**The collection of this sensitive information is authorized under Section 501.2 of the ISO Rules for compliance monitoring of a critical facility designated on the *Alberta Counter-Terrorism Crisis Management Plan* Critical Infrastructure list.  The information collected shall be deemed confidential and shall, to the extent permitted by law, be treated accordingly. If you have any questions about the collection or use of this information, please contact the AESO by email at** **securityrulecompliance@aeso.ca****.**

**Reminders:**

1. Please edit the header of this template to incorporate the site reference no.
2. Ensure that you are using the most recent version of the template in effect and available on the AESO website.

**Part 1: ISO Rule Compliance Security Assessment**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** | **No** | **Comments, if any.** |
| Does the critical facility have an approved threat response plan (TRP) in place? |[ ] [ ]   |

| **Reference** | **SECURITY PROGRAM** |
| --- | --- |
|
| **1.** | ***PRELIMINARY ACTIONS*** |
| **A.** | **Site Information*****Site description*** - Describes the name and type of facility, estimated value of assets, and current list of critical assets not directly owned by operator. Also describes surrounding geography and includes maps, schematics and aerial photos.***Key Personnel*** - Includes emergency contact info for police, critical staff. Identifies personnel that are critical to operations and security and includes 24-hour contact information. |
| ***Describe how the threat response plan addresses the following, as detailed above.*****Site description****Key Personnel** |
| **B.** | **Vulnerability Assessment** |
|  | ***Assets*** - Identifies assets critical to operations and assesses impact of injuries/death/damage to each.**People Assets** - Assesses the risk of injury or death, and the impact to business, in the event of an attack. Considers employees’ links to terrorism or organized crime.**Material Assets** - Assesses the risk and impact to critical assets from possible attacks (explosive, fire, cyber).***Access*** - Assesses the level of difficulty in gaining unauthorized access to facility.***Attack*** - Considers the most likely types of attack that could be undertaken against the facility. Considers the worst case scenario attack.**HAZMAT** - Maintains an inventory of HAZMAT in use at the facility. Assesses the impact of a HAZMAT spill or fire as a result of an attack. |
| ***Describe how the threat response plan addresses each of the following, as detailed above, and describe the results of each assessment performed.*** **Assets****People Assets****Material Assets****Access****Attack****HAZMAT** |
| **2.** | ***PLANS, POLICIES & PROCEDURES*** |
| **A.** | **Security Policy** |
|  | ***Security Plan*** - Separate security plan in place; circulation centrally controlled. Record of past and current problems. Security threat response plan is layered. Security threat response plan allows for increased threat level. Periodic review of security threat response plan.***Legal*** - Have consulted company’s legal counsel with respect to rights of arrest, search, use of force, etc., for each level of security. |
| ***Describe how the threat response plan addresses the following, as detailed above.*****Security Plan****Legal** |
| **B.** | **Communications** |
|  | ***Protocols*** - Identify points of contact with police, fire, and emergency management; establish and test call-out system for points of contact as well as critical employees.***Hardware*** - Build redundancy into communication system. Where applicable, make the following available to security force: Encrypted email, secure fax and phone, sat phone, secure radio.***Control Centre*** - Establish communications control centre, with alternate, to be operational at and above designated security level. |
| ***For each subheading as detailed above, please comment on how the threat response plan addresses the suggested security measures.*****Protocols****Hardware****Control Centre** |
| **C.** | **Training** |
|  | ***Program*** - Establish security training and orientation program for employees that covers security policy, awareness, responsibilities, and duties.***Exercises*** - Facility exercises include security incident; record kept of past exercises & lessons learned. |
| ***For each subheading as detailed above, please comment on both how the threat response plan addresses the topic and describe any specific security measures implemented at the site.*****Program****Exercises** |
| **3.** | ***OUTER PERIMETER*** |
| **A.** | **Grounds** |
|  | ***Landscaping*** - Landscaping enhances security: screens points of entry and critical assets from outside observations, does not allow for hiding places or climbing.***Road Barriers*** - Road barriers able to withstand vehicular collision and/or designed to prevent unauthorized vehicular access. Pre-plan delivery and placement of additional barriers at higher levels.***Signage*** - Signage clearly indicates directions for proper access and designates “no access”.***Contingency for Higher Threat Levels:*** (a) Close and secure redundant access points. (b) Increase number of random patrols. (c) Operate with a single access point. (d) Contingency plan to operate with a no-fly zone in place. |
| ***For each subheading as detailed above, please comment on both how the threat response plan addresses the topic and describe any specific security measures implemented at the site.*****Landscaping****Road Barriers****Signage****Contingency for Higher Threat Levels** |
| **B.** | **Perimeter Barrier** |
|  | (i) Complete site exterior perimeter fence. (ii) Fence equipped with top guards. iii) Fence bottom flush with ground. (iv) Fence integrity - good repair. (v) Scheduled interval for maintenance/integrity checks. (vi) Gate/gate corners flush with ground. (vii) Pedestrian gates un-operable from outside. (viii) Vehicle gates locked when site vacant. (ix) Unused access points are secured.(x) ***Contingency for Higher Threat Levels:*** (a) All identified repairs are to be carried out. (b) Where warranted height/topper of barrier is increased. (c) Intrusion alarms are tested daily. (d) CCTV coverage of entire perimeter is established. |
| ***For each subheading as detailed above, please comment on both how the threat response plan addresses the topic and describe any specific security measures implemented at the site.*** ***(i) Complete site exterior perimeter fence. (ii) Fence equipped with top guards. iii) Fence bottom flush with ground. (iv) Fence integrity - good repair. (v) Scheduled interval for maintenance/integrity checks. (vi) Gate/gate corners flush with ground. (vii) Pedestrian gates un-operable from outside. (viii) Vehicle gates locked when site vacant. (ix) Unused access points are secured.*** ***(x) Contingency for Higher Threat Levels.*** |
| **C.** | **Lighting** |
|  | ***Illumination*** - All access points are illuminated, along with the majority of the perimeter where practicable; parking lots illuminated.***Controls*** - Weather proof and tamper resistant, inaccessible from outside perimeter and master switches centrally located.***Contingency for Higher Threat Levels:*** (a) Contingency in place for additional/brighter lighting. (b) All identified repairs to be carried out. (c) Back-up power supply established for security lighting. (d) Security lighting tested daily. |
| ***For each subheading as detailed above, please comment on both how the threat response plan addresses the topic and describe any specific security measures implemented at the site.*****Illumination****Controls****Contingency for Higher Threat Levels** |
| **D.** | **Security** |
|  | ***Visibility*** - Security force and check in point are visible from main approaches. ***Reporting Policy*** - Security policy includes procedures for reporting non-ordinary activities.***Monitoring*** - Regular monitoring of alarms and CCTV; secure storage of images/video; backup power.***Contingency for Higher Threat Levels:*** (a) Increase size of security force. (b) Perimeter and grounds inspected once/shift for damage, suspicious packages, etc. (c) Canine support included at security check-in. (d) Inspect vehicles entering facility. |
| ***For each subheading as detailed above, please comment on both how the threat response plan addresses the topic and describe any specific security measures implemented at the site.*****Visibility****Reporting Policy****Monitoring****Contingency for Higher Threat Levels** |
| **4.** | ***INNER PERIMETER*** |
| **A.** | **Structures**  |
|  | ***Systems*** - Connections to utilities, and back-up systems, located in secure areas. Where practical consider fire and blast protection enhancements. Modify exterior wall to prevent concealment of destructive devices.***Doors*** - Doors to critical areas should be constructed to resist fire, explosion, tampering, and forced entry. Security supervisor has overall authority for issue, changes, and replacements of all manner of door access. Locks and padlocks changed or rotated annually.***Windows*** - Exterior windows can be locked/alarmed. Windows in place for ventilation could be replaced by smaller opening or functionally replaced by internal ventilation. Windows in place for illumination could be replaced with smaller opening coupled with interior reflector. Damage from shattered glass can be reduced by the application of a protective film on the interior of the window.***Other Access Points*** - Manhole covers, grates, vents, skylights are normally locked.***Lighting*** - Motion sensitive lighting in critical areas; where practicable, majority of perimeter is lit; regular maintenance.***Alarms*** - Intrusion alarms installed wherever practical. Centrally monitored, tied to CCTV system. Connected to police. Tested regularly.***Contingency for Higher Threat Levels:*** (a) Critical areas are swept for electronic eavesdropping devices. (b) Consider closing/securing minimum use areas. (c) Intrusion prevention mechanisms increased. (d) Blast protection of critical structures enhanced. |
| ***For each subheading as detailed above, please comment on both how the threat response plan addresses the topic and describe any specific security measures implemented at the site.*****Systems****Doors****Windows****Other Access Points****Lighting****Alarms****Contingency for Higher Threat Levels** |
| **B.** | **Commodities** |
|  | ***Screening*** - Suppliers of HAZMAT and critical material known to be reliable; drivers and staff properly cleared***Control Movement*** – Record kept of volume and locations of HazMat on site. Dates of expected orders given to security personnel. Secure procedures followed upon receipt, movement, and storage of HazMat.***Redundancy*** - Keep updated list of alternate suppliers. Keep sufficient amount of supplies on hand for higher levels of security.***Storage*** - Critical and hazardous material securely stored, available on a need basis only. |
| ***For each subheading as detailed above, please comment on both how the threat response plan addresses the topic and describe any specific security measures implemented at the site.*****Screening****Control Movement****Redundancy****Storage** |
| **C.** | **Equipment** |
|  | ***Storage/Movement*** - Secure storage of essential equipment with same priority as essential areas of site. Movement of essential equipment controlled, current inventory maintained.***Identification*** - Equipment identified via barcode or engraving; ID tied to inventory, updated regularly.***Maintenance*** - Off-site maintenance of equipment done by screened personnel. Plan to conduct maintenance on-site at higher threat levels. If on-site maintenance is routine, maintain sufficient supplies/parts on site.***Redundancy*** - Essential functions able to continue in event of equipment breakdown. Redundant units of essential equipment maintained on site, or interdependencies with neighbouring sites established. Plans for repairing/replacing essential equipment at higher threat levels.***Contingency for Higher Threat Levels:*** (a) Equipment used off-site is inspected upon return. (b) Essential equipment stored with 24-hr surveillance. (c) Conduct all equipment maintenance on-site. |
| ***For each subheading as detailed above, please comment on both how the threat response plan addresses the topic and describe any specific security measures implemented at the site.*****Storage/Movement****Identification****Maintenance****Redundancy****Contingency for Higher Threat Levels** |
| **D.** | **Operations** |
|  | ***Prioritization*** Critical operations identified and prioritized; vulnerabilities of each assessed; consider redundancy/mobility in event of higher security level.***Location*** Wherever possible, locate critical operations away from public areas and far from exterior walls/perimeter.***Contingency for Higher Threat Levels:*** (a) Relocate critical operations to a secure area. (b) Ensure financial plans can meet security requirements of higher threat levels. (c) Shut down non-essential operations. |
| ***For each subheading as detailed above, please comment on both how the threat response plan addresses the topic and describe any specific security measures implemented at the site.*****Prioritization****Location****Contingency for Higher Threat Levels** |
| **5.** | ***ACCESS CONTROLS*** |
| **A** | **Employees/Contractors** |
|  | ***Screening*** - Background checks conducted on all employees and contractors, to the extent warranted by the position. Background inquiries are conducted on new suppliers.***Termination/Retirement*** - Policy exists for returning keys, passes, locking accounts, access codes. Lock/access codes to critical areas changed as required.***Roster*** - Maintain a list of people that have access to the facility that identifies them by name, DOB, level of access, home address and contact numbers.***Access Passes*** - Employees & contractors wear tamper-proof photographic ID that indicates level of access; card administration software on site; policy in place for lost/stolen ID. |
| ***For each subheading as detailed above, please comment on both how the threat response plan addresses the topic and describe any specific security measures implemented at the site.*****Screening****Termination/Retirement****Roster****Access Passes** |
| **B.** | **Visitors/Customers/Deliveries** |
|  | ***Access Passes*** - All visitors to wear passes separating them from employees/contractors. All passes are numbered and are to be signed out with name, company, contact number, and are returned on the same day. Missing and non-returned passes are logged and acted on. Visitor access is limited to that of the sponsoring employee/contractor.***Control Movement*** - Visitors are escorted by their sponsor. |
| ***For each subheading as detailed above, please comment on both how the threat response plan addresses the topic and describe any specific security measures implemented at the site.*****Access Passes****Control Movement** |
| **C.** | **Vehicles/Parking** |
|  | ***Vehicle Access*** - All vehicles clearly display a tag identifying it as employee/contractor, visitor, or delivery. Employee/contractor parking tags linked to license plates.***Parking Control*** - Where practical parking lots are outside perimeter. Employee/contractor parking is separate from visitor.***Overnight Policy*** - Maintain record of employees that have company vehicles overnight. Implement policy for securing company vehicles stored off-site.***Contingency for Higher Threat Levels:*** (a) Reduce parking to minimum required for essential employees. (b) Allow access only to employee shuttle, security, and first responder vehicles. |
| ***For each subheading as detailed above, please comment on both how the threat response plan addresses the topic and describe any specific security measures implemented at the site.*****Vehicle Access****Parking Control****Overnight Policy****Contingency for Higher Threat Levels** |
| **D.** | **Shipping/Receiving** |
|  | ***Control System*** - Identify number and type of shipping/receiving areas and minimize where possible. Identify secure areas away from critical operations that could be used at higher threat levels. Ensure communication between security check-in and shipping/receiving to confirm status of deliveries.***Policy*** - Employees made aware of suspicious package policy. Minimum number of employees can authorize deliveries. New suppliers/carriers are screened.***Contingency for Higher Threat Levels:*** (a) Where practical use inspection equipment for packages. (b) Only allow deliveries from known sources. |
| ***For each subheading as detailed above, please comment on both how the threat response plan addresses the topic and describe any specific security measures implemented at the site.*****Control System****Policy****Contingency for Higher Threat Levels** |
| **E.** | **Security** |
|  | ***Policy/Plan Review*** - Security personnel are to review all plans and policies periodically and sign acknowledgement.***Familiarization*** - Security personnel are to be aware of the employees responsible for meeting a security plan objective (i.e.: receiving, on-site repairs). Security personnel are /encouraged to become familiar with employees.***Contingency for Higher Threat Levels:*** (a) Immediately report non-ordinary activities. (b) Access points are to be manned constantly. (c) Radio communications to be established and kept open. |
| ***For each subheading as detailed above, please comment on both how the threat response plan addresses the topic and describe any specific security measures implemented at the site.*****Policy/Plan Review****Familiarization****Contingency for Higher Threat Level** |
| **6.** | ***INFORMATION TECHNOLOGY*** |
| **A.** | **Computerization** |
|  | ***Recovery Plan*** - Ensure plan is current and identify IT support, listing emergency contact numbers. Establish back-up systems such as on and off-site hardware, power.***Protection and Access*** - Ensure firewall and anti-virus are current and allow for daily scans. Inventory all hardware and software. Levels of access should be implemented and enforced if facility has access to internet or company intranet. Restrict access to unauthorized sites (e.g.: downloading and streaming services). Employ user ID and password when accessing systems. Restrict remote access to key personnel or certain levels.***Policy*** - Only company-approved software/hardware to be used. Foreign media are not to be inserted into company system unless approved and cleared by IT security. Portable company hardware (i.e.: laptops) are to be signed out to specific employees. Employees and contractors are to be made aware of email and internet policy.***Contingency for Higher Threat Levels:*** (a) Perform regular and sporadic penetration tests. (b) Restrict access to intranet sites and network drives to essential personnel. (c) Ensure sensitive/confidential information is encrypted. |
| ***For each subheading as detailed above, please comment on both how the threat response plan addresses the topic and describe any specific security measures implemented at the site.*****Recovery Plan****Protection and Access****Policy****Contingency for Higher Threat Levels** |

**Part 2: ISO Rule Compliance Emergency Response Plan Assessment**

The 2nd part of this self-assessment template pertains to corporate Emergency Response Plans (ERP) as required in Section 501.2 of the ISO Rules. Corporate ERPs should be prepared and updated in accordance with *Directive 071, Emergency Preparedness and Response Requirements for the Petroleum Industry*.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** | **No** | **Comments, if any.** |
| Does the critical facility have an approved emergency response plan (ERP) in place? |[ ] [ ]   |

| **Reference** | **EMERGENCY RESPONSE PLAN** |
| --- | --- |
|
| **1.** | **Basic Information/Requirements (Sections 2.1 – 2, 3, 4 and 14.1)**The ERP contains information about key corporate contacts of the legal owner and a 24-hour corporate emergency contact telephone number.A call to the 24-hour emergency telephone number initiates immediate action. The 24-hour emergency telephone number is posted by way of a conspicuous sign erected at the primary entrance to all critical facilities.An up-to-date copy of the ERP (hard copy or electronic) must be kept at a response location(s).**Telephone Lists (Section 5.6)**The ERP contains a telephone list of key internal personnel designated to assist in emergency response; and a telephone list of external emergency support services that may be required in an emergency, including, but not limited to, government departments and agencies, communication services, and emergency services. |
| ***Describe how the emergency response plan and/or other relevant plans/programs address the following, as detailed above.*****Basic Information/Requirements****Telephone Lists** |
| **2.** | **Assessment Matrix (Sections 2.1.1, 5.1 and Appendix 4)**The ERP identifies hazards and potential consequences of those emergency scenarios deemed relevant and the appropriate actions that would be taken for each such emergency scenario. Appendix 4 of DIR071 provides one approach for classifying scenarios and responses.  |
| ***As detailed above, please comment on how the emergency response plan and/or other relevant plans/programs address the suggested measure.*** |
| **3.** | **Communications Planning (Sections 2.1.2, 5.8, 5.13 and 11.1.2 – 5)**Considers a communications plan that addresses communication with response team, support services, and government; communication with the public and media; and downgrading and stand-down of emergency levels.The ERP has information that: * describes the procedures for contacting and maintaining communication with key personnel, local authority, the RCMP/police, other applicable government agencies, support services, members of the public, and the media;
* clearly defines the responsibility to contact responders in the event of an emergency; identifying responsibilities by role;
* describes procedures that will be implemented during an incident to contact and maintain communication with directly impacted members of the public in order to keep them informed of the situation and the actions being taken;
* describes procedures that will be used to inform and update the media and procedures in getting factual messages out to the public at large in an expeditious manner; and
* describes procedures to downgrade and stand-down levels of emergency.
 |
| ***As detailed above, please comment on how the emergency response plan and/or other relevant plans/programs address the suggested measure.*** |
| **4.** | **Responsibilities of Personnel (Sections 2.1.3 and 5.9)**Roles and responsibilities of personnel required to effectively respond to an emergency are identified in the ERP. One or more functions can be assigned to an individual depending on the complexity of the potential response to an emergency. The following responsibilities are assigned to personnel, if applicable: field incident command, public safety coordination, including evacuation and sheltering, roadblocks and rovers, and communication with the responders, media, and public. |
| ***As detailed above, please comment on how the emergency response plan and/or other relevant plans/programs address the suggested measure.*** |
| **5.** | **Incident Management System (Sections 2.1.4 and 5.10)**The ERP describes how a response to an emergency will be managed and coordinated, and addresses the roles and responsibilities of personnel in the response. The ERP may include the establishment of an on-site command post and/or the corporate Emergency Operations Centre (EOC) (An operations centre established in a suitable location to manage the larger aspects of an emergency).The ERP clearly outlines the communication protocols and procedures to provide effective information flow among representatives and other responders at the emergency site, corporate-level decision-makers, and other government departments and agencies. |
| ***As detailed above, please comment on how the emergency response plan and/or other relevant plans/programs address the suggested measure.*** |
| **6.** | **Reception Centre (Sections 2.1.5 and 5.12)**The ERP has procedures for activating a reception centre located at a safe distance, and meeting and registering evacuees at the reception centre. |
| ***As detailed above, please comment on how the emergency response plan and/or other relevant plans/programs address the suggested measure.*** |
| **7.** | **Public and Local Authority Involvement in Emergency Preparedness and Response (Sections 4.2 – 6, and 5.5)**Details of any mutual aid understandings with local authorities are included in the ERP. This would identify the specific needs and roles and responsibilities of each party during an emergency This is to ensure that there is no confusion or misunderstanding of the roles and responsibilities in the event of an incident requiring activation of the ERP. |
| ***As detailed above, please comment on how the emergency response plan and/or other relevant plans/programs address the suggested measure.*** |
| **8.** | **Maps (Section 5.3)**The ERP includes maps, as applicable, that are sized to provide a clear representation of the entire mapped area. Maps may contain, but are not limited to, the following: surface location(s) of the operation(s) and access roads; provincial, local, and access roadways; lakes, rivers, streams, and any elevation feature that could impact emergency response; urban density developments, campgrounds, recreation areas, public facilities (e.g., churches, schools, hospitals), and any other publicly used development; trapping area, grazing lease, and range allotment boundaries and their reference numbers; other industrial operations, including oil and gas operations; railways and airports; corporate boundaries (e.g., hamlets, villages, towns); and a legend, scale, and north directional indicator. |
| ***As detailed above, please comment on how the emergency response plan and/or other relevant plans/programs address the suggested measure.*** |
| **9.** | **Equipment List, Location and Calibration (Sections 5.4 and 14.4)**The ERP considers the necessary equipment that will be used by relevant personnel in responding to emergencies, such as communications equipment used by the public safety coordinator.Equipment identified in the ERP is available and located where specified in the ERP. Company equipment is operational and the appropriate documentation is available to verify testing and calibration requirements, as applicable. |
| ***As detailed above, please comment on how the emergency response plan and/or other relevant plans/programs address the suggested measure.*** |
| **10.** | **Plan Distribution (Section 5.7)**Copies (either full or partial) of the ERP are provided to all responders requiring one. The need for distribution is determined through communication with all responders during plan development. A record of ERP distribution, including amendments, is maintained. |
| ***As detailed above, please comment on how the emergency response plan and/or other relevant plans/programs address the suggested measure.*** |
| **11.** | **Plan Management Process (Section 14.6 – 22)**The plan management process keeps ERPs up to date. A plan management process ensures that plans are reviewed on a regular basis and updated as necessary, with changes made to ensure that the information remains accurate; updates could be triggered by events such as changes to current emergency information, any changes to response staff information or response capabilities, and facility additions. |
| ***As detailed above, please comment on how the emergency response plan and/or other relevant plans/programs address the suggested measure.*** |
| **12.** | **Training Sessions (Section 14.9)**Training sessions are provided to ensure that response personnel are competent in emergency response procedures. ERP training is provided on the overall plan, roles and responsibilities during an incident, public protection measures used during an emergency, and available communication methods. |
| ***As detailed above, please comment on how the emergency response plan and/or other relevant plans/programs address the suggested measure.*** |
| **13.** | **Exercise Requirements (Section 14.10)**The ERP is tested through planned exercises to promote emergency response preparedness. Examples of exercises may include tabletop or communications exercise, held annually for each area ERP, except in a year when a major exercise is held, and major exercise, held once every three years for each area ERP. |
| ***As detailed above, please comment on how the emergency response plan and/or other relevant plans/programs address the suggested measure.*** |
| **14.** | **Record Keeping (Section 14.11)**There should be a process for recording the following activities:Incident Records* information gathered during and following an incident: these records provide documentation to be used for assessment, historical, and analytical purposes

Keeping ERPs Current* efforts to keep the ERP current

Training, Meetings, and Exercise Records* records of staff training
* within 60 days of an exercise, a report of exercise results to be maintained for assessment purposes that includes
	+ type of exercise held
	+ scope and objectives
	+ persons involved
	+ outcome (i.e., whether objectives were achieved)
	+ lessons learned
	+ action plan, including timelines

All records are expected to be retained for a period of three years or more. |
| ***For each subheading as detailed above, please comment on how the emergency response plan and/or other relevant plans/programs address the suggested measure.*****Incident Records****Keeping ERPs Current****Training, Meetings, and Exercise Records** |

**Part 3: Declaration**

|  |
| --- |
| I confirm, to the best of my knowledge, that the information in this self-assessment is correct and complete. |

|  |  |  |  |
| --- | --- | --- | --- |
| Name of officer and position: |  | Signature: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Telephone: |  | Date: |  |