


Petroleum	Health, Safety & Environment Management System Security and Emergency Management	 bhpbilliton <small>resourcing the future</small>
------------------	---	--

PETROLEUM CSG


HSE MANAGEMENT SYSTEM CONTROL

SECURITY AND EMERGENCY MANAGEMENT
--

Petroleum HSE Control No: PHSE-11-C01	
Date: March 23, 2011	Revision: 1
Owner: Garry Evans, Asset Protection Manager	
Approver: Matthew Ridolfi, Vice President HSE	Signature On File

TABLE OF CONTENTS

INTRODUCTION.....	3
Purpose	3
Application and Scope	3
Responsibility	3
Incidents, Emergencies and Security	3
Control 1 – Security Risk Management.....	4
Control 2 – Security Risk Assessment	5
Control 3 – Security Plans and Control Design.....	6
Control 4 – Public and Private Security Resources	7
Control 5 – Security Training and Awareness	8
Control 6 – Crisis and Emergency Management.....	9
Appendix A: Security and Emergency Management Approvals Framework.....	10

<p>Petroleum</p>	<p align="center">Health, Safety & Environment Management System</p> <p align="center">Security and Emergency Management</p>	
-------------------------	--	---

INTRODUCTION

Purpose

The Petroleum Security and Emergency Management Controls define requirements for managing security risks associated with Petroleum Operations and associated activities and managing crisis or emergency situations in order to protect the safety of people, the environment, assets and reputation.

The Security and Emergency Management Controls are part of the Petroleum HSE Management System and are established using industry best practices, guidelines and standards. Effective implementation of these Controls will reduce exposure to security risks, mitigate the impact of incidents or emergencies, and protect personnel, the environment and facilities within an operating framework that ensures respect for human rights.

Application and Scope

The Petroleum Security and Emergency Management Controls apply to Petroleum Controlled Sites and to Petroleum employees and contractors performing Controlled Activities relating to Exploration, Development and Production operations including:

- Passage through heliports and shore bases;
- The design and construction of new facilities or significant changes to existing facilities and;
- Company provided residences.

Petroleum monitored activities should have equivalent systems in place to meet the intent of this document and partners, suppliers and contractors are also encouraged to adopt the intent of these Controls.

Where a conflict exists between the requirements in these Controls and applicable local regulatory laws, the applicable law must be applied. Where the requirements of these Controls are more stringent than local laws then the requirements of these Controls must be applied.

Responsibility

Unless otherwise stated, Senior Line Managers and supervisors responsible for Controlled Activities are accountable for the implementation of the performance requirements outlined in the Controls in accordance with the approvals framework at Appendix A.


INCIDENTS, EMERGENCIES AND SECURITY

This document defines the high level requirements for managing security risks and emergency response activities within Petroleum. More detailed requirements for management of incidents, emergencies and security are contained within the following Petroleum HSE Procedures:

- [Site Security](#)
- [Firearms Management](#)
- [Safe Travel](#)
- [Crisis and Emergency Management](#)
- [Oil Spill Contingency Plan](#)
- Kidnap for Ransom or Extortion Incident Management (*Available through Asset Protection*)

Additional requirements relating to Information Management and Security are contained within corresponding Petroleum Information Management Standards and Procedures.

<p>PHSE-11-C01</p>	<p align="center">CONTROLLED DOCUMENT</p> <p align="center">Page 3 of 10</p> <p align="center"><small>Printed copies of this document are not controlled. To verify this copy is current, check the Petroleum Portal.</small></p>	<p align="center">Rev. 1</p>
--------------------	--	------------------------------

Petroleum	Health, Safety & Environment Management System Security and Emergency Management	 bhpbilliton <small>resourcing the future</small>
------------------	---	---

CONTROL 1 – SECURITY RISK MANAGEMENT

INTENT

Personnel with security management responsibilities or specific security duties are suitably experienced or trained to perform the function and individual roles are understood and documented.

PERFORMANCE REQUIREMENTS

- | | |
|--|--|
| <p>1.1 Security Managers shall be responsible for the implementation and management of security controls and provision of functional support within the respective Exploration or Development Project, Production Unit or Country office. If a Security Manager has not been appointed then the appropriate HSE Manager shall assume these responsibilities.</p> <p>1.2 A Security Focal Point (SFP) must be nominated for each Company site or activity by the Senior Line Manager responsible for the site or activity and recorded in a site security plan.</p> <p>1.3 The SFP may be part of the Operations, Facilities or HSE Management team and must have demonstrable experience or training in security management. Further advice on adequacy of experience or training should be sought from Petroleum Asset Protection in accordance with the functional approvals framework at Appendix A.</p> <p>1.4 The SFP shall be responsible for:</p> <ul style="list-style-type: none"> - Co-ordination of security related activities with the Security Manager or HSE Manager. - Development and management of the site security plan. - Implementation, supervision and maintenance of site security controls, procedures, systems and equipment. - Management of external security service providers. - Liaison with local security agencies and monitoring local security risks. | <p>1.5 Line Managers with security oversight responsibilities and SFPs shall be appropriately experienced or trained in the following competencies:</p> <ul style="list-style-type: none"> - Awareness and identification of security risks - Implementation and measurement of effective security controls - Jurisdiction and the law in relation to criminal incidents, private security companies and the Company - Response to a security incident and preservation of evidence - The Voluntary Principles on Security and Human Rights (VPSHR) <p>1.6 Personnel with maritime security management responsibilities shall attend an appropriate International Maritime Organization (IMO) security course.</p> <p>1.7 All Company sites and activities shall have resources in place to effectively manage security risks and perform specific security duties including:</p> <ul style="list-style-type: none"> - Public / Visitor Reception - Access Control & Screening - Surveillance - Property & Key Management - Mail & Cargo Management <p>1.8 Personnel with security duties shall rehearse specific emergency response scenarios at a frequency determined in the site security plan under the co-ordination of the SFP.</p> |
|--|--|

PHSE-11-C01	CONTROLLED DOCUMENT Page 4 of 10 <small>Printed copies of this document are not controlled. To verify this copy is current, check the Petroleum Portal.</small>	Rev. 1
-------------	--	--------


CONTROL 2 – SECURITY RISK ASSESSMENT

INTENT

Security risks and operational vulnerabilities are identified and assessed as part of the risk management process.

PERFORMANCE REQUIREMENTS

- | | |
|---|--|
| <p>2.1 Security risk assessments shall be conducted:</p> <ul style="list-style-type: none"> - Annually. - Prior to commencement of any new activity or significant change to routine activities. - Following a significant security incident that impacts the risk profile or change in security response level. <p>2.2 SFPs and HSE Managers shall be responsible for the co-ordination of security risk and vulnerability assessments by a cross functional team that must include Petroleum Asset Protection personnel or a competent security practitioner.</p> <p>2.3 The following security risks shall be assessed:</p> <ul style="list-style-type: none"> - Crime - Civil unrest / disorder - Terrorism - Threat of armed conflict or war - Kidnap - Explosive remnants of war - Piracy (for marine operations) <p>2.4 Security risks shall be assessed as a function of consequence to the business and likelihood of a security incident using the Petroleum HSE Risk Matrix procedure.</p> <p>2.5 The assessment of likelihood shall be based on the attractiveness of a target, the degree of credible threat posed by a potential adversary and the vulnerability of the business and existing controls.</p> | <p>2.6 The assessment of likelihood should take into consideration security related information and records from a mixture of sources, including:</p> <ul style="list-style-type: none"> - General security information and records available from public sources. - Information and analysis from specialist sources and peer industry networks. - Reports from local, national and international security forces and agencies. <p>2.7 The results of the risk assessment shall be used to determine where more detailed assessment of vulnerability may be required and enhanced controls or countermeasures put in place to reduce security risks to within tolerable limits.</p> <p>2.8 The specific results of the security assessments shall be documented in an endorsed report. Any material risks identified shall be recorded in the appropriate risk register and briefed to the relevant Divisional President.</p> <p>2.9 Improvement opportunities identified by the security risk and vulnerability assessment shall be documented and discussed with the relevant Senior Line Manager with agreed actions, timelines and responsibilities entered into an appropriate action tracker for implementation.</p> |
|---|--|

Petroleum	Health, Safety & Environment Management System Security and Emergency Management	 bhpbilliton resourcing the future
------------------	---	--

CONTROL 3 – SECURITY PLANS AND CONTROL DESIGN

INTENT

Security controls are established to reduce and mitigate identified vulnerabilities or risks with detailed responsibilities and operating procedures captured within an approved security plan.

PERFORMANCE REQUIREMENTS

- 3.1 All Controlled Sites must have an approved security plan in accordance with Appendix A.
- 3.2 Short-term Controlled Activities, or special events, which are not covered by a site security plan shall be assessed on a case by case basis and ensure security risks and controls are included within a bespoke security or emergency response plan and contractual documentation created specifically for the activity or event.
- 3.3 Security planning and design shall be conducted by a competent security practitioner.
- 3.4 Functional guidance shall be sought from Petroleum Asset Protection during the design phase of new facilities, or significant change to existing facilities, to ensure security controls and physical layout are considered and incorporated in advance of construction.
- 3.5 Security plans and controls shall be scaled according to the prevailing security risks and results of security risk and vulnerability assessments. Security plans and controls must include the mandatory controls listed within the Petroleum Site Security Procedure.
- 3.6 Security plans shall contain:
- Description of Facility/Operation/Activity.
 - Summary of credible security risks.
 - Overview of security management organization with detailed individual responsibilities.
 - Description and performance standards for all security controls, equipment and resources.
 - Identification of critical areas, equipment or resources with relevant floor plans and site diagrams.
 - Detail of standard security procedures and triggers for (and details of) enhanced controls during escalated response levels.
- 3.7 Security plans shall contain specific response actions for the following scenarios:
- Unannounced visitor
 - Intruder / trespasser
 - Theft
 - Alarm activation
 - Facility / Site evacuation
 - Suspicious activity / incident
 - Receipt of threats (verbal / written / bomb)
 - Workplace violence and/or direct attack
 - Protest or demonstration on, or near, Company premises
 - Access requested by government authorities
- 3.8 Security plans shall be included for review as part of security risk and vulnerability assessments.

PHSE-11-C01	CONTROLLED DOCUMENT Page 6 of 10 <small>Printed copies of this document are not controlled. To verify this copy is current, check the Petroleum Portal.</small>	Rev. 1
-------------	--	--------


CONTROL 4 – PUBLIC AND PRIVATE SECURITY RESOURCES

INTENT

Effective resources are in place to protect Company personnel and property within an operating framework that upholds respect for human rights.

PERFORMANCE REQUIREMENTS

- | | |
|--|---|
| <p>4.1 Public security resources or private security companies (PSC) should be used to provide site based security and response services:</p> <ul style="list-style-type: none"> - Public security forces should provide general area security outside the perimeters of Company sites and respond to security incidents in accordance with their jurisdiction. - PSCs should be tasked with provision of direct security support to Company activities and in response to specific incidents or alarms. <p>4.2 Public or private security resources shall be assessed to ensure core values are consistent with the Company's values and must comply with all relevant Company policies and applicable laws including, without limitation:</p> <ul style="list-style-type: none"> - The US Foreign and Corrupt Practices Act (FCPA) and all other relevant anti-corruption laws - The Voluntary Principles on Security and Human Rights (VPSHR) <p>4.3 Any engagement of services from a PSC shall be covered by an appropriate contract which must include:</p> <ul style="list-style-type: none"> - Description of the services to be performed with key performance indicators (KPIs). - Obligation to comply with all relevant Company policies and applicable laws. - Obligation to provide detailed site instructions, in writing, covering all services to be provided. <p>4.4 If public security forces are engaged to provide security services in direct support of Company operations, outside of their normal duties, then a formal contract or agreement must be established.</p> <p>4.5 In the event that a combination of public and private security resources is used, clear delineation of jurisdiction and responsibilities must be established and documented within security plans.</p> <p>4.6 Public security forces should only be requested to enter Company sites in response to security incidents and to uphold the law in accordance</p> | <p>with their jurisdiction. Appropriate Line Managers and SFP(s) shall be notified immediately upon the arrival of any public security force at a Company site.</p> <p>4.7 Human rights records and any complaints shall be investigated prior to contracting any security resource and monitored throughout any contract period by the SFP with any breaches, or suspected breaches, reported to the appropriate Senior Line Manager and Petroleum Asset Protection.</p> <p>4.8 Any intended engagement of a public or private security resource that does not comply with the VPSHR must be approved by the Chief Executive Petroleum.</p> <p>4.9 Security resources must demonstrate core competencies specific to the role and service that they are expected to provide in advance of contracts being awarded.</p> <p>4.10 PSCs must be appropriately licensed and authorized to operate in the country and specific location where services are required.</p> <p>4.11 Armed security services must comply with the Petroleum Firearms Management Procedure.</p> <p>4.12 Individual security resources and guards operating for a PSC shall undergo background screening and criminal record check prior to employment in support of the Company.</p> <p>4.13 Security resources shall undergo a full site orientation and familiarization with site specific procedures and policies prior to providing services to the Company.</p> <p>4.14 KPI progress shall be recorded by the PSC, monitored by security focal points and formally assessed by the appropriate Company Security or HSE Manager approximately every six months.</p> <p>4.15 Any change in PSC manning levels or providers at a Company site shall be subject to the Management of Change process and a security risk assessment shall be conducted.</p> |
|--|---|

Petroleum	Health, Safety & Environment Management System Security and Emergency Management	 bhpbilliton resourcing the future
------------------	---	--

CONTROL 5 – SECURITY TRAINING AND AWARENESS

INTENT

All personnel understand their personal responsibilities, are aware of security risks and are competent to perform specific security duties.

PERFORMANCE REQUIREMENTS

Site Specific Training

5.1 All employees and visitors should receive an appropriate site specific security briefing as part of the HSE induction and orientation process.

- 5.2 Site specific security briefings should include:
- An overview of local security risks
 - An overview of security controls in place
 - Personal responsibilities for preservation of security and incident reporting.
 - Detail of relevant security incident response actions including:
 - o Workplace violence
 - o Unauthorized access / intruder
 - o Theft
 - o Receipt of threats
 - o Security alarms

5.3 An annual security drill shall be conducted in accordance with the site security plan.

Security Awareness Training

5.4 All employees should receive general security awareness training annually.

5.5 All personnel working at marine facilities shall receive specific marine security awareness training in alignment with ISPS Code.

- 5.6 General security awareness training should include:
- Individual responsibilities
 - Personal security and situational awareness
 - Travel security
 - Information security
 - Internet / email security

Personnel with Security Duties

5.7 Personnel with security duties shall be suitably trained and competent to perform their duties as documented in security plans, standard operating procedures and emergency response plans.

5.8 Personnel involved in access control or surveillance duties shall receive specific security training including situational awareness, behavioral recognition and screening techniques.

5.9 Operators of CCTV systems shall be appropriately trained and licensed in accordance with local laws or regulations.

5.10 Personnel with mail handling duties shall be trained in the use of mail screening equipment and recognition of, and response to, suspicious mail and packages.

Security Resource Training

5.11 Security resources should be trained in the following core competencies prior to providing services at a Company site:

- First Aid
- Basic Firefighting
- Jurisdiction and the law in relation to criminal incidents and the powers of security officers
- Voluntary Principles on Security and Human Rights
- Force continuum and use of force guidelines
- Access controls, screening and search techniques
- Recognition of dangerous or prohibited items
- Surveillance and patrol techniques
- Theft prevention and property controls
- Communications equipment and protocols
- Incident and emergency response and investigation
- Preservation of evidence and chain of custody
- Report Writing

5.12 Security resources shall undergo periodic refresher and continuation training on core competencies and site specific procedures.

5.13 Training records shall be maintained by the PSC and made available to the Company upon request.

PHSE-11-C01	CONTROLLED DOCUMENT Page 8 of 10 <small>Printed copies of this document are not controlled. To verify this copy is current, check the Petroleum Portal.</small>	Rev. 1
-------------	--	--------

CONTROL 6 – CRISIS AND EMERGENCY MANAGEMENT

INTENT

Effective plans and resources are in place to respond to crisis or emergency situations mitigate the impact on people, the environment, assets and reputation and, assist recovery.

PERFORMANCE REQUIREMENTS

Crisis & Emergency Management Resources

- | | |
|--|--|
| <p>6.1 A tiered crisis and emergency management (CEM) organization shall be used to respond to crisis and emergency situations according to the severity of the incident.</p> <p>6.2 In the event an incident causes significant impact and interruption to normal business operations the CEM resources shall be augmented or replaced by a broader business continuity team to maintain critical processes and manage the recovery and resumption of normal business operations.</p> <p>6.3 A Field or Facility Response Team (FRT) shall be identified for each Company site and operational activity, to provide immediate response to control and contain the source of the incident or emergency.</p> <p>6.4 An Incident Management Team (IMT) shall be established within each Production Unit (PU) and main country office to manage the incident within the PU or country of operations and support respective FRTs.</p> <p>6.5 A single Emergency Management Team (EMT) shall be established in the Petroleum headquarters to manage the strategic response for incidents that have significant impact (or potential impact) to the business and support respective IMTs.</p> <p>6.6 All CEM teams shall establish and maintain adequate primary and secondary resources, including equipment and facilities, to respond to an incident on a 24/7 basis.</p> | <p>6.10 Communication protocols and media releases shall follow Petroleum External Affairs approvals processes.</p> <p>6.11 IMTs shall produce a weekly operations summary to the EMT via FPe.</p> <p>6.12 An incident briefing document shall be produced for any incident requiring IMT or EMT response.</p> |
|--|--|

Activation Criteria

- 6.13 FRTs should respond immediately to any incident or emergency on site and notify the corresponding IMT as soon as it is safe to do so.
- 6.14 IMTs should mobilize for any incident with a potential consequence severity level of 3 or above (as defined by the Petroleum HSE Risk Matrix Procedure) and when deemed necessary by the IMT Leader.
- 6.15 IMTs shall inform the EMT Leader of any mobilization as soon as possible and discuss any support requirements of the EMT.
- 6.16 The EMT should mobilize for any incident with a potential consequence severity level of 4 or above and when deemed necessary by the EMT Leader.
- 6.17 The EMT Leader shall inform the Chief Executive Petroleum of any incident requiring EMT mobilization as soon as possible.

Training

- 6.18 CEM teams shall develop a training schedule and co-ordinate joint training with Petroleum Asset Protection at the frequency listed below:

Team	Induction Role Trg	Test Call Out	Desk Top Exercise	Full Exercise
FRT	-	Weekly	6 per year	1 per year
IMT	-	Weekly	4 per year	1 per year
EMT	-	Weekly	3 per year	1 per year
Individual	On joining	-	Annual	Every 2 years

Plans and Reports

- 6.7 Approved emergency response plans shall be developed to cover all operational activities in compliance with the Petroleum CEM Procedure.
- 6.8 Oil spill response plans and resources shall be scaled according to the associated risk in accordance with the Petroleum Oil Spill Contingency Procedure.
- 6.9 IMT and EMT level stakeholder management plans shall be developed and maintained with up to date information.

APPENDIX A: SECURITY AND EMERGENCY MANAGEMENT APPROVALS FRAMEWORK¹

	Country / PU / Project Security Mgr	Country / PU / Project HSE Mgr	Asset Protection	Divisional HSE Mgr	Country / PU / Project Mgr	VP HSE	Legal	Head of Gp HSEC	Division President	CSG President
1. Selection and appointment of Security or CEM employees or contractors.	R	R	E	As required by Petroleum HR Approvals Framework.						
2. Selection and appointment of security or CEM consultants or service providers, including training.	R	R	E	I	A		E ²			
3. Engagement of any security provider not compliant with the Voluntary Principles on Security and Human Rights.	R	R	E	I	R	E	E		I	A
4. Design or modification of physical and technical site security controls.	R	R	E		A					
5. PU, Project or Country level security procedures and plans.	R	R	E	I	A					
6. FRT Procedures and plans.	R	R			A					
7. IMT procedures and plans.	R	R	E	I	A					
8. EMT procedures and plans.			R	I		E			I	A
9. PU, Project or Country level journey management procedures.	R	R	E	I	A					
10. Safe travel plans for travel in high , or extreme, risk areas without established Production Units or Project Controls.		R	E	I					A	A ³
11. Security response levels higher than Amber and any reduction in the security response level. (Security Response Levels are defined in the Petroleum Site Security Procedure)	R	R	E		A	I			IA ₄	A ⁵
12. Security risk assessments, if performed by an external agency or non-Asset Protection personnel.	R	R	A	I	I					
13. Deployment of firearms in support of Petroleum operations.	R	R	E	I	R	E	E	E	A	A

R – Recommend E – Endorse I – Informed A - Approve

¹ These approvals are intended in addition to normal approvals required by the Petroleum Approvals Framework.

² Legal endorsement may be required for contracting of specific security services.

³ CSG President approval required for travel to destinations rated as Extreme risk.

⁴ Division President to be informed of any increase in security response level and approve any reduction

⁵ The CSG President must approve any increase or reduction in security response level to, or from, Black.