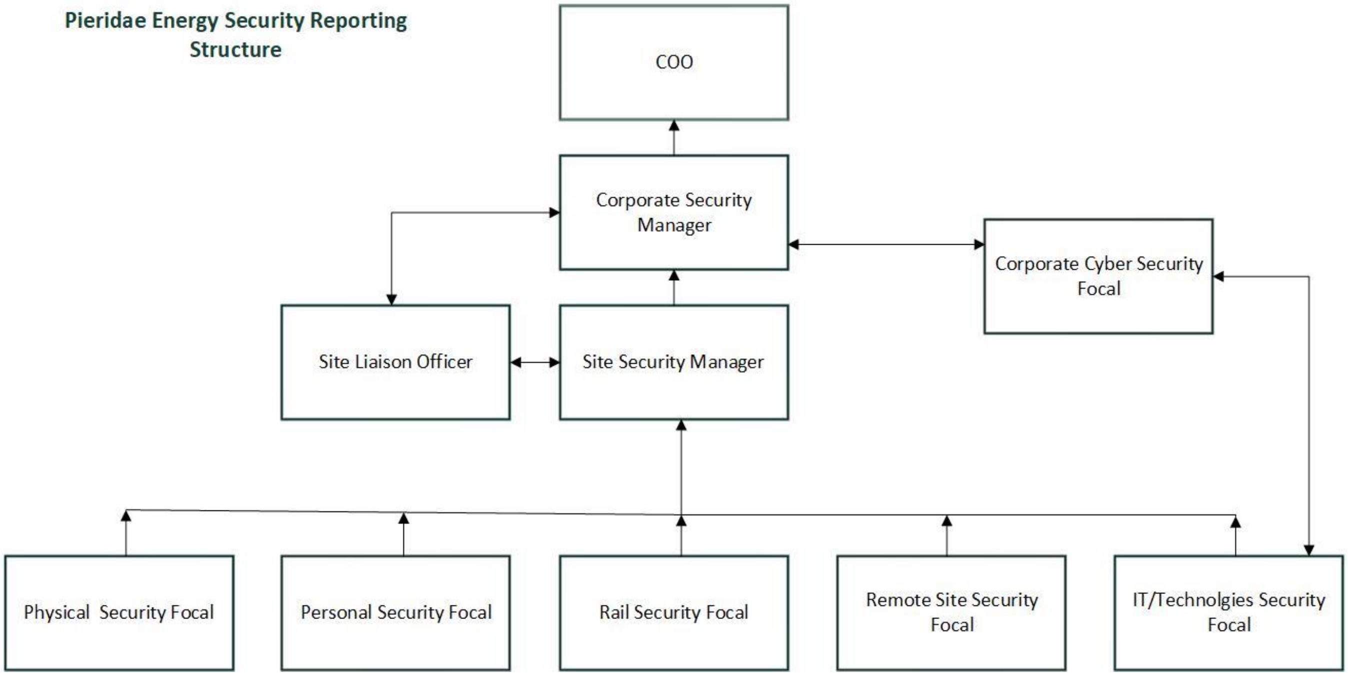
The Area Foreman may be the first point of contact. The Pieridae 24-hour emergency telephone number may be the first contact made. The on-call senior personnel are usually contacted immediately thereafter when a security incident or threat is reported. A Control Room at any Pieridae facilities that is manned 24/7 with operators on duty has the responsibility to communicate the incident or threat to Site Security Manager - Corporate Security Manager, and District / Area / Production Superintendent and to appropriate Government Agencies and Emergency Response personnel as per the applicable Pieridae site specific ERPs and the Company's internal notification system. In addition, the applicable Control Room and/or Pieridae Corporate EOC are responsible for adjusting system operations in the event of a security incident or threat to minimize the real or potential impact.

4.3.5 *Security Incident Investigation Team*

A security incident investigation team will consist of a Department Representative, The Site Security Focal, Site Security Manager, Corporate Security Manager and Senior Management in accordance with the security level and situation.

4.3.6 *Initial Media Statement*

During the initial stages of the incident, the Corporate Spokesperson or designate will prepare a brief factual media statement, as per Pieridae Corporate ERP and the Pieridae crisis communications plan.


Pieridae Energy Security Reporting Structure
COO
Corporate Security Manager
Corporate Cyber Security Focal
Site Liaison Officer
Site Security Manager
Physical Security Focal
Personal Security Focal
Rail Security Focal
Remote Site Security Focal
IT/Technolgies Security Focal

4.4 Indicators

Indicators are events and or actions that highlight a trend of violence or acts targeted to cause disruption. Specific to Pieridae, these indicators, when combined, show an increase in the probability that a threat or security incident may take place.

Monitoring for security incidents will be achieved through:

- Direct observation by company personnel, vendors and contractors on site,
- Indirectly through the monitoring of global conditions and indicators,
- Intelligence information from both public and private sectors.

As an example of a Pieridae CER regulated pipeline, pipeline conditions are monitored and controlled by the applicable Pieridae Control Room(s) in Alberta on a 24-hour basis through the use of the Supervisory Control and Data Acquisition (SCADA) system. In addition, the operator of the pipeline (Canadian Natural Resources Limited) uses the SCADA System to monitor and control Pieridae’s (licensee) Ojay operations.

4.4.1 *Global, Regional and Local Indicators*

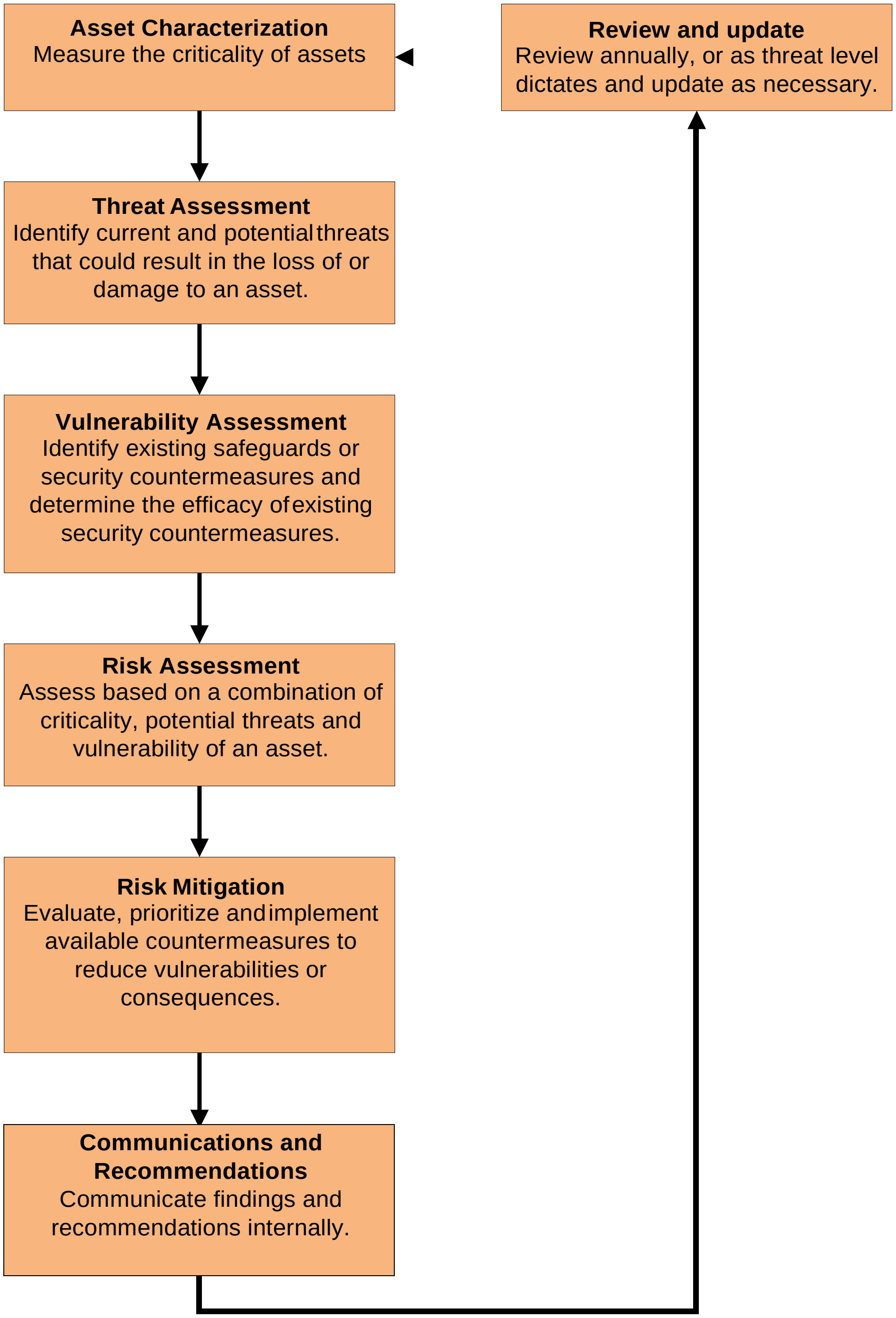
The table below outlines indicators of potential security incidents and threats that could impact Pieridae operations globally, regionally and locally.

	GLOBAL	REGIONAL	LOCAL
	Middle East, African, Central and South American, as well as Asian instability and conflict remain high. The humanitarian crisis and violence in Syria and Iraq; and the failure of the Arab League to moderate are indicators of a power shift from Saudi Arabia to individual despots. Iran nuclear issue. The Iran nuclear deal framework is significant, as it has eased sanctions and allows Iran to once again export oil. Hezbollah in Gaza and Lebanon remains an issue. There continues to be a high risk of political and religious violence in Lebanon. Wahhabi extremism is currently seen as the greatest threat to western nations rather than al-Qaeda. The chaos in Libya as it transits from autocratic rule has been exploited by extremist groups. Al-Qaeda in the Arabian Peninsula (AQAP) has been widely recognized as a more dangerous regional and international terrorist organization than the original al-Qaeda. The humanitarian crisis in the middle east, arising from fighting between allied forces and ISIS, has forced refugee evacuation on an unprecedented scale. Intake of refugees by western European countries, such as Germany, Denmark and Sweden, has created internal violence in these countries. The decision by Canada to take in 25,000 Syrian refugees is of concern. Threats against western nations and global policies continue through internet-based propaganda and insurgent training web portals, as well as training facilities abroad. Terrorist groups like ISIS and al-Qaeda continue working to radicalize individuals and inciting them to leave their homes to become foreign	Pieridae operations are relatively safe from the effects of global and regional security threats, given the geographic distribution of operations and the economic stability of Canada. However, key Alberta industries, such as the oil and gas industry, face the challenge that a terrorist disruption to one industry could significantly impact all industries (e.g. catastrophic destruction of refineries, which would reduce production). In addition, activist groups are becoming increasingly more vocal and demonstrative (oil sands protests, Enbridge Northern Gateway pipeline, and the Keystone XL pipeline project are but a few of the examples). Cybersecurity attacks. Due to increased numbers of remote working stations, accelerated cloud infrastructure and applications, growth in online collaboration tools and the rising use of mobil apps, Cyber attacks have become more prevalent. These attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.	Local threats and security incidents are more likely to be opportunistic rather than premeditated in nature; therefore the consequence of these types of security incidents is usually minor. Threat specific information on a local nature for a premeditated incident will likely be communicated to Pieridae through a number of different sources including Federal agencies and departments.

	terrorist fighters. Those who return to their countries of origin pose even greater security risks, as they can exploit their military skills learned abroad to carry out attacks in their home countries. Canadian intelligence agencies have reported incidents of know terrorist groups planning terrorist acts against other nations from Canadian soil Terrorist organizations have named Canada as a target country of terrorist aggression due to its allegiance to the US. Monitoring the RCMP and National Terrorism Advisory System will indicate increased/decreased concern regarding global security issues and should provide some standoff time for enhanced security preparations.		
PRIMARY	Security incidents against Pieridae types of infrastructure take place globally.	Security incidents are targeted against co-users of Pieridae assets, co-located assets (in proximity), and like assets of other operators.	Direct information from reliable sources that a security incident will occur.
SECONDARY	Security incidents are targeted against company specific assets (European/CAN/US origin).	Heightened demonstrations against US and/or Canadian foreign policies expanding across a region.	Confirmation following an incident that it was premeditated in nature.
TERTIARY	Security incidents are linked to National actions and Company specific policies.	Escalation of the level of violence in demonstrations including but not limited to Western Embassy siege/occupation, destruction of visible North American assets abroad.	Site specific in nature, with little or no impact on operations and no risk to personnel indicates an opportunistic security incident and should be handled as such.

5.0 SECURITY RISK MANAGEMENT PROCESS

The security risk management process provides the flexibility needed for proactive decision making to address the security risks to Pieridae. Security risk management activities should be commensurate with the type, size, location and criticality of the assets being protected.



Asset Characterization
Measure the criticality of assets

Threat Assessment
Identify current and potential threats that could result in the loss of or damage to an asset.

Vulnerability Assessment
Identify existing safeguards or security countermeasures and determine the efficacy of existing security countermeasures.

Risk Assessment
Assess based on a combination of criticality, potential threats and vulnerability of an asset.

Risk Mitigation
Evaluate, prioritize and implement available countermeasures to reduce vulnerabilities or consequences.

Communications and Recommendations
Communicate findings and recommendations internally.

Review and update
Review annually, or as threat level dictates and update as necessary.

5.1 Asset Characterization

All assets, whether they are persons, a facility, material, information, a business reputation or an activity that has a positive value to the operator, shall undergo an evaluation of their criticality. Severity of consequences and asset attractiveness can be used to screen assets to identify those that require only general security countermeasures and those that require more specific security countermeasures. Using this information, assets can be prioritized based on the severity of consequences.

Criticality of assets will be reviewed annually as a minimum or as security threat levels dictate, and will be updated as required. Commensurate with this review will be the requirement to ascertain the impact if any asset were to be damaged or destroyed using the risk matrix in Sections 4.1 and 4.2.

5.1.1 *Process*

Asset characterization should:

- Identify and address any contractual and legal requirements.
- Consider time factors if certain assets become more important at different times during the year due to weather, turnarounds, and other regularly occurring events.
- Identify any critical interdependencies (e.g., other supporting assets, how loss ofone interdependent asset affects others).
- Be harmonized with Pieridae's business continuity program.
- Consider the worst-case scenario (e.g. catastrophic loss of asset).

5.2 Threat Assessment

5.2.1 *General*

A documented process will be developed and implemented to identify any current and potential threats against Pieridae assets that could result in the loss or damage to an asset. The threat assessment will:

- Consider available and relevant information from both internal (CLO- Community Liaison Officer) and external sources (RCMP graduated threat level, National Terrorism Advisory System, ACTCMP, news, etc.); and
- Be reviewed and updated at regular intervals or as circumstance require. Minimum 3 year review.

5.2.2 *Process*

The threat assessment process should determine the following:

- Presence and identification of a potential adversary.
- Capability of an adversary to carry out a threat based on an assessment and evaluation of the nature of the threat and degree of sophistication needed to carry out the threat (e.g., specific training, financial support, and industry expertise).
- Intentions as to whether the threat has been stated or implied and belief that the threat is real.
- History of a similar threat having occurred in the past to another similar operation within the same industry or region.
- Specific information as to whether the threat identifies the target or the potential attractiveness of a target.
- Immediacy of the threat being carried out (e.g., date or timeline).

- Probability of the threat being carried out based on the reliability or credibility of available information.

Once a threat assessment has been carried out, a vulnerability assessment will need to be completed to identify existing safeguards or security countermeasures and determine the efficiency of existing security countermeasures.

5.3 Vulnerability Assessment

A documented process will be developed and implemented to assess asset vulnerability. The assessment shall:

- Be performed at regular intervals – annually, or as the security threat level dictates.
- Identify relationships between the prioritized assets and potential threats.
- Evaluate the effectiveness of existing security measures.

The vulnerability assessment should consider:

- Interdependencies between assets.
- The likelihood of an adversary successfully carrying out the threat.
- Specific vulnerabilities based on existing safeguards and countermeasures, and location.

On completion of a vulnerability assessment (security vulnerability assessment or SVA), Pieridae will evaluate, prioritize and implement available countermeasures to reduce vulnerabilities or consequences. This will be in the form of a graduated threat mitigation matrix (see Section 5.5).

5.4 Risk Assessment

Risk assessment is the overall process of risk analysis and risk evaluation. The process will take into account findings from the asset characterization, threat and vulnerability processes.

5.5 Security Risk Assessment

A Security Risk Assessment (SRA) is a systematic process that evaluates the probability that a threat against a facility or asset will be successful and considers the vulnerability and potential consequences to the facility itself, to the surrounding community, the environment and on the energy supply chain.

Pieridae follows the methodologies for a Threat Risk Assessment utilizing SS GD1.04.012 Pieridae Energy Risk Assessment Matrix as its baseline for risk ranking. SRA methodology process is defined below.

Differences in geographic location, type of operations, and on-site quantities of hazardous substances, if any, all play a role in determining the level of SRA and the approach taken.

The objective of conducting a SRA is to identify security hazards, vulnerabilities and countermeasures that will provide for the protection of the public, workers, national interests, the environment and Pieridae.

All Pieridae major facilities and will complete an SRA identifying security risks and mitigations. SRA's will be reviewed every 3 years or as change circumstances dictate.

All Pieridae CER regulated pipelines and facilities had an SRA conducted in April 2016. SRAs will be reviewed every 3 years or as circumstances dictate (raised security profile, after a significant security incident, new facility, and expanded operations and periodically for validation).

5.6 Risk Matrix

Pieridae has instituted Minimum Operational Security Standards (MOSS) mitigating measures to deal with potential threats. Based on SS GD1.04.012 Pieridae Energy Risk Assessment Matrix. The risk matrix evaluates the likelihood of identified threats occurring, uses a documented quantitative or qualitative method to determine consequences and considers other risks associated with security stakeholders, contractors and suppliers.

The Likelihood and consequence of a threat is measured according to the following tables:

Likelihood

PIERIDAE THREAT LEVEL	DEFINITION	RISK RATING	PIERIDAE ENERGY Security Threat Alert Level	DEFINITION
Remote/ No known threat	Normal operations and low slight risk.	Light Blue	**Green Alert lowest threat level**	
Highly Unlikely/ Low	Intelligence identified an adversary with capability here or abroad.	Dark Blue	**Blue Alert Level Possible Capability**	Warns that the capability of a security threat has been identified.
Unlikely/ Medium	Intelligence identified an adversary with capability and intent. With Medium Consequences	Yellow excluding 5A & 5B	**Amber Alert Level Elevated Threat Alert**	Warns of a capable credible security threat against Pieridae Energy.
Possible/ High	Intelligence identified an adversary with capability and intent, attack is deemed probable.	Yellow 5A & 5B	**Red Alert Level Imminent Threat Alert**	Warns of a credible, specific, and impending security threat against Pieridae Energy.
Likely/ Imminent	Specific target identified. Imminent Probability	Red		

Consequence

This Chart should be used in conjunction with the Probability Chart.

CONSEQUENCE	IMPACT ON PERSONNEL, ENVIRONMENT AND ASSETS
No impact (0-1)	Normal operations, low/slight risk.
Slight (0-1)	Normal operations, no/low risk.
Minor (2-3)	Minor risk to assets and the environment, no significant risk to personnel.
Moderate (4-5)	Increased risk to assets, environmental damage probable, Moderate risk to personnel.
Major (6)	Major risk to personnel, environment and assets,
Catastrophic (7-8)	Loss of life, environmental disaster, destruction of assets

5.7 Risk Matrix

The following table provides Pieridae decision support for security incidents, based on the formula as follows: Based on SS GD1.04.012 Pieridae Energy Risk Assessment Matrix.

$$\frac{\text{Risk Rating} = \text{Probability x Consequence}}{\text{Mitigating Measures}}$$

Using this equation, each security incident can be measured against current MOSS and additional measures can be implemented in a timely fashion.

			CONSEQUENCE					
			0	1	2	3	4	5
			No Impact	Slight	Minor	Moderate	Severe	Catastrophic
LIKELYHOOD	Imminent	E	0E	1E	2E	3E	4E	5E
	High	D	0D	1D	2D	3D	4D	5D
	Medium	C	0C	1C	2C	3C	4C	5C
	Low	B	0B	1B	2B	3B	4B	5B
	Remote	A	0A	1A	2A	3A	4A	5A

5.8 Risk Mitigation

Risk mitigation is the process that identifies countermeasures commensurate to each threat level. The Threat Response Matrix (Graduated Threat Mitigation) is identified in Section 5.10. When the threat level changes, Pieridae will reassess the risk and establish countermeasures appropriate to the threat.

5.9 Communication and Recommendations

Findings and recommendations from the security risk management process are to be communicated through the appropriate supervisor(s) and superintendents to the Corporate Security Manager for acknowledgement and additional decision-making as required.

5.10 Threat Response to Security Alert Levels

Security Alert Levels are set by Pieridae Corporate Security and may change in response to a new or escalated threat. During periods of a prolonged heightened Security Alert, Pieridae Corporate Security will provide the Site Security Manager with updates as the situation dictates. Security Alert Levels shall be evaluated in accordance with Corporate Security Plan Security Alert Levels.

Security levels are:

- Green (lowest level)
- Blue
- Amber
- Red

Green Security Alert Levels - Baseline (minimum) Security Performance Criteria will be applied

Blue Security Alert Levels - Additional to the requirements of the Facility Security Plan, the Site Security officer shall:

- Communicate the change in alert levels to facility Management
- Re-assess security risks or vulnerabilities based on the current situation
- Review the Emergency Response Plan; ensure plan (if implemented) is capable of mitigating potential adversarial actions
- Ensure increase vigilance by office attendants and site security personnel (where applicable)
- Ensure all deliveries (not just mail) are screened for suspicious items/parcels
- Conduct security spot checks of vehicles and personnel entering the facility
- Investigate reported unusual activities, behaviour or utterances
- Ensure perimeter fencing integrity (where applicable, established periodic checks)
- Enhance mail/email inspection procedures (e.g., post reminders, email notices)
- Ensure buildings and storage areas not normally used are secured (e.g., locked)
- Review housekeeping; ensure all unnecessary items are either secured or removed to a safe area (e.g., dumpsters, surplus materials, containers)
- Monitor the national and local security situation
- Monitor news reports
- Inform Business Continuity/Senior Risk Managers and other appropriate managers/departments of Security Threat Level/Operating Level changes
- Make Facilities/Premises/Location Manager or their nominees aware promptly of the changed SOL
- On a change of SOL, consider immediate security re-assessment of estate security arrangements (guarding/access controls/all equipment and alarms) to ensure that all are in working order

- Perimeter/fences/doors etc to be frequently checked for signs of attempted entry
- Institute vehicle access controls (e.g. access for named individuals; consider removing vehicles if owners cannot be identified)
- Communicate changes in SOLs to all staff ensuring that they are aware of any new protective security measures being deployed, thereby gaining their support. Consider re-issuing existing written security guidelines

Amber Security Alert Levels - Additional to the requirements of the Facility Security Plan, and the increased measure required for Blue Alert Levels, the Site Security Officer and facility Management shall:

- Consider temporary enhancements to closed circuit television and intrusion alarm equipment
- Consider providing 24-hour security service for those normally unmanned or attended locations
- Consider screening all mail off-site
- Consider placing all back-up personnel on call
- Consider shutting down all or part of the site operation
- Increase liaison with local law enforcement, neighboring facilities and stakeholders regarding mutual countermeasures
- Consider activating the Emergency Response Plan
- Depending on the nature of the threat, evacuate site and buildings
- Review all non-essential activities, and consider suspension (e.g., construction, shutdowns, tours)
- Reduce access and access points to an absolute minimum
- Restrict delivery vehicle access (e.g., consider leaving parcels at the gate and shuttle inside by an internal vehicle)
- Inspect and escort all vehicles (other than Pieridae owner/authorized vehicles) requiring on-site access (consider use of trained security guards as opposed to Pieridae personnel)
- Establish periodic security patrols with emphasis on parking areas and perimeter boundaries
- Inspect the interior and exterior of all buildings and storage areas in regular use at the beginning and end of each day
- Institute more regular building perimeter patrols and increased CCTV monitoring
- Conduct response refresher training on particular threats
- Brief staff on reasons for greater security awareness and to report any suspicious behavior strangers (e.g. possible site reconnaissance)
- Institute bag searches for all visitors and possible random searching of employee bags; consider possible acquisition of, or additional metal arch detectors and scanners
- Institute searching of vehicles (contractors and /or staff) that access the site
- Consult Corporate Security Manager (SRM) for specialist protective security advice and consider additional, short-term security measures
- Review security equipment to ensure all is in working order
- Implement reduced access to premises and additional controls on all access points

Red Security Alert Levels - Additional to the requirements for Blue and Amber Alert Levels, the Site Security Officer and Management shall:

- Implement the Emergency Response Plan

- Suspend all non-essential activities
- Increase access control measures (closer checking of passes; enforcement of pass-wearing; checking identity of all visitors before entering building or facility; bag searches; mail security; security screening of all visitors and staff
- Restrict access to essential staff only and cancel or reduce activities, operations and meetings
- Ensure that security efforts are coordinated with police and other authorities
- If practical, and possibly with help from local authorities, prevent vehicles from parking within 25 meters (82 feet) from building or the facility's most vulnerable points
- Increase patrols of perimeter by security officers and ensure that security staff are fully aware and reminded of their roles/actions to take if an incident occurs

MOSS	Remote/No Known	Highly Unlikely/Low	Unlikely/Medium	Possible/High	Likely/Imminent
Physical Security	Review measures in place (locks, fences, IDS, CCTV, barriers, access control points).	Secure areas not in regular use, review outstanding maintenance work orders.	Lock all gates except immediate usage.	Limit entry points to absolute minimum. Check all systems. Review and augment lighting as required.	Establish security points, reporting criteria and procedures.
Access Control	Sign in/out and badge policy. Photo ID required. Designate access control points.	Spot check of personnel and vehicles. Reduce access points. Inspect all packages, deliveries.	Limit and escort all visitors.	Detailed vehicle inspections for all vehicles. Positive ID and verified entry need required for all personnel. Package inspections.	Lock down of all facilities.
Cyber Security	Cyber Security Training. Strong Password Strategy Up to date antivirus and malware for both corporate and field. Proper backup and recovery procedures	Strong filters for SPAM, Phishing and other suspicious emails. Tighten firewall security Algorithm. Cyber attack incident response plan.	Yearly Mandatory Security Training. Alignment for cyber insurance. Added advanced filtering to executives email accounts. Tighten remote desktop protocol and VPN access. Increase data security. Ensure vendor cloud services align with our security procedures	Initiate password changes. Limit network accesses. Issue alerts and warnings	Lockdown network
Contingency Plans	Review and ensure contingency plans are current and viable.	Review all plans in light of additional actions at higher threat levels.	Review all plans in light of additional actions at higher threat levels.	Review shut-down and evacuation procedures.	Prepare to implement Business Continuity and Disaster Recovery Plan.

Communications	Establish communication protocols including external agencies. Implement IT security protocols.	Inform all personnel of the change in threat level. Test protocols.	Inform all personnel of the change in threat level.	Advise appropriate Agencies. Inform all personnel of the change in threat level.	Inform all personnel of the change in threat level. Account for all personnel and visitors at sites.
Training	Security awareness training. Public education programs.	Implement periodic updating of all staff.	Confirm availability of security resources over an extended period of time.	Confirm procedures for shut-down and evacuation.	Consider evacuation and shut down of operations.
Patrols	Survey local areas; identify security risks that may affect the facility.	Increase patrols of perimeter, exterior and interior of all buildings.	Increase patrols, including unmanned sites. Identify likely IED sites. Dedicate staff or contract security staff to assist with security duties.	Increase perimeter and building patrols. Request additional patrols from local authorities. Consult with local authorities concerning limiting public access routes.	Augment security forces. Solicit assistance from appropriate Agencies. Cooperate with Authorities.

6.0 INFORMATION SECURITY MANAGEMENT

Procedures and policies pertaining to information technology security and information security are contained in the Pieridae Information Security Policies and Procedures and are in accordance with *CAN/CSA Z246.1-13 Security Management for Petroleum and Natural Gas Industry Systems*. This includes:

- Training and awareness on information security management process, policies and procedures.
- A policy for protection of intellectual property.
- Classifying internal information (e.g., assigning classification levels, ranging from least to most sensitive, such as “restricted”, “confidential” and “proprietary”).
- Handling and storage of information commensurate with its classification level and its security risk. This includes physical and electronic confidential or security sensitive information.
- Handling of external information and assignment of classification at an equivalent or higher level than the classification assigned by the external party.
- Security clearances for individuals with designated positions.
- Records and documentation that comply with the company’s security and privacy policies and procedures, including destruction.
- Information security management measures appropriate to the risk presented for each classification level within the classification system.
- Information technology/control systems security process.
- Documented procedures to integrate information security management policies as part of the information security management program.
- Means of communicating policies and procedures to employees and on-site personnel.
- Expectations for creators, owners, and custodians of information to appropriately classify and secure information from the time it is originated through to its final disposition.

7.0 INFORMATION TECHNOLOGY / CONTROL SYSTEMS SECURITY

7.1 Information Technology

Procedures and policies pertaining to information technology security are contained in the Pieridae Information Technology Security Policies and Procedures and are in accordance with *CAN/CSA Z246.1-13 Security Management for Petroleum and Natural Gas Industry Systems*. This includes:

- Identification of critical assets/systems.
- Implementing appropriate measures, including processes, procedures, organizational structures, and software and hardware functions that are commensurate with the risks to the critical assets/systems to ensure the specific security and business objectives are met.

7.2 Control System Security

The control systems used by Pieridae to manage its infrastructure and products are vital to the company's safe and efficient operation. The growing convergence of information technology (IT) and control systems brings increased capabilities, but also increased exposure to cyber-attacks. Pieridae's Information Technology Security Policies and Procedures include:

- A cyber security strategy.
- Methodologies, industry standards and best practices for securing control systems.

Cyber security measures include, but are not limited to:

- Provision of physical security and access controls to cyber assets.
- Monitoring and periodically reviewing, network connections, including remote and third party connections.
- Evaluating and assessing the role of wireless networking for risk before implementation.
- Reviewing and assessing all cyber security procedures annually and updating as necessary.
- Reviewing and re-assessing cyber asset criticality on an annual basis.
- An operational framework to ensure coordination, communication and accountability for information security on and between the control systems and enterprise networks.
- Defined cyber security roles, responsibilities and lines of communication.
- Documented standards for cyber security controls for use in evaluating systems and services for acquisition.
- Documented policies and procedures for assessing and maintaining system status and configuration information.
- Documented policies and procedures for the secure disposal of equipment and associated media.
- Policies and procedures for cyber intrusion monitoring, detection, incident handling and reporting.

8.0 PERSONNEL SECURITY

Pieridae has developed a personnel security process that addresses:

- The protection of employees and other on-site personnel.
- The roles, responsibilities and management accountability structure to ensure compliance with Pieridae's security policy.
- The conduct of background checks on employees and on-site personnel.
- Mitigation of security risks resulting from voluntary and involuntary termination of employees and on-site personnel.
- Mitigation of security risks and threats during business travel.
- The protection measures required to provide a safe and secure workplace.

8.1 Security Awareness Training

Security Awareness Training (SAT) shall include:

- Training for employees and on-site personnel working at any Pieridae facility including CER and Transport Canada regulated areas.
- Be conducted as part of new employee orientation.
- Be provided on a regular basis.
- Be conducted in accordance with Pieridae's Human Resources Policies, such as personnel screening for those personnel who may have access to restricted areas or information, employee/on-site personnel termination policies, work alone policy, travel policies/procedures to minimize security risks and threats during business travel.
- Include development of security messages for internal communication that will promote a security culture and support the security practices.
- Incorporates:
- Operational security including:
  - Threat environment.
  - Surveillance techniques.
  - Suspicious activities.
- Threat-level response measures and policies.
- Physical security measures, including access controls and security badges.
- Confrontation and communication training.
- Personal protection training.
- Mandatory Cyber Security Training.
- Recognition and reporting of security-related threats/incidents or information that might help detect security threats.
- Includes a component that tests and assesses knowledge and understanding across the organization in applying the security awareness content specific to operational requirements.
- Includes a relevant security stakeholder component to enhance community awareness through various communication methods.
- Maintains procedures to protect the integrity of training records in accordance with Pieridae's record retention policy.

9.0 PHYSICAL SECURITY MEASURES

9.1 Threats to Pieridae Energy Limited personnel, assets AND environment

Threats to Pieridae personnel, assets and environment can be divided into four (4) categories:

- **Premeditated**:
  - Improvised Explosive Devices (IED)
  - Violence directed against Pieridae personnel
  - Hostage taking
  - Cyber terrorism
  - Chemical, Biological, Radiological, Nuclear (CBRN) weapons

- **Opportunistic**:
  - Vandalism
  - Petty theft

- **Accidental**:
  - Human error
  - Equipment malfunction

- **Natural**:
  - Natural disasters
  - Forest fire
  - Pandemics

9.2 Minimum Operational Security Standards (MOSS)

The following sub-sections provide the six (6) measures and procedures that are the MOSS for all Pieridae facilities:

- Physical Security Measures
- Access Control
- Contingency Plans
- Communications
- Training
- Patrols

9.2.1 *Physical Security*

- **Gates**: Pedestrian and vehicular gates should be appropriately secured, and periodically inspected by facility personnel. Vehicle gates should be sufficiently set back from roadways to ensure safety and security of personnel.
- **Fences**: A perimeter fence defines the boundaries of a facility and creates a physical and psychological deterrent to unauthorized entry. Standard fencing should be at minimum chain-link, 2 meters high. Fencing requirements will be determined by reviewing regulations and evaluating risk.
- **Locks**. High quality locks should be used to deter access to important equipment, facilities or areas. If locks are used, a key control procedure must be established and documented, with provision for an issuance and tracking system to prevent unauthorized use or loss of keys or locks.
- **Lighting:** Effective security lighting illuminates areas of a facility with sufficient illumination to identify persons and vehicles, as well as security concerns, such as buildings, storage tanks, and storage areas, active entrances for vehicles and people, and parking areas.
- **Signs:** Signs that restrict access or warn trespassers should be mounted on all sides of the facility’s perimeter fence at regular intervals. Where appropriate, signs may also warn that the premises are under 24-hour surveillance and that all vehicles and personal items are subject to inspection.
- **Intrusion Detection Systems** (IDS): These are designed to protect buildings and/or secure zones from unauthorized intruders. If installed, they shall be maintained and tested on a regular basis and response procedures should be developed.
- **CCTV:** CCTV can provide surveillance to and area or security perimeter. If installed, they shall be maintained and inspected on a regular basis. A privacy impact should also be conducted.
- **Barriers**: Protective barriers control or deny access to a facility by vehicles. Barriers should be placed in avenues of approach, or in locations where the proximity of roadways may endanger exposed piping or buildings. Natural barriers, such as large trees or steep embankments, may serve as anti-vehicular barriers to augment perimeter fencing.
- **Access Control**. Access control for office and field site locations should provide a level of security that is consistent with the assessed criticality of the facility and current threat levels to prevent unauthorized admittance.

	1	**2**	**3**	**4**	**5**	**6**
Physical Security Measures	Gates, Fences, Locks	Lights	Intrusion Detection System	Closed Circuit Television	Barriers	Access Control Points

Physical Security Measures	**Category of Threat**	**Facility**	
		Critical	**Non-Critical**
	Pre-meditated	1-6	1-2
	Opportunistic	1, 2 & 6	1-2
	Accidental	1, 2	1-2
	Natural	1, 2	1-2

9.2.2 *Access Control Procedures*

Access control procedures are designed to control and monitor movement into, out of, and within a protected / restricted area. Procedures must therefore be put in place to enable positive control and monitoring capability of movement of personnel (visitors, on-site personnel) and vehicles.

	Access Control Procedures				
Threat Level	**No Known**	**Low**	**Medium**	**High**	**Imminent**
Procedure	Sign In where available	Spot Check Vehicles, personnel	Escort Visitors	Vehicle inspections, packages, positive ID for all personnel	Lock Down

9.2.3 *Contingency Plans*

Contingency plans for Pieridae are available at Pieridae's corporate office.

	Specific Plan	Source / Location
Contingency Plans	Information Technology Plan	▪ SCADA ▪ Internal (Crisis Communications Plan) ▪ Radio / Satellite / 2-way radio ▪ Cyber Security Plan ▪ Cyber Security Risk Assessment
	Communications Plan	▪ Federal/Provincial Agencies ▪ External Media
	Emergency Response Plan	▪ Corporate ▪ CER Regulated ▪ Site Specific
	Transportation of Dangerous Good by Rail Security Plan	▪ Corporate ▪ Site Specific Facility Security Plan (If required) ▪ Transports Canada Regulated ▪ Rail Security Plan Available upon request Transports Canada

9.2.4 *Communications*

Internal and external communications, notifications, contacts and call down systems with Pieridae employees, the public and government agencies is delineated in the Pieridae Incident Management System; Emergency Response Plan (ERP), and site specific Emergency Response Plans (ERPs).

9.2.5 *Security Training and Awareness*

All Pieridae Energy employees and permanent contractors at any Pieridae Energy office and operating facilities will undergo security awareness training on commencement of employment, periodically at minimum every three years, or as situations dictate. Training will be managed with the Pieridae Energy Learning Management System in conjunction with the ERP training schedule for completion of drills, under the auspices of the Corporate Security Manager.

	Threat Level				
	No Known	**Low**	**Medium**	**High**	**Imminent**
Training	Security Awareness Training	▪ Inform of change in alert status ▪ Review plans ▪ Periodic updates to personnel	▪ Inform of change in alert status ▪ Review plans ▪ Periodic updates to personnel	▪ Review procedures for shut down	Shut down of operations.

Security Training and awareness shall include:

- Training for employees and on-site personnel working at any CER regulated areas.
- Training for employees and on-site personnel working at any Transports Canada regulated areas.
- Be conducted as part of new employee orientation.
- Be provided on a regular basis.
- Be conducted in accordance with Pieridae's Human Resources Policies, such as personnel screening for those personnel who may have access to restricted areas or information, employee/on-site personnel termination policies, work alone policy, travel policies/procedures to minimize security risks and threats during business travel. Personal screening is completed through HR reference checks during hiring, ADP review policy sign off and Learning Management System policy and competencies sign off.
- Include development of security messages for internal communication that will promote a security culture and support the security practices.
- Incorporates:
  - Operational security including:
    - Threat environment.
    - Surveillance techniques.
    - 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.
- A component that tests and assesses knowledge and understanding across the organization in applying the security awareness content specific to operational requirements.

- A relevant security stakeholder component to enhance community awareness through various communication methods.
- Maintaining procedures to protect the integrity of training records in accordance with Pieridae's record retention policy.

9.2.6 *Guards and Patrol Force*

A patrol force may be necessary at a High or Imminent threat level. Pieridae may use either a private security firm or use its own personnel to patrol unmanned facilities. Private security firms may provide additional guard and patrol forces as necessary. See Section 12.0 for Security Services contact information.

If conditions require the use of uniformed security officers, Pieridae will develop clearly defined post orders and ensure that any contracted uniformed security officers are properly licensed, bonded and insured. Pieridae will determine whether security personnel will be contracted or in- house.

	Threat Level				
	No Known	**Low**	**Medium**	**High**	**Imminent**
Patrols	Random	▪ All facilities – state of physical security ▪ Review outstanding capital program	▪ Increase patrols, including ROW	▪ All physical security ▪ Cancel non-vital work at each facility	▪ Maximum patrols sustainable and augment with local police and security forces

10.0 SECURITY INCIDENT MANAGEMENT

10.1 Incident Management and Reporting

All security incidents shall be reported in Pieridae Energy’s Incident Management System (Maximo)

The following examples, although they can also be classified as emergencies, should be handled and reported as security incidents:

- Bomb threats.
- Suspicious packages.
- Workplace violence.
- Theft.
- Terrorism.
- Vandalism.
- Unauthorized entry.
- SCADA or information technology attack.
- Suspicious activities.
- Cyber Threats

The incident management process also includes:

- Identification of the applicable local, provincial, and federal agencies to contact upon a suspected security threat or incident.
- Development of a crisis communications plan that includes communication procedures, capabilities and resources and contains a telephone directory of various groups to be contacted during a security-related threat or incident (See Agency Contact List in Section 12.0 of this Plan and the applicable ERPs)
- Development of an incident report log and records to serve as an official record of actions and lessons learned from the post-incident review (see Time and Event Log in the Corporate or applicable site specific ERP).
- Working and coordinating with other agencies in response to a security-related incident or threat.
- Procedures for changes to the threat level, to include notification, reporting and appropriate responses.

10.2 First Responder

The first responder, after assessing the situation, will contact their immediate supervisor. The immediate supervisor, or Incident Commander if they have been activated, will assign an Alert or Level of Emergency to the incident and activate the applicable Pieridae Emergency Response Plan (ERP). If an emergency is declared, responders will coordinate duties and proceed with roles and responsibilities for a Level One, Two or Three Emergency as per the applicable ERP.

10.3 Reporting

For a pipeline emergency involving a Canada Energy Board regulated pipeline or facility, the **Transportation Safety Board** should also be notified at their **24-Hour hotline at 1-819-997-7887**.

If unable to reach the Transportation Safety Board 24-Hour hotline, the **Canada Energy Board** is to be notified via the CER **24 Hour Incident Cellular Phone** at 1-**403-807-9473**.

Reporting forms are available in Section 15.0 of the Pieridae's Corporate Security Plan, and in the applicable section containing forms in any of the Pieridae Incident Command System ERPs.

For Alberta, the First Call Communications Form must be completed and forwarded to the Alberta Energy Regulator (AER) at all Emergency levels (Levels 1-3).

For British Columbia, the Operator Pipeline Incident Report must be completed and forwarded to the BC Oil and Gas Commission and Emergency Management BC at all levels.

For Rail, in an emergency situation rail loader to report to Transport Canada Situation Center, otherwise it is the Rail Carriers responsibility to report.

10.4 Communications

Internal communications regarding any security incident(s) will be handled in accordance with the Pieridae CSP and / or ERP.

10.5 Documentation

Documentation of security-related threats and incidents shall be retained in accordance with Pieridae information security management protocols at Section 6.0.

10.6 Security Exercises and Drills

The security incident process will be evaluated through exercises, drills and lessons learned from actual incidents.

Exercise and drills are considered part of the overall Emergency Response Plan training cycle and are in accordance with the established Pieridae Resources Corp. ERP training cycle.

11.0 MONITORING AND REVIEW

Pieridae is committed to ensuring its Security Management Program is monitored continuously for improvement and performance. This will be accomplished through performance indicators related to security goals and objectives, compiling of incident statistics and lessons learned from exercises and actual incidents.

11.1 Evaluation and Review

Pieridae will conduct an annual review of its SMP, or more frequently if required. The review will:

- Consider external audit results.
- Consider Internal LOD audit results
- Consider any significant change in assets.
- Consider the success of achieving measurable internal goals (short and long-term objectives).
- Analyze conformance to legal requirements.
- Are required, ensure outcomes of the review are addressed through the Change Management process.
- Be approved by Senior Management.

11.2 Change Management Process

Pieridae’s change management process is in place to ensure internal and external changes are continually evaluated in order to assess the potential impact that change will have on the SMP. This will be accomplished by ensuring that modifications throughout Pieridae’s organization are identified and integrated in an efficient manner.

The Change Management Process:

- Oversight is provided by the VP Engineering.
- Accountability rests with the VP Engineering to ensure the change management process is completed in an efficient manner.
- Will be approved by the VP Engineering in consultation with the President and COO.
- Assigns responsibility to each department for identifying potential changes regarding each element in the SMP.
- Provides opportunity for internal and external stakeholders to suggest improvements.
- Includes an evaluation to see if changes are warranted, while considering available resources for implementation.
- Will consider applicable integration into other processes within Pieridae’s organization.
- Will include communication to all departments and employees of implemented changes to the SMP.

12.0 GOVERNMENT AGENCY RESPONSES

12.1 External Communications – Canada Energy Board

All incidents, accidents and occurrences as defined by the Onshore Pipeline Regulations (OPR), the Canada Labour Code, and the Transportation Safety Board (TSB) Regulations should be reported.

FIRST CALL
For emergencies involving inter-provincial or cross border pipelines, the CER is the Regulatory Authority. In the event of an CER regulated pipeline emergency, call the TSB's 24 hour hotline (collect calls accepted). The TSB will contact the CER to notify them of the incident.
1-819-997-7887

SECONDARY CALLS
Call the TSB's 24 Hr Incident Line to report significant incidents, other than emergencies, on CER regulated pipelines and facilities.
403-807-9473

ONLINE REPORTING
Report all events on the CER's Online Event Reporting System. This system is intended for use by regulated companies to provide notification to the Canada Energy Board (CER) and Transportation Safety Board (TSB) of various events that are defined in regulation including incidents, unauthorized activities, and operations and maintenance activities.
https://apps.CER-one.gc.ca/ers/home/index

The Canada Energy Board (CER or Board) is an independent federal agency established in 1959 by the Parliament of Canada to regulate international and interprovincial aspects of the oil, gas and electric utility industries.

CER-regulated companies have the primary responsibility for ensuring safety and environmental protection because they are the owners, designers, builders and operators of the facilities. The CER recognizes this responsibility in the ongoing development of goal-oriented regulation that places the onus on companies to ensure their facilities are safe and secure and are operated in an environmentally responsible manner. The CER plays a significant role by ensuring that the companies maintain or improve their safety and environmental performance. The Board ensures that companies:

- Identify and manage the potential hazards associated with their facilities and
- operations;
- Conduct a risk analysis of those hazards; and
- Eliminate, reduce and manage the risks in order to protect the public and regulated company personnel, the safety and security of the facilities and operations, and the protection of property and the environment.

All companies under the Board's jurisdiction are responsible for developing and maintaining an Emergency Response and Preparedness Program generically referred to as “Emergency Management Program” for all aspects of their operations. In the event an emergency occurs, the regulated company is responsible for responding to the emergency and coordinating emergency response activities.

- That result in death or serious injury;
- Involve a significant release of hydrocarbons;
- Could result in potential or real impact due to loss of service;
- Pose imminent threats identified by Public Safety and Emergency Preparedness Canada(PSEPC) or other agencies;
- Attract significant media attention, or
- On the advice of Natural Resources Canada (NRCan) or other federal Agencies.

All inter-provincial and cross border pipelines are regulated by the CER and require an Emergency Response Plan. To fully comply with the CER Onshore Pipeline Regulations (OPR) and meet CER expectations for an effective emergency preparedness program, Pieridae is required to have an emergency procedures section for the field operations and conduct emergency response training and exercises.

12.2 Roles and Responsibilities

	CANADA ENERGY BOARD	
□	Monitors, observes and assesses the overall effectiveness of the company’s emergency response in terms of: • Emergency Management • Safety • Security • Environment • Integrity of operations and facilities, and • Energy Supply.	CANADA ENERGY BOARD
□	Investigates the event, either in cooperation with the Transportation Safety Board of Canada, under the Canada Labour Code, or as per the Canada Energy Board Act or Canada Oil & Gas Operations Act (whichever is applicable).	
□	Inspects the pipeline or facility.	
□	Examines the integrity of the pipeline or facility	
□	Requires appropriate repair methods are being used.	
□	Requires appropriate environmental remediation of contaminated areas is conducted.	
□	Coordinate stakeholders and Aboriginal community feedback regarding environmental clean-up and remediation.	
□	Confirms that a company is following its Emergency Procedures Manual(s), commitments, plans, procedures, and CER regulations and identifies non-compliances.	
□	Initiates enforcements action as required.	
□	Approves the restart of the pipelines.	

12.3 CER Definitions of Incident and Emergency

Incident

For the purposes of these expected elements, as incident is considered to be "incidents and releases" (including and discharge, spray, leak, seep, pour, emit, dump and exhaust) that are defended and reportable to the CER under sections 1 and 52 of OPR-99. These are:

- The death of or serious injury to a person;
- Releases that may have significant adverse impact on the environment;
- Unintended fire or explosion;
- Unintended or unexplained release of gas or HVP hydrocarbons; and
- Operation of a pipeline beyond its design limits as defined by CSA Z662, CSA Z276 or any operating limits imposed by the CER."

Although incidents are defined in OPR-99, it is also necessary for companies to have a clear understanding of what constitutes incidents and emergencies at their facilities, as well as methods or procedures for determining the magnitude and levels of an emergency as circumstances change.

Emergency

Can/CSA – Z731 defines an emergency as "a present or imminent event that requires prompt co-ordination of actions or special regulation of persons or property to protect the health, safety or welfare of people or to limit damage to property and the environment".

Companies must consider all probable emergencies and have applicable procedures in place to deal with potential effects and treats to people, property and the environment, as determined through a formal hazard assessment.

Level 1	Level 2	Level 3
• NO effects outside company property • Control of Hazardous substance completed or pending • No immediate threat to the public or company personnel • Minimal environmental effects • Incident / Spill handled by company personnel • Low potential to escalate	• No immediate threat outside company property but potential exists to extend beyond property boundaries • Outside services and government agencies likely to be directly involved • Imminent control of hazardous substance probable • Some injury or threat to the public and company personnel • Moderate environmental effects	• Serious injury to the public and company personnel and ongoing treat to the public • Uncontrolled release of hazardous substance continuing • Significant and ongoing environmental effects • Immediate and significant government agency involvement • Assistance from outside parties required • Effects extend beyond company property

12.4 CER Incident Reporting

As defined in Section 52 of the CER's Onshore Pipeline Regulation:

(1) A company shall immediately notify the Board of any incident relating to the construction, operation or abandonment of its pipeline and shall submit a preliminary and detailed incident report to the Board as soon as practicable.

(2) After notification of an incident, an inspection officer may partially or completely relieve a company from the requirement to submit a preliminary and detailed incident report.

As soon as practicable after becoming aware of an incident (typically within 1 hour), a company should communicate all available factual information to the TSB. To correct any information provided previously or to provide additional information, a company should file a preliminary incident report, which should:

- Describe the incident, including the events leading up to and following the incident.
- List all relevant agencies contacted and persons affected by the incident.
- Summarize any losses or impacts to people (e.g., injury, fatalities), environment (e.g., terrain, habitats, and animals), production (e.g., interruption or reduction in service) and property.
- Identify any unsafe acts or conditions contribution to or causing the incident.
- Provide details on any emergency response.
- State any corrective actions taken or planned to be taken to minimize the effects of the incident.

A detailed incident report should correct any information provided in the preliminary incident report and/or provide additional information. The detailed incident report should:

- Provide any details regarding the failure mechanism and detailed analysis of the failed component (if necessary).
- Identify the underlying causes and contributing factors of the incident.
- Update the progress of any corrective actions taken or planned to be taken to minimize the effects of the incident.
- State any actions taken or planned to be taken to prevent a similar incident.

The task of completing the notifications will be completed by the Company's CEOC Liaison Officer. For the detailed report use the CER Detailed Reporting Form on the following pages.

The Transportation Safety Board of Canada (TSB) has the option to choose to be the lead investigator for determining the cause and contributing factors leading to an incident/ emergency.

12.5 Published Manuals

All companies operating an oil or a gas pipeline under the jurisdiction of the Board must:

1. Unless the Board otherwise directs, publish the entirety of their emergency procedures manuals on their company's public internet site; provided however, manuals are not required to be published for pipelines described in the exemption clause below. Companies may protect from publication the following information:
   a. an identifiable individual, including their name, phone number, email address, mailing address and medical condition;

   b. the vulnerability of particular structures, including methods employed to protect those structures;
   c. that could prejudice their competitive position or reasonably be expected to result in a material loss or gain to a person affected by publication; and
   d. about a person, such as a daycare, school or hospital, that was requested by that person to be withheld from publication;
2. Describe information that is protected from publication; and
3. File a written confirmation from the company's accountable officer that the company's emergency procedures manuals have been published and provide a link to the published manuals to the Board and to any interested person that has expressed an interest to the company in the published manuals.

Exemption Clause

Pipelines described in this section are exempt from publication.

High vapour pressure pipelines that are:

1. 168 millimeters or less in outside nominal diameter;
2. 10 kilometres or less in length; and
3. Outside of class 2 or greater locations, as determined by CSA Z662.

Liquid pipelines that are:

1. 168 millimeters or less in outside nominal diameter;
2. 10 kilometres or less in length; and
3. Located more than 500 metres from a navigable water, public drinking water source or a designated environmentally sensitive area.

12.6 Transportation Safety Board

The Transportation Safety Board of Canada (TSB) has a mandate to advance transportation safety in the marine, pipeline, rail and air modes of transportation.

The CER and the TSB have adopted a single window reporting approach for inter-provincial or cross border pipelines. The new Online Event Reporting System (OERS) automates the single-window pipeline occurrence notification process that was established by the TSB and the CER.

A. Roles and Responsibilities

TRANSPORTATION SAFETY BOARD	
❑	Conduct independent investigations, including public inquiries when necessary, into selected transportation occurrences in order to make findings as to their causes and contributing factors.
❑	Identify safety deficiencies, as evidenced by transportation occurrences.
❑	Make recommendations designed to eliminate or reduce any such safety deficiencies.
❑	Report publicly on their investigations and on the findings in relation thereto.

TSB

B. TSB Pipeline Occurrence Reporting

Requirement to Report

A "pipeline occurrence" must be reported if it results directly from the operation of the pipeline, where

1. a person is killed or sustains a serious injury;
2. the safe operation of the pipeline is affected by
    1. damage sustained when another object came into contact with it, or
    2. a fire or explosion or an ignition that is not associated with normal pipeline operations;
3. an event or an operational malfunction results in
    1. an unintended or uncontrolled release of gas,
    2. an unintended or uncontrolled release of HVP hydrocarbons,
    3. an unintended or uncontained release of LVP hydrocarbons in excess of 1.5 m^3, or
    4. an unintended or uncontrolled release of a commodity other than gas, HVP hydrocarbons or LVP hydrocarbons;
4. there is a release of a commodity from the line pipe body;
5. the pipeline is operated beyond design limits or any operating restrictions imposed by the Canada Energy Board;
6. the pipeline restricts the safety operation of any mode of transportation;
7. an unauthorized third party activity within the safety zone poses a threat to the safe operation of the pipeline;
8. a geotechnical, hydraulic or environmental activity poses a threat to the safe operation of the pipeline;
9. the operation of a portion of the pipeline is interrupted as a result of a situation or condition that poses a threat to any person, property or the environment; or
10. an unintended fire or explosion has occurred that poses a threat to any person, property or the environment.

Source: *Transportation Safety Board Regulations Section 4(1)*

Input the information you have as soon as possible after the occurrence

As soon as possible after the occurrence, enter the information you have about it into the Online Event Reporting System (OERS). When the information is submitted, the OERS will automatically notify the TSB and the CER.

Information must be entered in the OERS even if you have reported the occurrence by telephone.

Enter factual information only. Information that is considered a witness statement and/or personal information must not be entered in the OERS.

Submit additional information as soon as available

Provide the remainder of the information required by the TSB through the OERS as soon as it becomes available and no later than 30 days after the occurrence.

If you have any questions or concerns about using the Online Event Reporting System for reporting occurrences to the TSB, call the TSB.

Online Event Reporting System (OERS)

https://apps.CER-one.gc.ca/ERS/Home/Index/

12.7 Transport Canada

A railway carrier must immediately report any potential threat or other security concern by telephone to the Transports Canada Situation Centre. Potential threats and other security concerns include:

1. Any interference with a train crew:
2. Any bomb threats, either specific or non-specific;
3. Any reports or discoveries of suspicious items when the report or discovery results in a disruption of railway operations;
4. Any suspicious activities observed on or near a railway vehicle, at or near infrastructure used in railway operations or at or near a facility or location used in railway operations;
5. The discovery, seizure or discharge of a firearm or other weapon on or near a railway vehicle, at or near infrastructure used in railway operations or at or near a facility or location used in railway operations;
6. Any signs of tampering with a railway vehicle if a railway carrier determines that security has been compromised; and
7. Any information relating to a possible surveillance of a railway vehicle, or infrastructure used in railway operations or at or near a facility or location used in railway operations.

The report must include, if applicable and to the extent known, the following information:

1. The rail carrier’s name and contact information, including telephone number and email address;
2. The name of the person who is making the report on behalf of the railway carrier and the person’s title and contact information, including telephone number and email address;

3. Any information that identifies any train that is affected by the potential threat or other security concerns, including its itinerary and line or route position;
4. The classification and quantity of any dangerous goods that are involved in the potential threat or other security concern; and
5. A description of the potential threat or other security concern, including the date and time that the railway carrier became aware of it and the date and time of any incident linked to it.

In Pieridae Energy context we are not a rail carrier we are a loader, so it is the requirement of the carrier to report any potential threat. As loader we would only report if carrier was unable or in emergency situations. The Transport Canada Situation Center contact number is: 1-888-857-4003

12.8 External Communications - Alberta

12.7.1 *Government Notification and Call-Down System*

Alberta INCIDENT TYPE / AGENCY OR	Initial Responders			Lead Agencies				Other Government Contacts							Support Services
	Ambulance Services	**Local Fire Department or Industrial Fire Service**	**Police**	**AER**	**Local Authorities (i.e. urban centres, MDs, and first nations reserves)**	**AEP - Spill Reporting Line**	**AHS - Alberta Health and Safety[1]**	**Alberta Occupational Health and Safety**	**Workers' Compensation Board**	**AEMA - Alberta Emergency Management Agency**	**ABSA - Alberta Boilers Association**	**Alberta Agriculture and Forestry[2]**	**Alberta Safety Services - Electrical Branch**	**Alberta Ministry of Transportation[3]**	**Oil Spill Cooperative (WCSS)**
Sour Gas Release			✓	✓	✓	✓	✓			✔		✓		✓	
Sweet Combustible Gas Release			✓	✓	✓	✓	✓			✔		✓		✓	
Spill - Unrefined Products*				✓	✓	✓	✓			✔		✓		✓	✓
Spill - Refined Products*				✓	✓	✓	✓			✔		✓		✓	✓
Trucking/Motor Vehicle Incident			✓	✓	✓	✓								✓	
Serious Injury or Fatality (including sour gas exposure)	✓		✓	✓				✓	✓						
Fire/Explosion		✓	✓	✓	✓		✓			✔		✓		✓	
Pressure Vessel or Piping Incident				✓							✓			✓	
Electrical Incident				✓									✓	✓	
Security Incident			✓	✓										✓	

✓ Compulsory contact ✔ Request that the AER notify these agencies and services as required * Refer to the Alberta Petroleum Industry Release Reporting Requirements chart included in the ERP

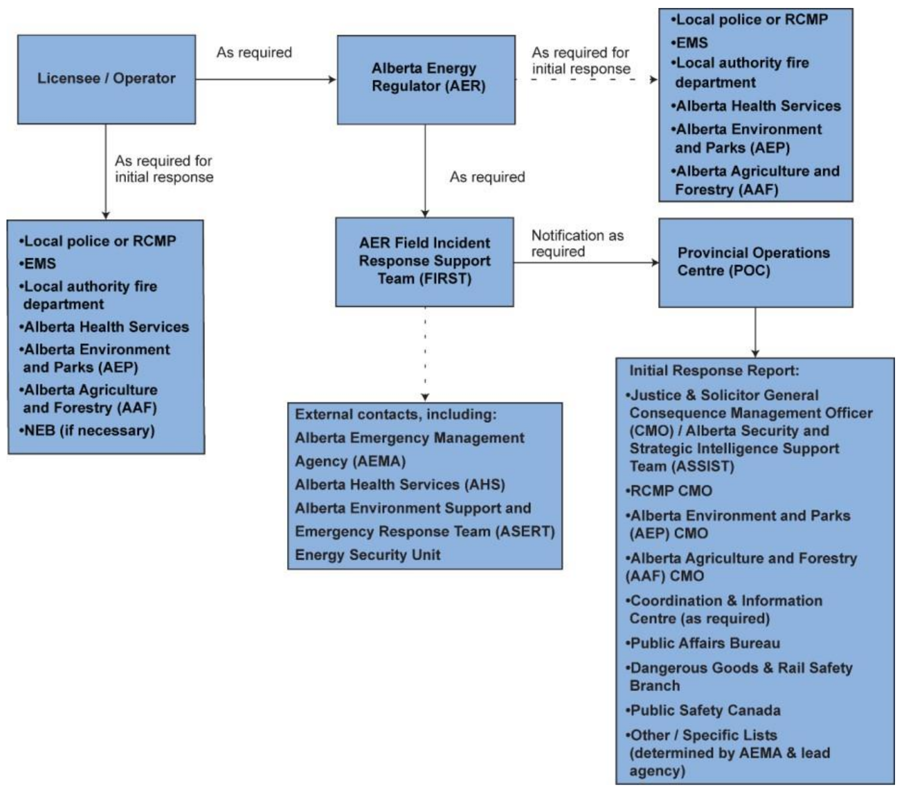
1 Contact Alberta Health Services (AHS) if the incident has the potential to impact public health
2 Contact Alberta Agriculture and Forestry for any event that could affect forested areas.
3 Contact Alberta Ministry of Transportation or the RCMP if the emergency affects a highway designated by 1, 2, or 3 digits (e.g. Hwy 2, Hwy 47, Hwy 837).

Federal INCIDENT TYPE / AGENCY OR RESOURCE	Initial Responders	Lead Agencies		Other Government Contacts					Support Services
	RCMP	**CER[1]**	**Transportation Safety Board (TSB)**	**Transport Canada**	**Environment Canada[2]**	**Indian Oil and Gas Canada**	**DFO**	**CANUTEC[3]**	**ERAC - Emergency Response Assistance Canada**
Sour Gas Release	✓	✓			✓	✓	✓		
Sweet Combustible Gas Release	✓	✓			✓	✓	✓		
Spill - Unrefined Products*		✓			✓	✓	✓	✓	✓
Spill - Refined Products*		✓			✓	✓	✓	✓	✓
Trucking/Motor Vehicle Incident	✓				✓				✓
Marine, pipeline, rail and air modes			✓						
Serious Injury or Fatality (including sour gas exposure)	✓	✓				✓			
Fire/Explosion	✓	✓			✓	✓			
Pressure Vessel or Piping Incident		✓			✓				
Electrical Incident		✓			✓				
Security Incident	✓	✓							
Railway Security Threat				✓					

✓ Compulsory contact

1 Contact the Canada Energy Board (via the Transportation Safety Board of Canada) for emergencies involving CER regulated sites and inter-provincial pipelines.
2 Contact Environment Canada for incidents involving spills on first nation's lands, in National Parks, into river or lake systems containing fish or onto railway rights-of-way.
3 Contact the Canadian Transport Emergency Centre (CANUTEC) if information is required about handling procedures for toxic material releases.

Incident Notification Process



Licensee / Operator
As required
Alberta Energy Regulator (AER)
As required for initial response
- Local police or RCMP
- EMS
- Local authority fire department
- Alberta Health Services
- Alberta Environment and Parks (AEP)
- Alberta Agriculture and Forestry (AAF)

As required for initial response
- Local police or RCMP
- EMS
- Local authority fire department
- Alberta Health Services
- Alberta Environment and Parks (AEP)
- Alberta Agriculture and Forestry (AAF)
- NEB (if necessary)

As required
AER Field Incident Response Support Team (FIRST)
Notification as required
Provincial Operations Centre (POC)

External contacts, including:
Alberta Emergency Management Agency (AEMA)
Alberta Health Services (AHS)
Alberta Environment Support and Emergency Response Team (ASERT)
Energy Security Unit

Initial Response Report:
- Justice & Solicitor General Consequence Management Officer (CMO) / Alberta Security and Strategic Intelligence Support Team (ASSIST)
- RCMP CMO
- Alberta Environment and Parks (AEP) CMO
- Alberta Agriculture and Forestry (AAF) CMO
- Coordination & Information Centre (as required)
- Public Affairs Bureau
- Dangerous Goods & Rail Safety Branch
- Public Safety Canada
- Other / Specific Lists (determined by AEMA & lead agency)

12.7.2 *Alberta Energy Regulator (AER)*

The AER ensures the safe, efficient, orderly, and environmentally responsible development of hydrocarbon resources over their entire life cycle. This includes allocating and conserving water resources, managing public lands, and protecting the environment while providing economic benefits for all Albertans.

The AER will provide full-lifecycle regulatory oversight of energy resource development in Alberta - from application and construction to abandonment and reclamation, and everything in between.

The AER is the lead government agency that initiates and oversees government response. The AER can provide assistance to alert other applicable government and emergency response agencies.

	ALBERTA ENERGY REGULATOR	
❑	Acts as lead provincial government organization in petroleum industry emergency responses.	**ALBERTA ENERGY REGULATOR**
❑	Review and approve licensee ERPs.	
❑	Participate in selected licensee ERP exercises.	
❑	Review and recommend changes to ERPs.	
❑	Participate in validation and testing of ERPs.	
❑	Maintain a 24 hour emergency contact number where resources can be accessed for a response related to Emergency Response Plans.	
❑	Receive information pertaining to petroleum industry incidents.	
❑	Determine the emergency level of an incident through consultation with the licensee.	
❑	Dispatch AER representative to the site of the incident, as required.	
❑	Confirm that local resources have been notified as appropriate.	
❑	Identify and request initial provincial resources to support the incident, to be coordinated at the regional level if necessary through the REOC.	
❑	Notify CIC to carry out notification in accordance with this plan.	
❑	Confirm, plan and/or implement public safety actions taken to ensure the safety of the public and the environment, including issuing fire hazard orders or requesting NOTAMs.	
❑	Provide Situation Reports to AEMA if requested.	
❑	Send AER representative to the On-Site Command Post.	
❑	Establish an EOC at the local AER Field Centre until the licensee or local authority establishes a MEOC.	
❑	Dispatch an AER Regulatory Liaison to the MEOC or POC and issue timely media releases in conjunction with the licensee and PAB.	
❑	Request, through AEMA, the deployment of the other provincial Government staff be sent to the MEOC or the local Field Centre EOC.	
❑	Request a local authority liaison officer to be present at the MEOC if necessary.	
❑	Carry out investigations.	
❑	Provide timely situation reports, through AEMA, to other Government departments activated by this plan.	
❑	Notify all participants when the event has concluded and there is no longer any hazard to the public.	
❑	Complete reporting protocols.	
❑	As part of the lessons-learned process, recommend any mitigating actions that may reduce the event from re-occurring.	
❑	Establish processes to receive and address community concerns.	
❑	In consultation with AEMA, review and recommend updates for the ERP.	

12.7.3 *Alberta Utilities Commission*

The Alberta Utilities Commission works in concert with the AER as an “appropriate regulatory body” meaning that the Alberta Utilities Commission, with respect to a critical facility that is a gas utility pipeline, hydro development, power plant, transmission line or electric distribution system, will also provide direction to operators.

Threat of Terrorist Activity - Alberta

Where the appropriate regulating body (CER, Alberta Utilities Commission, AER) has been informed of the existence of a threat of terrorist activity against a well or facility, pipeline, gas utility pipeline, in situ operation, mining operation or processing plant, mine or coal processing plant, hydro development, power plant, transmission line or electric distribution system, the appropriate regulating body shall

- Inform the licensee or approval holder of the threat of terrorist activity and the level of threat, and
- Request the licensee or approval holder to provide information about the manner in which the licensee or approval holder will address the threat.

Where the threat of terrorist activity is high or imminent against a well, facility, pipeline, gas utility pipeline, in situ operation, mining operation, processing plant, mine, coal processing plant, hydro development, power plant, transmission line or electric distribution system, and the appropriate regulating body is of the view after consultation with the licensee or approval holder that the licensee or approval holder is unwilling or unable to take measures to address the threat, the appropriate regulating body may

- Order the licensee or approval holder to shut in the well or shut down the facility, pipeline, gas utility pipeline, in situ operation, mining operation, processing plant, mine, coal processing plant, hydro development, power plant, transmission line or electric distribution system and set out the terms under which the order may cease, or
- Take the necessary action to shut in the well or shut down the facility, pipeline, gas utility pipeline, in situ operation, mining operation, processing plant, mine, coal processing plant, hydro development, power plant, transmission line or electric distribution system and recover the costs incurred by the appropriate regulating body to take action from the licensee or approval holder as a debt owed to the appropriate regulating body.

12.7.4 *Alberta Emergency Management Agency*

The Alberta Emergency Management Agency is a division of the Ministry of Municipal Affairs and Housing. AEMA leads the coordination, collaboration and co-operation of all organizations involved in the prevention, preparedness, and response to disasters and emergencies.

AEMA has its headquarters in Edmonton and incorporates several domains of practise which encompass; emergency response, disaster recovery programs, business continuity, government ERPs, grants and funding, and municipal wildfire assistance programs.

The AEMA management structure is divided into two divisions: Provincial Operations, and Public Safety initiatives. Each separate division has five separate branches who report to an executive director. A Director oversees all activities of the Agency.

AEMA maintains a 24 hour a day, 7 day a week Agency Response and Readiness Centre (AARC) that monitors and maintains contact with various regional and local authorities. This centre is the central point of contact for the collection, evaluation, and dissemination concerning a single incident or for multiple incidents. The centre is responsible for co-ordinating an initial response at which time it will change roles into an active management centre known as the Provincial Operations Centre (POC). The POC is responsible for establishing and maintaining contacts with federal assistance and agencies.

	ALBERTA EMERGENCY MANAGEMENT AGENCY	
□	Act as the provincial coordinating agency in petroleum industry emergency responses as per the Emergency Management Act.	**ALBERTA EMERGENCY MANAGEMENT AGENCY**
□	Make the plan available to stakeholders.	
□	Train provincial personnel to carry out functions as assigned by their emergency plan or procedures.	
□	Communicate changes to the plan with plan holders.	
□	Maintain 24 hour a day, 7 day a week duty manager system.	
□	Assist in the planning and coordination of exercises with the AER.	
□	Confirm AER has been notified.	
□	Conduct the Initial Response Report (IRR) notification.	
□	Obtain a situation report from the AER, AEP, local authority, etc.	
□	Confirm the level of emergency.	
□	Activate the Provincial Operations Centre (POC) as required.	
□	Notify the appropriate provincial officials as per standard operating procedures.	
□	Release consolidated SITREPs in accordance with the Petroleum Industry Incident Support Plan (PIISP).	
□	Coordinate the Government of Alberta response including requests for provincial/federal resources.	
□	Provide ongoing situation reports or briefing notes to appropriate provincial officials.	
□	Notify partners and stakeholders when the event is over.	
□	Conduct the post-incident assessment.	
□	Communicate any changes to the plan to all plan holders.	
□	Complete documentation or reporting in relation to the activation of the PIISP and the incident.	

12.7.5 *Provincial Operations Centre (POC)*

The Provincial Operations Centre (POC) serves as a communication and response coordination centre that is staffed 24 hours a day, 7 days a week. The POC is a central point for the collection, evaluation and dissemination of information concerning a single incident or multiple incidents in the province of Alberta. The POC is responsible for coordinating the initial response and maintaining support for a response to a natural or human-induced disaster.

The Alberta Provincial Emergency Operations Centre (POC) set up under the Government's Response Readiness Plan will provide notification by radio, television, or other practical means. The Company shall have a representative at the POC to assist as liaison. The broadcast media (radio, television) will be used to notify residents outside the EPZ in the event of an immediate evacuation of the area.

12.7.6 *Alberta Solicitor General and Public Security*

	ALBERTA JUSTICE AND SOLICITOR GENERAL	SOLICITOR GENERAL
❑	Maintain the list of critical infrastructure in the Province of Alberta.	
❑	Maintain and regularly test the emergency notification system.	
❑	Maintain awareness of threats, vulnerabilities, and risks related to human induced intentional hazards.	
❑	Notify Government department of concerns arising from the effects of the incident on critical infrastructure.	
❑	Advise other Government departments of modifications to procedures if the incident was intentionally caused.	
❑	Provide technical expertise to all stakeholders in the event of an intentional incident and advise appropriate Government officials of potential future targets.	
❑	Ensure that effects on critical infrastructure have been resolved.	
❑	Recommend changes to critical infrastructure plans to mitigate future events.	

12.9 External Communications – British Columbia

12.8.1 *Government Notification and Call-Down System*

British Columbia INCIDENT TYPE	Initial Responders			Lead Agencies					Other Government Contacts					Support Services
AGENCY OR RESOURCE	Ambulance Services	Local Fire Department or Industrial Fire Service	Police	EMBC	OGC	Ministry of Environment	Local Authorities	Local Health Authority[1]	WorkSafe BC	BC Safety Authority	BC Ministry of Forests, Lands and Natural Resource Operations[2]	Ministry of Transportation[3]	Electrical Provider	Oil Spill Cooperative (WCSS)
Sour Gas Release			✓	✓	✓	✓	✓	✓			✓	✓		
Sweet Combustible Gas Release			✓	✓	✓	✓	✓	✓			✓	✓		
Spill - Unrefined Products*				✓	✓	✓	✓	✓			✓	✓		✓
Spill - Refined Products*				✓	✓	✓	✓	✓			✓	✓		✓
Trucking/Motor Vehicle Incident			✓	✓	✓	✓	✓					✓		
Serious Injury or Fatality (including sour gas exposure)	✓		✓	✓					✓					
Fire/Explosion		✓	✓	✓	✓		✓	✓		✓	✓	✓		
Pressure Vessel or Piping Incident				✓								✓		
Electrical Incident				✓							✓	✓	✓	
Security Incident			✓	✓								✓		

✓ Compulsory contact * Refer to the British Columbia Petroleum Industry Release Reporting Requirements chart included in the ERP

[1] Contact the Local Health Authority if the incident has the potential to impact public health

[2] Contact BC Ministry of Forests, Lands and Natural Resource Operation for any event that could affect forested areas.

[3] Contact British Columbia Ministry of Transportation or the RCMP if the emergency affects a highway designated by 1, 2, or 3 digits (e.g. Hwy 2, Hwy 47, Hwy 837).

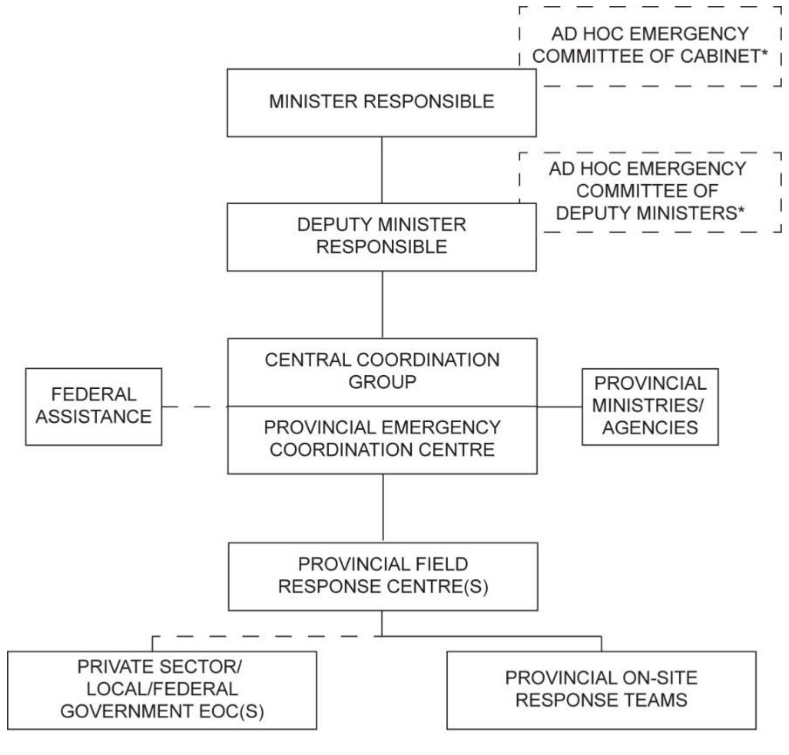
Federal INCIDENT TYPE	Initial Responders	Lead Agencies	Other Government Contacts					Support Services
AGENCY OR RESOURCE	RCMP	CER[1]	Transportation Safety Board (TSB)	Environment Canada[2]	*Indian Oil and Gas Canada*	DFO	CANUTEC[3]	ERAC - Emergency Response Assistance Canada
Sour Gas Release	✓	✓		✓	✓	✓		
Sweet Combustible Gas Release	✓	✓		✓	✓	✓		
Spill - Unrefined Products*		✓		✓	✓	✓	✓	✓
Spill - Refined Products*		✓		✓	✓	✓	✓	✓
Trucking/Motor Vehicle Incident	✓			✓				✓
Marine, pipeline, rail and air modes			✓					
Serious Injury or Fatality (including sour gas exposure)	✓	✓			✓			
Fire/Explosion	✓	✓		✓	✓			
Pressure Vessel or Piping Incident		✓		✓				
Electrical Incident		✓		✓				
Security Incident	✓	✓						

✓ Compulsory contact

[1] Contact the Canada Energy Board (via the Transportation Safety Board of Canada) for emergencies involving CER regulated sites and inter-provincial pipelines.

[2] Contact Environment Canada for incidents involving spills on first nations lands, in National Parks, into river or lake systems containing fish or onto railway rights-of-way.

[3] Contact the Canadian Transport Emergency Centre (CANUTEC) if information is required about handling procedures for toxic material releases.


AD HOC EMERGENCY COMMITTEE OF CABINET*
MINISTER RESPONSIBLE
AD HOC EMERGENCY COMMITTEE OF DEPUTY MINISTERS*
DEPUTY MINISTER RESPONSIBLE
FEDERAL ASSISTANCE
CENTRAL COORDINATION GROUP
PROVINCIAL EMERGENCY COORDINATION CENTRE
PROVINCIAL MINISTRIES/ AGENCIES
PROVINCIAL FIELD RESPONSE CENTRE(S)
PRIVATE SECTOR/ LOCAL/FEDERAL GOVERNMENT EOC(S)
PROVINCIAL ON-SITE RESPONSE TEAMS

*AD HOC COMMITTEE THAT MAY BE FORMED IN THE EVENT OF A SEVERE EMERGENCY OR CATASTROPHIC EVENT.

12.8.2 *Provincial Regional Emergency Operations Centre (PREOC)*

The Provincial Regional Emergency Operations Centre manages activities at the Provincial Regional Coordination Level and coordinates the joint efforts of government and non-government agencies.

If the situation escalated beyond OGC control, EMBC may establish a Provincial Regional Emergency Operations Centre (PREOC) near the emergency site to coordinate provincial response. The PREOC also keeps elected provincial officials informed through personal contacts and briefing notes.

12.8.3 *Oil and Gas Commission*

The OGC is a Crown Corporation of the province of British Columbia whose mandate is to regulate oil and gas activities and pipelines in the province. It is the petroleum authority that will participate in the emergency response to all situations involving or threatening oilfield wells, production facilities, or pipelines in British Columbia.

In an emergency the OGC would be notified by EMBC, however, as EMBC works on a priority basis, the Company should take action and contact the OGC personally.

	OIL AND GAS COMMISSION	**OIL AND GAS**
❑	Oversee the operator’s response to an incident.	
❑	Establish communication with the operator.	
❑	Confirm incident level with operator.	
❑	Confirm downgrade of incident level.	
❑	Issue road closure order upon request from the operator.	
❑	Request NOTAM order from NAV Canada upon request from the operator.	
❑	Send an OGC representative to the Operator’s On-Site Command Post and/or Evacuation Centre.	
❑	Establish a government EOC at the OGC office.	
❑	Confirm ignition decision with operator if time permits.	
❑	Confirm media releases to be sent out by operator.	

12.8.4 *OGC Pipeline Incident Report*

Non-CER regulated security incidents that affect a Company’s facilities / pipelines or wells are to be reported to the OGC via **EMBC 24 Hour emergency telephone number (1-800-663-3456)** as well as through completion of the OGC Pipeline Incident Report (See Form #3).

12.8.5 *Emergency Management British Columbia (EMBC)*

Emergency Management BC (EMBC) was formed to be the lead coordinating agency in the provincial government for all emergency management activities. EMBC provides executive coordination, strategic planning, and multi-agency facilitation and strives to develop effective working relationships in an increasingly complex emergency management environment.

EMBC works with local governments, First Nations, federal departments, industry, non-government organizations and volunteers to support the emergency management phases of mitigation/ prevention, preparedness, response and recovery. Additionally, EMBC engages provincial, national and international partners to enhance collective emergency preparedness.

The EMBC acts as a 24 hour incident reporting line and initiates government notification fan-out by notifying the OGC, Ministry of Environment and Environment Canada.

13.0 TELEPHONE DIRECTORY

13.1 Corporate Telephone List

Pieridae Energy Limited	
24 Hour Emergency Telephone Number	**1-866-267-5298**
Company Main Telephone Number	**403-261-5900**
Field Office Telephone Number	**1-780-827-4178**
Company Main Office Address	**3100, 308 – 4th Avenue SW** **Calgary, AB T2P 0H7**
Company Main Facsimile Number	**403-261-5902**

Name	Position	Office	Cell
Yvonne McLeod	VP Drilling, Completions & HSE	403-351-5427	403-921-7744
Carolyn Normand	VP Engineering	587-392-9394	403-598-3188
Ken Scheirer	Development Engineering Manager	403-351-4030	403-826-0200
Jason Praise	Facilities Engineering Manager	587-392-9376	
Petra Struck	Sr. Engineering Technician	403-351-4033	403-830-2263
Vacant	VP Exploration		
Rich Rowe	VP Land	403-351-5420	403-512-2160
Vacant	Operations Manager		
Darcy Reding	Chief Operating Officer	403-351-5427	403

13.2 Field Personnel Telephone List

Name	Position	Office	Cell	Other
NORTHERN ALBERTA and BRITISH COLUMBIA				
Josh Storle	Northern Foothills Foreman		1-780-897-0851	
Palliser	Dehydrator Control Room	1-780-827-4178		
Dwayne Stuart	Op #2 Ekwan/Sierra	1-403-685-2459	1-306-737-8798	
James Leckie	Op #2 Ekwan/Sierra	1-403-685-2459	1-403-620-2459	
CENTRAL ALBERTA NORDEGG				
Trevor Prenevost	Central Foothills Foreman	1-403-685-2449	1-403-846-0526	
Devin Prins	Lead Operator		1-403-846-6941	
CAROLINE GAS PLANT				
Mark Weiss	Superintendent, Caroline	1-587-392-9398	1-403-542-3004	
John Fordham	Plant Foreman, Caroline	1-587-392-9367		
Billy Joe Jensen	Field Foreman, Caroline	1-587-392-9353	1-403-559-7373	
Clair Crosbie	Maintenance Foreman Caroline	1-587-392-9358	1-403-998-6376	

SHANTZ SULPHUR PLANT				
Paul Smith	Shantz Foreman	1-587-392-9402	1-403-638-1452	
JUMPING POUND GAS PLANT				
Conrad Kenny	Superintendent, Jumping Pound	1-587-392-9360	1-403-472-5593	
Dan Flynn	Plant Foreman, Jumping Pound	1-587-392-9361	1-403-829-7723	
Matthew Gartner	Field Foreman, Jumping Pound	1-587-392-9393	1-403-472-5017	
Mike Carr	Maintenance Foreman, Jumping Pound	1-587-392-9397	1-403-816-0100	
WATERTON GAS PLANT				
Darrell Archibald	Superintendent, Waterton	1-587-392-9364	1-403-652-5055	
Randy Urlacher	Plant Foreman, Waterton	1-587-392-9404	1-403-638-7984	
Lorne Harty	Field Foreman, Waterton	1-587-392-9388	1-403-888-3153	
Jason Jacobs	Maintenance Foreman, Waterton	1-587-392-9375	1-778-256-1197	

13.3 Security Services Contact List

Agency	Location	Telephone
ALBERTA		
Calgary Security Services www.calgarysecurityservices.calls.net	Calgary	1-587-331-8288
Paladin Security	Calgary	1-403-508-1888
Securitas www.securitas.ca/en-CA/	Calgary Toll Free Edmonton	403- 273-0337 1-877-770-3456 780-429-9695
Paladin Security	Grande Prairie	1-780-539-1152
All Peace Protection www.allpeaceprotection.com	Grande Prairie	1-780-538-1166
BRITISH COLUMBIA		
Action Health and Safety Services www.actionservices.ca	Toll-free Dawson Creek	1-888-782-8204 1-250-782-8202
Armada Security www.armadasecurity.ca	Dawson Creek	1-250-784-0717
All Peace Protection www.allpeaceprotection.com	Grande Prairie	1-780-538-1166

13.4 Agency Contact List – Alberta

Resource	Contact	Office	Cell/24 Hour
Alberta Energy Regulator	Environmental Emergency or Complaint	---	1-800-222-6514
	Inquiry Line		1-855-297-8311
	Grande Prairie	1-780-538-5138	
	24/7 Media Centre	-	1-855-474-6356
MD of Greenview	Jeff Francis Dir. of Disaster Services	1-780-524-7600	1-866-524-7608
RCMP (Grande Prairie)	NCO In Charge		911
Alberta Health Services, North Zone	Shane Hussey Manager of Environmental Health Program	1-780-841-3275	1-800-732-8981 Ask for the EPH on-call.
Alberta Emergency Management Agency	Emergency Management Field Officer		1-866-618-2362
Alberta Environment and Parks	Environmental Emergencies		1-800-222-6514
Alberta Agriculture and Forestry	Ag-Info Centre		310-FARM (310-3276)
Forest Fires - to report a wildfire	Province-wide	--	310-3473
Alberta Occupational Health and Safety	Province-wide	1-866-415-8690	1-866-415-8690
Alberta Infrastructure and Transportation	Province-wide	1-780-427-2731 Transportation 1-780-415-0507 Infrastructure	1-800-272-9600
Highway Maintenance Contractor			Phone
Alberta One Call	Province-wide	--	1-800-242-3447
Poison Centre	Province-wide	--	1-800-332-1414
Alberta Boilers Safety Association	Edmonton	--	1-780-437-9100 Monday - Friday 8 AM - 4:30 PM
Dial toll-free for Government Agencies	Province -wide	--	310-0000 then 10 digit number or 0 for operator

13.5 Agency Contact List – British Columbia

Resource	Contact	Office	Cell/24 Hour
Emergency Management B.C. (EMBC)	Emergency Coordination Centre	1-800-663-3456	1-800-663-3456
BC Oil and Gas Commission	On Call Emergency Coordinator Incident Reporting Line	1-250-794-5200 1-800-663-3456	1-250-794-5200 1-800-663-3456
Peace River Regional District	Dan Ross Protective Services Manager	1-250-784-3215	1-800-670-7773
RCMP (Dawson Creek)	NCO in Charge		911
Northern Health Authority	Dawson Creek - Environmental Health Office	1-250-719-6500	1-250-565-2000 Ask for the Medical Health Officer on call.
Ministry of Environment (Peace Region)	Terry Sawchuck Emergency Response Officer	1-250-787-3391	1-800-663-3456
Ministry of Forests, Lands and Natural Resource Operations - Peace Forest District	Greg Vandolah Acting District Manager	1-250-787-3415	1-250-784-1200
WorkSafe B.C.	Occupational Safety Officer Report a serious injury or fatality during business hours After hours (toll free)	1-250-785-1283 1-888-621-7233 (SAFE) 1-866-922-4357 WCB-HELP	1-800-663-4630
Ministry of Transportation and infrastructure - Peace District	Maria Butts District Manager	1-250 787-3237	1-888-883-6688 (works in BC only)
Caribou Road Services (South) Ltd.	Tumbler Ridge Area	1-250-242-4388	1-800-667-2322
BC One Call	Province-wide	1-800-474-6886	--
Drug and Poison Information Centre	Province-wide	1-604-682-5050	1-800-567-8911
Report a Wildfire	Province-wide	--	1-800-663-5555 *5555 Cell Phone
BC Safety Authority	Province-wide	1-866-566-7233	--
BC Hydro	Province-wide	1-888-POWERON (1-888-769-3766) *49376 Cell Phone	--

13.6 Federal Agencies and Emergency Support

Resource	Contact	Office	Cell/24 Hour
Environment Canada - Environmental Emergency Reporting Line	Province -wide	--	1-800-222-6514
CN Railways - CN Police	Canada-wide	--	1-800-465-9239
CP Railways - CP Police	Canada-wide	--	1-800-716-9132
CANUTEC TDG - Emergency Reporting Line	Canada-wide	--	1-888-CAN-UTEC (226-8832)
Transportation Safety Board (CER Regulated Pipeline Emergencies)	Canada-wide	--	1-819-997-7887
Transport Canada	Canada-wide	1888-675-6863	1-888-857-4003
Canada Energy Board (CER Regulated Facilities)	Canada-wide	--	1-403-807-9473
NAV Canada	Canada-wide	--	1-800-876-4693

14.0 FORMS

FORM # 1	CER DETAILED INCIDENT REPORT
FORM # 2	FIRST CALL COMMUNICATION FORM
FORM # 3	BC INCIDENT NOTIFICATION REPORT

14.1 FORM # 1: Canada Energy Board Detailed Incident Report

1

Canada Energy Board
Calgary, Alberta

Appendix 1
DETAILED INCIDENT REPORT
Type or print in black pen

Board Use Only

CER Incident No.______________Date Received_________________CER Investigator __________________

Investigator's Comments ____

____

____

Secretary
Canada Energy Board
517 Tenth Avenue S.W.
Calgary, Alberta T2R 0A8 • Fax: 403-292-5503

PART A - OPERATOR INFORMATION

Name of Company ____

Address of Company ____

____

Pipeline Name ____

PART B - TIME, WEATHER AND LOCATION OF INCIDENT

Date (month) (day) (year)

Hour (24 hour system & time zone)

Weather temperature: °C precipitation: wind speed & direction:

CSA Class Location ☐ 1 ☐ 2 ☐ 3 ☐ 4

Location (provide specific location using a chainage description (MLV, kmP), land survey description or prominent landmarks)

____

____

PART C - ORIGIN OF SPILL/RELEASE

Facility Involved:

☐ Line Pipe ☐ Tank Farm ☐ Pump Station ☐ Compressor Station ☐ Regulator/Meter Station ☐ Gas Plant

☐ Other Related Facility (specify) ____

Equipment Involved:

☐ Pipe ☐ Valve ☐ Pressure relief device ☐ Fitting ☐ Compressor ☐ Pump ☐ Pressure vessel ☐ Tank

☐ Instrumentation

☐ Other (specify) ____

PART D - SPILLS AND RELEASES (Report LVP and HVP spills only if in excess of 1.5 m³)

☐ Gas ☐ LVP ☐ HVP ☐ Toxic Substance

Name of product/substance ____

Volume spilled/released _________ m³ Volume recovered _________ m³

Was there a fire? ☐ Yes ☐ No Was there an explosion? ☐ Yes ☐ No

*Local reproduction of this form is permitted

PART E - IMMEDIATE CAUSE FOR INCIDENTS ON OPERATING PIPELINES (Immediate Cause: means unsafe acts or unsafe conditions)

☐ Failed pipe ☐ Operator personnel error ☐ Other (*specify*) ____________________
☐ Failed weld ☐ External loading or natural forces ____________________
☐ Corrosion ☐ Equipment malfunction/failure ____________________
Refer to part G Refer to part I ____________________

PART F - LINE PIPE DATA

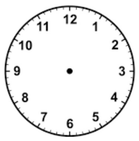
Type of Failure ____________________

Nominal Diameter (mm)__________Wall Thickness (mm)__________Date of Manufacture __________
Weld Process____________________SMYS (MPa) ________
Pipe Specification ☐ Z 245 ☐ Other (specify) Pipe Location: ☐ Below Ground ☐ Above Ground
Maximum Operating Pressure (kPa)__________Pressure at Time of Incident (kPa) __________

PART G - CORROSION FAILURES

Corrosion location: ☐ Internal ☐ External
Type of Corrosion (*specify*)____________________
Type of Coating____________________

Circumferential Position Looking Downstream
(mark an X)



PART H - FAILURES DUE TO EXTERNAL LOAD OR NATURAL FORCES

☐ Damage by operator or its contractor ☐ Damage by other parties ☐ Earth movement ☐ Lightning/Fire
☐ Other (specify) ____________________
Name or Contractor/Other Party ____________________
Address____________________
Telephone ( )____________________Name of Representative ____________________

PART I - EQUIPMENT MALFUNCTION/FAILURE

Equipment____________________Manufacturer____________________Model# __________
Year Equipment Installed____________________Year Equipment Manufactured __________

PART J - ESTIMATE OF TOTAL INCIDENT COST (Including repair, cleanup and restoration)

$

PART K - REPAIR DESCRIPTION (Description of all repairs to the pipeline made necessary by the incident and date of return to service of the pipeline)

*Local reproduction of this form is permitted

PART L - INJURY AND FATALITY DESCRIPTIONS

□ **Number of Fatalities** □ **Number of Serious Injuries**

Serious Injury - includes an injury that results in: fracture of a major bone, amputation of a body part, loss of sight - one or both eyes, internal hemorrhage, third degree burns, unconsciousness, or loss of a body part

NAME	AFFILIATION	FATALITY OR INJURY DESCRIPTION AND CURRENT PATIENT CONDITION
	□ Company Employee □ Contractor □ Public	
	□ Company Employee □ Contractor □ Public	
	□ Company Employee □ Contractor □ Public	
	□ Company Employee □ Contractor □ Public	
	□ Company Employee □ Contractor □ Public	
	□ Company Employee □ Contractor □ Public	
	□ Company Employee □ Contractor □ Public	

PART M - IMMEDIATE INCIDENT CAUSE OF SERIOUS INJURY/FATALITY (Immediate Cause - means unsafe acts and conditions)

- □ Defective/inadequate safety devices, tools or equipment
- □ Improper loading or placement
- □ Congested work area/disorderly workplace
- □ Improper operation of safety devices, tools or equipment
- □ Hazardous environment (gases, dust, smoke, fumes or vapours)
- □ Other (specify)

PART N - NARRATIVE OF INCIDENT

Provide a complete description of the incident, including events leading up to, and following the incident. Also include additional information as specified in the guidelines to section 52 of the Onshore Pipeline Regulations. Attach any additional information that may supplement the narrative such as 1) drawing of the incident site 2) photographs 3) schematics 4) maps 5) reports (metallurgical, NDT, inspection, pressure test, etc.)

Attach additional sheets of narrative as required.

*Local reproduction of this form is permitted

PART O - WITNESS INFORMATION

NAME ______________________________ TELEPHONE NO. ( ) ____________________

______________________________ ( ) ____________________

______________________________ ( ) ____________________

______________________________ ( ) ____________________

PART P - BASIC CAUSES OF INCIDENT

(Identify all basic causes contributing to the incident. Basic Cause - means the real or root causes of why the unsafe acts and unsafe conditions as described in the immediate cause occurred. Several Basic Causes may be assigned for one incident.)

☐ Inadequate training ☐ Inadequate work standards or procedures ☐ Inadequate materials, tools or equipment

☐ Inadequate design/maintenance ☐ Non-compliance with work standards or procedures

☐ Other (specify) ____

Additional comments on selected basic cause: ______________________________________

PART Q - CORRECTIVE ACTIONS TAKEN TO PREVENT SIMILAR INCIDENTS (If no corrective action taken, state reasons why)

PART R - NAME OF PERSON CONDUCTING A COMPANY INCIDENT INVESTIGATION

Name____

Title____

Telephone ( )____________________Fax ( ) ____________________

PART S - NAMES OF OTHER AGENCIES INVESTIGATING INCIDENT

Agency	____________________	Agency	____________________
Telephone	____________________	Telephone	____________________
Contact Name	____________________	Contact Name	____________________
Agency		Agency	

PART T - NAME AND TITLE OF COMPANY REPRESENTATIVE FILING REPORT

Name____________________Signature____________________

Title____

Telephone ( )__________Fax ( )__________Date (time)_(month)_(day)_(year) ____

*Local reproduction of this form is permitted

14.2 FORM # 2: First Call Communication Form

Alberta Energy Regulator

First Call Communication (Page 1)

CONTACT DETAILS	AER Contact	Field Centre			
	Caller*	Phone*			
	Notification* date* time*	Release s tart date* start time* end time*	□ Ongoing		
	Licensee	Phone			
	Location*	Nearest Town			
	Nearest Resident	Distance/Direction	Phone		
	Media Involvement?*	□ Local □ Regional	□ National □ International	Media Contact	
	Operator	Phone			
PUBLIC IMPACT	Public Health and Safety*	□ Could be jeopardized □ Is jeopardized	Worker Injuries*	□ First aid □ Hospitalization	□ Fatality
	Emergency Assessment Matrix completed with licensee*	□ Alert □ One	□ Two □ Three	ERP activated?	□ Site Specific □ Field/Area	□ Corporate
	EPZ Size (2 km if unknown)	Numbers and Types of Public in the EPZ	EOC/ICP Location		
	Public Protection Measure Implemented	□ Notification □ Shelter	□ Road blocks □ Evacuation	Number Evacuated	
RELEASE TYPE	Release Impact *	□ On lease	□ Off lease	H_2S Concentration*	
	□ Sensitive Environment*	Environment Affected*	□ Air □ Land	□ Standing Water □ Flowing Water	Water Body Name
	Area Affected (m^2)*	□ Property Damage*	□ Equipment Loss*	□ Wildlife/Livestock Affected*	
	Gas Release	□ Sweet	□ Sour	Volume/Rate	
	Liquid Release	□ Oi	□ Water	□ Effluent	Volume/Rate
	□ Release Point Determined				
CONTAINMENT	Third Party/Outside Assistance required*	□ Incident contained or controlled □ Intermittent control possible	□ Imminent control probable □ Incident is uncontrolled		
	Company	WCSS Co-op			

*These fields must be completed to generate an FIS number and/or to complete an Emergency Assessment Matrix.

First Call Communication (Page 2)

OPERATION TYPE	Well Licence No.		Type of Incident	□ Kick	□ Blowout	□ Loss of Circulation
	Well Status	□ Drilling □ Standing	□ Servicing □ Sweet	□ Producing □ Sour	□ Injection □ Critical	□ Suspended
	Pipeline Licence No.		Line No.	□ Hit	□ Leak	□ Rupture
	Production Facility License No.		□ Gas □ Oil	□ Gas Plant □ Battery	□ Compressor □ Other	AESRD Approval No.
AIR MONITORING	□ Licensee Air Monitoring Occurring		□ Mobile	□ Handheld	Estimated Time of Arrival	
	Initial Readings/Location		□ PPB □ PPM	□ On Site □ Off Site	Distance	
	Contractor Name		Phone		AMU Phone	
	Wind Direction	Speed	Meteorological Conditions		AER AMU ETA	
COMMUNICATIONS	Communications completed by Licensee and/or AER					
	□ AEMA □ AEP □ WH&S	□ AB Health Services □ AHW □ Local Authority	□ CER □ DFO □ Environment Canada	□ TDG □ First Nations □ Indian Oil and Gas	□ Fire □ RCMP/Police □ Ambulance	□ WCSS □ Other
	Contact names and phone numbers					
	Incident Cause	□ Natural	□ Human-Induced Unintentional		□ Human-Induced Intentional	
OTHER INFORMATION	□ First Nations Band □ Métis Settlement	Band/Settlement Name/Contact			Phone	
	Complaints	□ Local □ Large Area				
	Private Land Title Holder				Phone	
	Public Land Type	□ Irrigation	□ Forestry	□ Grazing	□ Other	
	Public Land Administrator Contact				Phone	
	Additional Information					

14.3 FORM # 3: BC Incident Notification Report

BC Oil & Gas COMMISSION

Incident Notification Report (Page 1)

*This form is NOT to be submitted to the OGC. It is for responders to use when contacting the OGC regarding an incident so that they are prepared for the questions that the OGC will ask.

Incident Date: ____________________ Incident Time: ______________________________________

Received Date: __________________ Received Time: _____________________________________

INCIDENT DESCRIPTION

LEVEL OF EMERGENCY (as defined in the OGC Emergency Response Plan Requirements)

□	Unknown	Investigate and confirm
□	Level One	There is no immediate danger to the public or environment as NO H_2S has been released; the emergency is confined to lease or company property. Creates little or no media interest. Low potential for it to escalate. Handled by company personnel. No immediate threat to workers.
□	Level Two	There is the potential for risk to the public or environment, as the emergency could extend beyond Company property. However, control is still possible. Creates local or regional media interest. May require the involvement of external emergency services, federal, provincial or local agencies.
□	Level Three	There exists an immediate danger to the public or environment; control of the situation has been lost – uncontrolled release of hazardous substance. Creates provincial or national media interest. Extensive involvement of external emergency services, federal and/or provincial agencies. Emergency extends beyond company property.

AFFECTED AREA (Be prepared to provide directions)

Location: _______-_______-_______/ --------------------_______or
LSD_________, SEC_________, TWP________, RGE________W6M

GPS Location: Latitude:__________________________Longitude:____________________________________or
UTM (NAD 83):_________________________m easting______________________________m northing

Field Name: ____

Geographic Region: □ North □ Central West □ Central East □ South

PEP Region: □ NE □ NW □ Central □ SE □ SW □ Vancouver Island

Area Type : Describe affected area: □ Forest □ Muskeg □ Farmland □ Residential □ Other

Comments: ____

BC Oil & Gas COMMISSION

Incident Notification Report (Page 2)

*This form is NOT to be submitted to the OGC. It is for responders to use when contacting the OGC regarding an incident so that they are prepared for the questions that the OGC will ask.

AFFECTED AREA (continued)

Confined to company property? □ Yes □ No

Area Access: □ ATV □ Helicopter □ Four-wheel-drive □ Two-wheel-drive □ Unknown

Road Conditions/Access:______________________________

Directions:______________________________

Nearest City/Town/camp:________________ Highway/Road number/name: ________________

Name of River or Mountain:________________ Kilometre/Milepost: ________________

INCIDENT TYPE

□ Gas Release □ Liquid Spill □ Fire/Explosion □ Drilling □ Completion □ Servicing

□ Other: ______________________________

SITE TYPE

□ Producing Wellsite □ Drilling and Completions Wellsite □ Pipeline □ Remote Sump

□ Battery/Plant/Facility □ Other □ Unknown

□ Drilling Rig:________________ □ Service Rig: ________________

□ Other______________________________

MATERIAL INFORMATION

Material Description:

GAS

Sour (H$_2$S) gas □ Yes____________% □ No □ Unknown

Gas Rate:________________10^3m^3/d or mmcfd Gas Volume:________________10^3m^3 or mmscf

Can you hear/smell gas? □ Yes □ No Propane/NGLs/LPGs? □ Yes □ No

LIQUID

Sour (H$_2$S) oil/water/condensate □ Yes____________% □ No □ Unknown

Liquid Rate:________________m^3/d or BPD Liquid Volume:________________m^3 or bbls or litres

Environmental Issues: □ Yes □ No

□ Near Waterways □ Contaminated Soil □ Other

Nature/extent of environmental effects: ______________________________

WEATHER

Weather Conditions: □ clear □ cloudy □ other ______________________________

Wind Direction: From: □ N □ NE NW □ E SE S SW W

Wind Strength: □ Calm □ Moderate □ Strong □ Gusty

Temperature:____________°C

Comments: ______________________________

Incident Notification Report (Page 3)

*This form is NOT to be submitted to the OGC. It is for responders to use when contacting the OGC regarding an incident so that they are prepared for the questions that the OGC will ask.

CAUSE

□ Third Party
□ Human Error
□ Over Pressuring Equipment

□ Manufacturing Defect
□ External Corrosion
□ Other Factors

□ Internal Corrosion
□ Equipment Failure
□ Geological

CAUSE DESCRIPTION

REMEDIAL ACTIONS

PREVENTION

Was the incident preventable? □ Yes □ No

What measures have been put in place to prevent same incident in the future?

SAFETY ISSUES

Emergency Planning Zone Size:_______________km (Only for Level 2 or 3)

Approximate distance and direction to closest residence or public facility:___________________________________

Are responders in danger? □ Unknown □ No □ Yes

Are public in danger? □ Unknown □ No □ Yes

Danger Description: ____

Public safety actions taken: □ Evacuation □ Sheltering □ Road blocks □ Road Closure Order □ NOTAM □ Transient Survey □ Media Release □ Mobile Air Quality Monitoring □ Ignition □ Trappers/Guide-Outfitters/Range Allotments/Grazing Lease have been notified

FIRST NATIONS INFORMATION

Affected First Nations □ No □ Yes Name ____

If yes, has First Nations been notified by operator? □ Yes □ No

Key Response/Consultation/Administrative/Critical Community Area ______________________________

BC Oil & Gas COMMISSION

Incident Notification Report (Page 4)

*This form is NOT to be submitted to the OGC. It is for responders to use when contacting the OGC regarding an incident so that they are prepared for the questions that the OGC will ask.

INJURIES / MEDICAL EMERGENCIES

Name	Affiliation	Description of Injury	Actions Taken

WITNESSES

A list of witnesses who were present when the incident took place:

Name	Address	Telephone Number

SITE #_____________________________

FACILITY STATUS

OGC Facility Code #: ____________________________

Design Capacity:________________________________Actual Throughput: ______________________________

Operating Pressure:_____________________________Operating Temperature: __________________________

Equipment/Process: P□roduction Storag□e Disposal/In□jection: Acid Gas Wate□r □

□ Metering □ Testing □ Separation □ Compression □ Dehydration - Type: _______________________

□ Sweetening □ Fractionation/Refrigeration □ Sulphur Recovery

□ Flare Systems: □ High Pressure □ Low Pressure □ Incinerator

WELL STATUS

Well Authorization #:_____________________________Status:____

Depth/Perforations_________________________m KB Wellbore Fluid Density_____________________kg/m^3

Pit Gain______________________________________m Kill Fluid Density___________________________kg/m^3

*SIDPP/SITP_________kPa *SICP________kPa Activity: *RSPP_________kPa Equipment:________________

Operating Pressure:_________________________kPa Shut In Pressure: _______________________________

Well Miscellaneous: ____

* SIDPP - Shut in Drill Pipe Pressure SITP - Shut in Tubing Pressure SICP - Shut in Casing Pressure
RSPP - Reduced Speed Pump Pressure

BC Oil & Gas COMMISSION

Incident Notification Report (Page 5)

*This form is NOT to be submitted to the OGC. It is for responders to use when contacting the OGC regarding an incident so that they are prepared for the questions that the OGC will ask.

PIPELINE STATUS

Project #:________________________________ Product:________________________________

From LSD:________________________________ To LSD: ________________________________

ID________________________________mm Operating Pressure______________________kPa

OD________________________________mm Maximum Operating Pressure kPa

Line Length between valves:______________km

ESD or Block Valve Closure? Yes □ No □ Unknown □

Location of ESDs or Block Valves: ____

GEOPHYSICAL PROGRAM

Geophysical Program #: ____________________

Comments: ____