

.....
(Nome della Nave)

.....
(Nome della Compagnia)

(fare rif.to ai dati che saranno contenuti nel "Continuous Synopsis Record richiesto dalla Solas XI-1/5")

PIANO SECURITY NAVE

(Ship Security Plan)

Conforme alla SOLAS 74 Capitolo XI-2 e al Codice Internazionale per la Sicurezza delle Navi e degli Impianti Portuali (ISPS Code)

Emesso il

.....
Preparato da

(Responsabile Security della Compagnia "Company security Officer (CSO)" nome e firma)

.....
Copia Controllata nr. di copie

Rilasciata a (vedere Cap. 16 per elenco distribuzione))

.....
Estremi Approvazione

.....(Autorità che procede all'approvazione)
.....(Data di approvazione)

Le informazioni contenute nel presente piano sono strettamente confidenziali e di proprietà della Compagnia. Divulgare informazioni su questo piano è proibito ed eventuali informazioni possono essere divulgate solo se autorizzate dal Comandante e/o CSO e/o SSO.

(tenere conto di quanto indicato nel ISPS Code Parte A paragrafo 9.8 e 9.8.1)

Politica sulla Security

Solas Chapter XI-2, ISPS Code Part A:

6.1 La società provvede affinché il piano di sicurezza della nave contenga una dichiarazione chiara che metta in rilievo l'autorità del Comandante. La società stabilisce nel piano di sicurezza della nave che il Comandante è investito della massima autorità e responsabilità di decidere per quanto riguarda la sicurezza a bordo e di richiedere l'assistenza della compagnia o di qualunque governo contraente nella misura del necessario.

6.2. La compagnia provvede affinché il CSO, il Comandante e l'SSO della nave ricevano il sostegno necessario per eseguire i loro compiti e responsabilità conformemente al capitolo XI-2 e alla presente parte del Codice.

Deve essere definita la politica sulla Security della Compagnia che gestisce la nave che dovrebbe essere complementare a quella sulla Sicurezza e per la protezione ambientale come ad esempio:

La politica si riferisce alle navi gestite dalla societàda qui in avanti chiamata "Compagnia."

La Compagnia, ben consapevole delle proprie responsabilità in questo campo, pone il massimo impegno nella Sicurezza, nella protezione dell'Ambiente e nella Security applicata alle navi gestite.

La Compagnia stabilisce che tutte le operazioni effettuate dal proprio personale, sia a terra che a bordo le navi, dovranno mettere in evidenza l'impegno affinché gli obiettivi aziendali, sia quelli relativi alla Sicurezza, che quelli relativi alla Security, elencati di seguito in ordine di priorità, siano raggiunti:

- *proteggere le navi e gli equipaggi dalle conseguenze di pratiche illegali, prevenendo eventuali attacchi terroristici o criminali*
- *operare le navi e trattare il carico in maniera sicura*
- *mantenere al massimo livello l'efficienza tecnica ed operativa delle navi*
- *evitare danni alle persone ed alle cose*
- *promuovere la conoscenza della Security tra tutto il proprio personale.*

La Compagnia stabilisce che in caso di conflitto tra ragioni economiche o commerciali e i punti di cui sopra, il Comandante decida dando priorità a questi ultimi. In particolare rientrano tra tali decisioni il rifiuto di salire a bordo a persone (ad eccezione di quelle identificate come debitamente autorizzate da un Governo contraente) e il rifiuto di caricare a bordo merci, ivi compresi container ed altre unità di trasporto chiuse.

Per raggiungere i sopra menzionati obiettivi, la Compagnia si impegna a fornire le necessarie risorse e personale qualificato, definendo la propria organizzazione, identificando specifici compiti e responsabilità, stabilendo requisiti di addestramento e coordinando tutte le attività in modo da:

- *garantire la sicura operatività delle navi in conformità alle norme ed ai regolamenti di legge nazionali ed internazionali applicabili;*
- *stabilire contromisure contro tutti i rischi identificati, provvedendo a mitigare quelli con livelli troppo alti;*
- *migliorare continuamente la preparazione tecnica e l'efficienza operativa del personale di bordo e di terra;*
- *mantenere al massimo livello il grado di manutenzione delle navi gestite;*
- *essere sempre pronti, sia a terra che a bordo, ad affrontare situazioni di emergenza.*

Per quanto riguarda la gestione operativa delle navi, e' sottinteso che e' il Comandante, secondo il suo giudizio professionale, ad avere l'autorità di agire ed impartire gli ordini necessari per la salvaguardia della vita umana, per la sicurezza della nave, per la protezione dell'ambiente e della security, siano essi in accordo o meno con le procedure ed istruzioni fornite dalla Compagnia, dal noleggiatore o da terzi.

Il Comandante dovrà in ogni caso comunicare immediatamente alla Compagnia ogni incidente o non-conformità che possa compromettere la sicurezza delle persone, della nave o che possa determinare un inquinamento all'ambiente. A tale scopo sono previste adeguate risorse umane e mezzi materiali.

La Compagnia riesamina periodicamente l'efficace applicazione della politica, in modo da assicurare che gli obiettivi prefissi siano raggiunti e che le procedure ed istruzioni siano adeguate ed efficaci.

Approvato

.....

Presidente (Amm. Delegato)

Data.....

Emesso da	Approvato da:	Data	Revisione 0	Pagina 1 di 3
PIANO SECURITY(NAVE)				
INDICE				
<i>Riferimento: SOLAS 74 Capitolo XI-2 e del Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				

CAPITOLO	TITOLO
0	DEFINIZIONI E ACRONIMI
1	DETTAGLI NAVE
1.1	Dati nave
17.1	Piani nave
1.3	Servizi
2	ORGANIZZAZIONE PER LA SECURITY
2.1	Generalità
2.2	Lingua di lavoro
2.3	Struttura organizzativa per la Security
2.4	Company Security Officer
2.5	Comandante
2.6	Ship Security Officer
2.7	Compiti del personale di bordo
Appendice 1	Struttura organizzativa per la Security
3	ADDESTRAMENTO, PROVE ED ESERCITAZIONI
3.1	Generalità
3.2	Formazione del Company e Ship Security Officer
3.3	Formazione del Personale di Bordo
3.4	Programma, prove ed esercitazioni
3.5	Gruppo di emergenza a terra
4	REGISTRAZIONI E DOCUMENTAZIONE
4.1	Generalità
4.2	Registrazioni
4.3	Conservazione ed archiviazione
4.4	Documentazione
4.5	Norme internazionali, europee e nazionali
5	LIVELLI SECURITY
5.1	Generalità
5.2	Livelli di Security
5.3	Attività non contemplate dall' ISPS Code
6	INTERFACCE CON AUTORITA', PORTI, IMPIANTI PORTUALI ED ALTRE NAVI
6.1	Generalità
6.2	Governi Contraenti ed Amministrazione di Bandiera
6.3	Porti
6.4	Impianto Portuale
6.5	Operazioni con altre navi
6.6	Attività non contemplate dal ISPS Code
6.7	Comunicazioni in situazioni di emergenza

Emesso da	Approvato da:	Data	Revisione 0	Pagina 2 di 3
PIANO SECURITY(NAVE)				
INDICE				
<i>Riferimento: SOLAS 74 Capitolo XI-2 e del Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				

7	DICHIARAZIONE DI SECURITY
17.1	Generalità
17.2	Governi Contraenti
17.3	Nave
8	SISTEMI DI COMUNICAZIONE
8.1	Generalità
8.2	Responsabilità delle comunicazioni
8.3	Segretezza delle comunicazioni
8.4	Radiocomunicazioni interne a bordo
9	DOTAZIONI ED EQUIPAGGIAMENTI PER LA SECURITY
9.1	Generalità
9.2	Dotazioni ed equipaggiamenti
10	CONTROLLO ACCESSI
10.1	Generalità
10.2	Punti di accesso
10.3	Controllo accessi
10.4	Controllo persone all'imbarco incluso bagagli e bagaglio non accompagnato
10.5	Controllo scalandroni
10.6	Controllo biscagline
10.7	Controllo Portelloni laterali
10.8	Controllo rampe
10.9
11	AREE AD ACCESSO LIMITATO E MONITORAGGIO
11.1	Generalità
11.2	Aree ad Accesso Limitato (Restricted Areas)
11.3	Punti Vulnerabili
11.4	Sistemi di chiusura accessi
11.5	Monitoraggio aree ad accesso limitato
12	CONTROLLO OPERAZIONI DEL CARICO
12.1	Generalità
12.2	Controllo operazioni del carico
13	CONTROLLO OPERAZIONI IMBARCO FORNITURE DI BORDO
13.1	Generalità
13.2	Controllo operazioni forniture di bordo
14	MONITORAGGIO SECURITY NAVE
14.1	Generalità
14.2	Controlli
15	PROCEDURE PER RISPONDERE ALLE MINACCE E VIOLAZIONE DELLA SECURITY
15.1	Generalità
15.2	Rapportazione

Emesso da	Approvato da:	Data	Revisione 0	Pagina 3 di 3
PIANO SECURITY(NAVE)				
INDICE				
<i>Riferimento:</i> SOLAS 74 Capitolo XI-2 e del Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)				

16	AUDITS E REVISIONI DEL PIANO SECURITY NAVE
16.1	Generalità
16.2	Lista di distribuzione controllata
16.3	Riesame
16.4	Audit Interni
16.5	Gestione rilievi
17	VALUTAZIONE SECURITY NAVE
17.1	Valutazione Security nave
17.2	Riesame

Emesso dal	Approvato da	Data	Revisione 0	Pagina 1 of 2
PIANO SECURITY.....(NAVE) DEFINIZIONI ED ACRONIMI				CAP. 0
<i>Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				

Incidente di Security

Qualsiasi atto o circostanza sospetti che minaccino la security di una nave, ivi comprese le unità mobili di perforazione offshore e le unità ad alta velocità, ovvero la security di un impianto portuale o di un'interfaccia nave/porto o di un'attività da nave a nave

Amministrazione

Ministero delle Infrastrutture e dei Trasporti

Audit

E' un controllo sistematico per accertare se le attività previste dal Security plan vengono applicate efficacemente e sono idonee per il raggiungimento degli obiettivi che il piano si propone.

Verifica

Attività di controllo ai sensi dell' ISPS Code Parte A Sezione A/19.1

Auditor interno

Una persona della Compagnia qualificata per effettuare verifiche interne di conformità alle pertinenti norme di security

Compagnia

L'Armatore o qualsiasi organizzazione o persona (es:il gestore oppure il Noleggiatore a scafo nudo,) che ha assunto dall'Armatore la responsabilità di gestire la nave per conto dell'armatore e che, assumendo tale responsabilità, ha convenuto di assumere tutti i compiti e le responsabilità imposte dal codice ISM e dall' ISPS Code

Ufficiale di Security della Compagnia (Company Security Officer)

E' la persona designata dalla compagnia per effettuare la valutazione della security della nave, per elaborare il piano di security della nave, provvedere alla sua presentazione per approvazione e curarne poi l'attuazione e l'osservanza, e infine per fungere da collegamento con gli ufficiali di security del porto, con l'ufficiale di security della nave e con le autorità.

Ufficiale di Security della nave (Ship Security Officer)

E' la persona a bordo della nave, che risponde al Comandante ed è designata dalla compagnia come responsabile della security della nave, e in particolare dell'attuazione e del rispetto del piano di security della nave, e come collegamento con il Company Security Officer e con il Port Facility Officer dell'impianto portuale.

Ufficiale di Security dell'impianto portuale (Port Facility Security Officer)

E' la persona designata come responsabile dell'elaborazione, attuazione, riesame e rispetto del piano di security dell'impianto portuale e come collegamento con gli Ship Security Officers delle navi e con i Company Security Officers delle Compagnie.

Emesso dal	Approvato da	Data	Revisione 0	Pagina 2 of 2
PIANO SECURITY.....(NAVE)				CAP.
DEFINIZIONI ED ACRONIMI				0
<i>Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				

Interfaccia nave/porto *Significa le interazioni che hanno luogo quando una nave è direttamente ed immediatamente interessata da azioni che comportano il movimento di persone, di merci o la fornitura di servizi portuali alla nave o dalla nave.*

Impianto portuale *E' una località, individuata dal Governo Contraente o dall'Autorità designata, nella quale ha luogo l'interfaccia nave/porto. Essa comprende aree come le zone di ancoraggio, banchine di sosta e gli specchi acquei di avvicinamento, a seconda dei casi.*

Attività da nave a nave *Significa ogni attività non connessa ad un impianto portuale che implichi il trasferimento di merci o persone da una nave all'altra.*

Autorità designata *Significa l'organizzazione (o le organizzazioni) o l'amministrazione (o le amministrazioni) cui il Governo Contraente abbia affidato il compito di far osservare le disposizioni relative alla sicurezza dell'impianto portuale e all'interfaccia nave/porto, dal punto di vista dell'impianto portuale.*

Codice ISPS (International Ship and Port Facility Security Code) *Significa il Codice internazionale per la sicurezza delle navi e degli impianti portuali, comprendente una parte A (le cui disposizioni hanno natura cogente) e una parte B (le cui disposizioni hanno natura cogente per alcuni paragrafi e di raccomandazione per altri) adottato il 12 dicembre 2002 con la risoluzione n. 2 della Conferenza dei Governi Contraenti della Convenzione internazionale del 1974 per la salvaguardia della vita in mare, così come emendato e per quanto applicabile.*

Livello di sicurezza *Significa la qualificazione del grado di rischio (probabilità/gravità delle conseguenze) relativo ad un incidente di security.*

Dichiarazione di Sicurezza *E' l'accordo raggiunto tra una nave da un lato e, dall'altro, un impianto portuale o un'altra nave con cui essa si interfaccia, nel quale sono specificate le misure di security che ciascuna delle parti attuerà*

Organizzazione di sicurezza riconosciuta *E' un'organizzazione dotata di adeguata esperienza nelle questioni legate alla security e di conoscenza adeguata del porto e delle operazioni portuali, autorizzata ad effettuare un'attività di valutazione o di verifica o di approvazione o di certificazione prescritta dal Capitolo XI-2 della SOLAS 74 e dal Codice ISPS.*

Acronimi

SSP	<i>Ship Security Plan</i>
SSA	<i>Ship Security Assessment</i>
DoS	<i>Declaration of Security</i>
CSO	<i>Company Security Officer</i>
SSO	<i>Ship Security Officer</i>
PFSO	<i>Port Facility Security Officer</i>
AIS	<i>Automatic Identification System</i>
SSAS	<i>Ship Security Alert System</i>

L'elenco delle definizioni/acronimi può essere completato come appropriato facendo riferimento alla SOLAS Cap. XI-2 Regola 1 e l' ISPS Code Parte A

Emesso da	Approvato	Data	Revisione 0	Pagina 1 di 1
PIANO SECURITY(NAVE) DETTAGLI NAVE <i>Riferimento</i> : SOLAS 74 Capitolo XI-2 e del Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)				CAP. 1

1.1 Dati nave

Devono essere inserite le caratteristiche nave e relativi dettagli ed informazioni per la Security a bordo.

1.2 Piani Nave

Devono essere inseriti, come minimo: 1) Piano Generale della nave, 2) Piano riportante le Aree ad Accesso limitato, 3) Piano dei Punti di Accesso, 4) Piano riportante ubicazione delle dotazioni di security.
 Dovrebbe essere fatta particolare attenzione sull'identificazione degli accessi alla nave (es.: portelloni, rampe, scalandroni ecc.), le aree ad accesso limitato (restricted areas) quali Ponte di Comando, Sala Macchine, Stazione radio, locale elica prodiera/poppiera, locale diesel emergenza, stazione controllo del carico, locali ventilazione in generale, casse acqua e fuel, locale timoneria, locale CO2, area del ponte dedicata ad operazioni con elicotteri, ecc., posizione del Ship Security Alert System (SOLAS Cap. XI-2 Reg. 6i punti considerati vulnerabili e su altre dotazioni come l'Automatic Identification System.

1.3 Servizi

Dettagli particolareggiati potrebbero essere un allegato al piano tenendo in considerazione fattori come il cambio viaggi, noleggiatore ecc.). Al riguardo vedere anche Capitolo "Interfacce con Autorità, porti, impianti portuali e altre navi".

La nave adibita al trasporto di....., effettua viaggi (regolari/spot etc.) nelle aree di..... e viene utilizzata dai noleggiatori:

Il Company Security Officer provvede a mantenere aggiornati i dettagli di quanto sopra indicato.

Emesso da	Approvato	Data	Revisione 0	Pagina 1 di 5
PIANO SECURITY(NAVE) ORGANIZZAZIONE PER LA SECURITY				CAP. 2
<i>Riferimento</i> : SOLAS 74 Capitolo XI-2 e del Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)				

Devono essere indicati tutti gli aspetti dell'organizzazione a bordo ed in Compagnia per la gestione della Security come individuazione delle persone e relativi dettagli, responsabilità, autorità ecc (fare riferimento anche al Manuale ISM), in conformità a quanto richiesto dal ISPS Code Parte A Sez. 9.4.7 e tenendo conto della guida fornita nella Parte B para. 9.2.1 e 9.7.1. Esempio:

2.1 Generalità

La Compagnia è :(riportare i data come da DOC integrati da informazioni di interesse per la security).

La Compagnia attraverso l'Amm.re Delegato (o altro) ha designato il/i Company Security Officer/s (CSO) come indicato nel seguito.

La Compagnia ha notificato all'.....(Amministrazione(i) interessata(e),le generalità e i dettagli del Company Security Officer che ha assunto tutti i compiti e le responsabilità imposte dal Codice ISPS.

Per la nave lo Ship Security Officer (SSO) è il(indicare grado e posizione).

2.2 Lingua di lavoro

La lingua formale di lavoro negli uffici della compagnia è.....ma tutti i capi Dipartimento, il/i CSO, gli Ispettori delle navi e gli Auditors interni hanno buona conoscenza della lingua inglese.

La documentazione del Piano emessa dal CSO (registrazioni, procedure, lettere circolari, memorandums, rapporti, comunicazioni ecc.) per gli uffici sarà in.....e.....(specificare lingua/e).

A bordo di navi passeggeri incluso navi ro-ro, la lingua comune di lavoro sarà quella debitamente registrata dal Comandante nel Giornale Nautico parte II.

2.3 Struttura organizzativa per la Security

L'organizzazione della Compagnia e a bordo della nave per la security è quella indicata nell'Organigramma dell'Appendice 1.

L'Amministratore Delegato (o altro rappresentante della Direzione) ha designato il/i Company Security Officer/s (CSO) per mezzo di una comunicazione scritta.

Egli provvede ,inoltre, a far fronte l'eventuale necessità di risorse ed al supporto da terra per mettere in grado il/i Company Security Officer/s (CSO) di espletare le proprie funzioni.

La Compagnia dovrà conservare una "**Descrizione del Lavoro**" dove le responsabilità, autorità, interrelazioni, nonché qualifiche e livelli di esperienza richiesti per ricoprire funzioni chiave fra tutte le persone che gestiscono, effettuano e verificano attività legate alla Security sono chiaramente definite.

Emesso da	Approvato	Data	Revisione 0	Pagina 2 di 5
PIANO SECURITY(NAVE) ORGANIZZAZIONE PER LA SECURITY				CAP. 2
<i>Riferimento</i> : SOLAS 74 Capitolo XI-2 e del Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)				

2.4 Company Security Officer (CSO)

I principali doveri e responsabilità sono:

- *prestare consulenza sul livello delle probabili minacce per la nave, sulle base delle valutazioni di security ed altre informazioni pertinenti;*
- *provvedere affinché siano effettuate le valutazioni di security della nave;*
- *occuparsi dell'elaborazione, della presentazione per approvazione, e in seguito dell'attuazione e rispetto del piano di security della nave;*
- *provvedere affinché il piano di security della nave venga modificato nella misura necessaria per correggerne i difetti e rispettare i requisiti di security della singola nave;*
- *organizzare audit interni e riesami delle attività di security;*
- *organizzare la verifica iniziale da parte dell'amministrazione o dell'ente di security riconosciuto, nonché le verifiche successive;*
- *provvedere affinché le anomalie e le non conformità individuate durante gli audit interni, i riesami periodici, le ispezioni di security e le verifiche della conformità siano tempestivamente corrette;*
- *potenziare la sensibilizzazione e la vigilanza in materia di security;*
- *assicurare l'addestramento adeguato per il personale responsabile della security della nave;*
- *assicurare comunicazioni e cooperazione efficaci tra lo Ship Security Officer della nave e i competenti Port Facility Security Officers degli impianti portuali;*
- *assicurare la coerenza tra i requisiti di safety e quelli di security;*
- *provvedere affinché, se si ricorre a piani di security per tipo di nave o per la flotta, il piano per ciascuna nave rifletta accuratamente le informazioni specifiche per ciascuna nave;*
- *assicurare l'attuazione e il rispetto delle eventuali disposizioni alternative od equivalenti approvate per una particolare nave o gruppo di navi.*
- *Assicurare l'effettivo coordinamento ed attuazione del piano di security partecipando alle esercitazioni previste.*

Deve essere inserita una tabella con tutti i dettagli del CSO ed in particolare nominativo, dettagli reperibilità nelle ore di lavoro e fuori dall'orario di lavoro, nonché indicazioni relative alla formazione in materia di security.

Emesso da	Approvato	Data	Revisione 0	Pagina 3 di 5
PIANO SECURITY(NAVE) ORGANIZZAZIONE PER LA SECURITY				CAP. 2
<i>Riferimento</i> : SOLAS 74 Capitolo XI-2 e del Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)				

Questa parte dovrebbe essere complementare a quanto contenuto nel Manuale ISM e quindi dovrebbe prevedere solo i compiti relativi alla Security; è pertanto da valutare attentamente come integrare i due aspetti ISM e Security. Di seguito si elencano per guida i doveri e responsabilità sulla Security per:

2.5 Comandante

<p><i>Le autorità e responsabilità per la security sono quelle indicate nella SOLAS Chapter XI-2 Regola 8 :</i></p> <p>1. Il comandante non deve essere obbligato dalla società, dal noleggiatore o da terzi a astenersi dal prendere od eseguire decisioni che, secondo il suo giudizio professionale, siano necessarie per salvaguardare l'efficiente funzionamento della nave o la sua sicurezza. Rientrano tra tali decisioni il rifiuto di accesso a persone (ad eccezione di quelle identificate come debitamente autorizzate da un Governo Contraente) o dei loro effetti e il rifiuto di caricare a bordo merci, ivi compresi container ed altre unità di trasporto chiuse.</p> <p>2. Se, a giudizio del comandante, durante le operazioni della nave si verifica un conflitto tra prescrizioni relative alla sicurezza intrinseca della nave e prescrizioni relative alla sua protezione, il comandante dà effetto alle prescrizioni necessarie a salvaguardare l'efficiente funzionamento della nave. In tali casi, il comandante può dar corso a misure temporanee di sicurezza e ne informa immediatamente l'amministrazione e, ove opportuno, il Governo Contraente nel cui porto la nave sta effettuando le proprie operazioni o intende entrare. Tutte le misure temporanee di protezione adottate a norma della presente Regola devono, per quanto possibile, essere commisurate al livello prevalente di protezione. Quando queste eventualità sono identificate, l'amministrazione provvede affinché tali conflitti vengano risolti e sia ridotta al minimo la possibilità che si ripresentino.</p> <p><i>Tali concetti sono da sviluppare come necessario.</i></p>
--

2.6 Ship Security Officer

I principali doveri e responsabilità sono:

- *svolgere regolari ispezioni di security della nave per verificare l'osservanza costante delle misure di security necessarie;*
- *garantire osservanza e supervisione dell'attuazione del piano di security della nave, comprese eventuali modifiche del piano;*
- *coordinare gli aspetti di security della movimentazione del carico e delle provviste di bordo con il restante personale della nave e con i competenti PFSO;*
- *proporre le modifiche al piano di security della nave;*
- *comunicare al CSO le eventuali anomalie e non conformità individuate durante gli audit interni, i riesami periodici, le ispezioni di security e le verifiche della conformità ed attuare eventuali azioni correttive;*
- *potenziare la sensibilizzazione e la vigilanza a bordo in materia di security;*
- *assicurare che il personale di bordo abbia ricevuto, nella misura opportuna, un adeguato addestramento in materia di security;*

Emesso da	Approvato	Data	Revisione 0	Pagina 4 di 5
PIANO SECURITY(NAVE) ORGANIZZAZIONE PER LA SECURITY				CAP. 2
<i>Riferimento</i> : SOLAS 74 Capitolo XI-2 e del Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)				

- *comunicare gli incidenti di security;*
- *coordinare l'attuazione del piano di security della nave con il Company Security Officer e con il competente Port Facility Security Officer dell'impianto portuale;*
- *assicurare il corretto impiego, prova, calibratura e manutenzione delle attrezzature di security eventualmente presenti.*

2.7 Compiti del personale di bordo

*I compiti di Security del personale di bordo possono essere diversi a seconda del livello di security che può essere 1,2 o 3 (1: normali condizioni, 2: minaccia non specifica, 3: Specifica minaccia)
Esempio nel caso di nave in porto per l'accesso alla nave:*

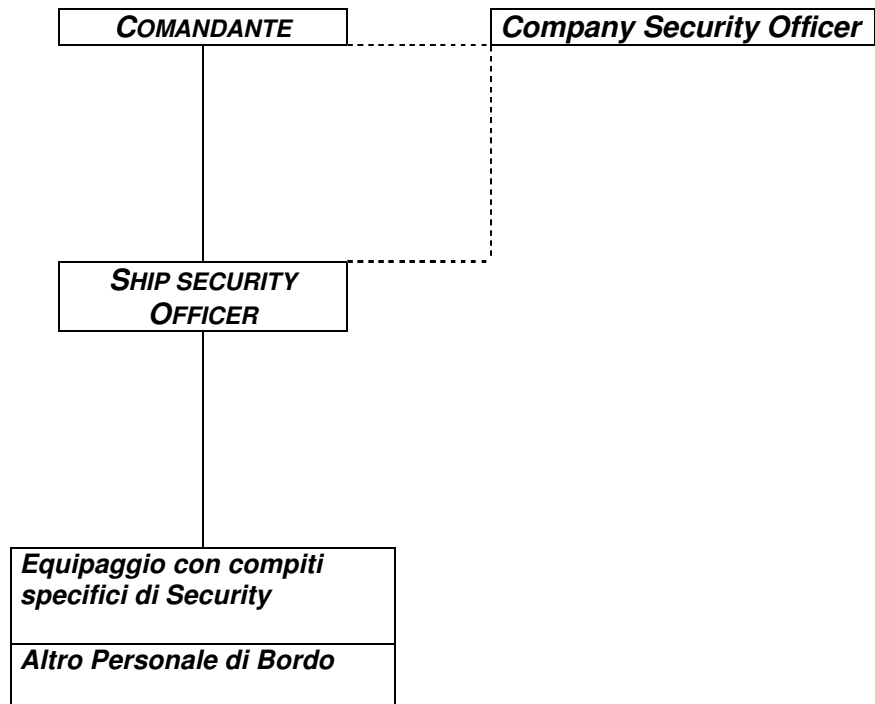
<i>Ruolo</i>	<i>Livello 1</i>	<i>Livello 2</i>	<i>Livello 3</i>
<i>3° Ufficiale</i>	<i>Nessuno</i>	<i>A disposizione a bordo</i>	<i>Rinforza zona scalandrone</i>
<i>Nostromo</i>	<i>Nessuno</i>	<i>A disposizione a bordo</i>	<i>Rinforza sorveglianza in centrale di controllo carico</i>
<i>Marinaio</i>	<i>Nessuno</i>	<i>Nessuno</i>	<i>Rinforza sorveglianza accesso nave dal lato mare</i>

(Quanto sopra è solo a titolo di esempio come metodo da applicare)

Emesso da	Approvato	Data	Revisione 0	Pagina 5 di 5
PIANO SECURITY(NAVE) ORGANIZZAZIONE PER LA SECURITY <i>Riferimento</i> : SOLAS 74 Capitolo XI-2 e del Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)				CAP. 2

Appendice 1

(NOME NAVE)..... **STRUTTURA ORGANIZZATIVA PER LA SECURITY**



Emesso da	Approvato da	Data	Revisione 0	Pagina 1 di 4
PIANO SECURITY....(NAVE) ADDESTRAMENTO, PROVE ED ESERCITAZIONI				CAP. 3
Riferimento: SOLAS 74 Capitolo XI-2 e del Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)				

Anche questo capitolo deve tenere in considerazione quanto già previsto nel Manuale ISM. Bisogna quindi definire la attività di formazione per il Company Security Officer, per lo Ship Security Officer e per il personale di bordo con compiti relativi alla security. I requisiti di riferimento sono quelli contenuti nell'ISPS Code Parte A Sez. 13 tenendo conto della guida fornita nella parte B medesimo paragrafo. Di seguito sono indicate le linee generali:

3.1 Generalità

La Compagnia ha identificato le seguenti potenziali situazioni di minaccia relative alla security a bordo che costituiscono un immediato pericolo per il personale e la nave:

- *danneggiamento o distruzione della nave o dell'impianto portuale causati, ad esempio, da ordigni esplosivi, incendi dolosi, sabotaggio o vandalismo;*
- *dirottamento o sequestro della nave o delle persone a bordo;*
- *manomissione dolosa del carico, dei sistemi o delle apparecchiature essenziali della nave o delle provviste di bordo;*
- *accesso o utilizzo non autorizzato, compresa la presenza di clandestini;*
- *contrabbando di armi o apparecchiature, tra cui armi di distruzione di massa;*
- *utilizzo della nave per trasportare persone intenzionate a causare un incidente di security e/o la loro attrezzatura;*
- *utilizzo della nave stessa come arma o come mezzo per causare danni o distruzioni;*
- *attacchi provenienti dal mare aperto mentre la nave è ormeggiata o ancorata; e*
- *attacchi mentre la nave è in mare aperto.*

Le istruzioni e le procedure per mitigare e prevenire tali situazioni possono essere trovate nel capitolo "Procedure per rispondere alle minacce e violazione della security".

Altre situazioni di minaccia possono essere identificate attraverso le analisi di incidenti, o minacce non classificate ricevute nel qual caso istruzioni, piani e procedure potranno essere preparate dalla Compagnia ed inviate ai comandi di bordo.

In aggiunta alle istruzioni e procedure prima citate, la Compagnia ha indicato nel presente piano le operazioni che devono essere effettuate per i compiti relativi alla Security assegnati al personale di bordo quali: controllo delle persone che imbarcano, controllo delle aree ad accesso limitato, controllo del carico..... (completare come applicabile)

La compagnia riconosce che solo attraverso un piano di formazione ed addestramento specifico sulla security a bordo può raggiungere la conformità ai requisiti imposti dal ISPS Code. Di seguito vengono

Emesso da	Approvato da	Data	Revisione 0	Pagina 2 di 4
PIANO SECURITY....(NAVE) ADDESTRAMENTO, PROVE ED ESERCITAZIONI				CAP. 3
<i>Riferimento: SOLAS 74 Capitolo XI-2 e del Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				

indicate le attività formative ed il piano di addestramento per il Company Security Officer, lo Ship Security Officer ed il personale di bordo (per i compiti vedasi Capitolo "Organizzazione per la Security")

3.2 Formazione del Company Security Officer e Ship Security Officer

Il Company Security Officer e lo Ship Security Officer ricevono adeguata formazione in accordo all'ISPS Code Parte A Sez. 13.1 e 13.2 tenendo conto della guida fornita nella parte B medesimi paragrafi. Detta formazione viene effettuata utilizzando personale con le dovute competenze e conoscenze sulle problematiche relative alla Security.
Evidenza della formazione di cui sopra viene mantenuta dalla Compagnia e dal personale così istruito. Da mantenere registrazione della formazione ricevuta. Per il personale di bordo di seguito un esempio:

3.3 Formazione del Personale di Bordo

Il personale di bordo con compiti specifici sulla security viene opportunamente addestrato dallo Ship Security Officer al fine di garantire:

- *conoscenza delle varie forme di minaccia alla security;*
- *riconoscimento ed identificazione di armi, sostanze e apparecchiature pericolose;*
- *riconoscimento delle caratteristiche e dei modelli comportamentali delle persone che possono costituire una minaccia per la security;*
- *tecniche utilizzate per aggirare le misure di security;*
- *tecniche di gestione e di controllo della folla;*
- *comunicazioni di security;*
- *conoscenza delle procedure e dei piani di emergenza;*
- *funzionamento delle apparecchiature e dei sistemi di security;*
- *collaudo, taratura e manutenzione in mare delle apparecchiature e dei sistemi di security;*
- *tecniche di ispezione, verifica, controllo e sorveglianza delle persone, degli effetti personali, dei bagagli, del carico e delle provviste di bordo.*

Il restante personale deve avere conoscenza e familiarità con le pertinenti disposizioni di questo piano come:

Emesso da	Approvato da	Data	Revisione 0	Pagina 3 di 4
PIANO SECURITY....(NAVE) ADDESTRAMENTO, PROVE ED ESERCITAZIONI				CAP. 3
<i>Riferimento: SOLAS 74 Capitolo XI-2 e del Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				

- *significato ed implicazioni dei vari livelli di security;*
- *conoscenza delle procedure e dei piani di emergenza;*
- *riconoscimento ed individuazione di armi, sostanze e apparecchiature pericolose;*
- *riconoscimento, su una base non discriminatoria, delle caratteristiche e dei modelli comportamentali delle persone che potrebbero costituire una minaccia per la security; e*
- *tecniche utilizzate per aggirare le misure di security.*

3.4 Programma, prove ed esercitazioni

<p>Al fine di addestrare il personale di bordo a fronteggiare queste situazioni, si ritiene necessario effettuare esercitazioni di security almeno una volta ogni mese per garantire un'efficace applicazione delle disposizioni del piano di security della nave. Inoltre, in caso di sostituzione, in un'unica volta, di oltre il 25% del personale con personale che non ha partecipato ad una precedente esercitazione a bordo della nave nel corso degli ultimi tre mesi, dovrà essere effettuata un'esercitazione nel corso della prima settimana che segue il cambiamento di personale. L'esercitazione deve servire a mettere alla prova i singoli elementi del piano di security, in particolare quelli relativi alle minacce per la security sopra elencate.</p> <p>Almeno una volta ogni anno civile e in ogni caso ad intervalli non superiori a 18 mesi, devono essere effettuate esercitazioni complesse che possono coinvolgere il Company Security Officer, il Port Facility Security Officer, lo Ship Security Officer, l'Autorità competente del Governo Contraente. Gli addestramenti devono servire a mettere alla prova le comunicazioni, il coordinamento, la disponibilità delle risorse e le reazioni. Gli addestramenti possono consistere in:</p> <ul style="list-style-type: none"> • esercitazioni su grande scala o in situazione reale; • simulazioni teoriche o seminari; o • essere associati ad altri tipi di addestramento, ad esempio alle operazioni di ricerca e di salvataggio o di intervento di emergenza. <p>Le esercitazioni devono essere registrate.</p> <p>Il Company Security Officer e lo Ship Security Officer sono responsabili di preparare il relativo programma.</p> <p>Si indica in tabella un metodo da utilizzare ricordando che è solo un esempio e l'elenco delle attività non esaustivo. Inoltre modifiche ai piani di add.to potrebbero essere necessarie in relazione ad eventuali modifiche della STCW per l'argomento formazione del personale navigante sulla Security:</p>
--

Emesso da	Approvato da	Data	Revisione 0	Pagina 4 di 4
PIANO SECURITY....(NAVE) ADDESTRAMENTO, PROVE ED ESERCITAZIONI				CAP. 3
<i>Riferimento: SOLAS 74 Capitolo XI-2 e del Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				

Programma addestramento, esercitazioni e prove

Attività	Personale coinvolto
Livelli di Security	Tutto il personale
Tecniche di ispezione, verifica, controllo e sorveglianza delle persone, degli effetti personali, dei bagagli, del carico e delle provviste di bordo.	Ufficiali di Guardia e Personale addetto al controllo persone
Tecniche di gestione e di controllo della folla	Ufficiali, personale addetto a compiti specifici di security
Tecniche utilizzate per aggirare le misure di security	Tutto il personale
Prove ed esercitazioni	
Atti di pirateria in mare aperto	Ufficiali di guardia e personale assegnato
Evacuazione nave per bomba	Tutto il personale

(Quanto sopra è solo a titolo di esempio come metodo da applicare)

Emesso da	Approvato da	Data	Revisione 0	Pagina 1 di 3
PIANO SECURITY(NAVE) REGISTRAZIONI E DOCUMENTAZIONE				CAP. 4
Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)				

Le registrazioni relative alle attività di security a bordo devono essere identificate in accordo a quanto indicato dall'ISPS Code Parte A Sez. 10 e tenendo conto della guida fornita nella parte B medesima numerazione. Esempio:

4.1 Generalità

I documenti e le registrazioni delle attività per la security possono essere cartacei e/o computerizzati.

Nel caso di documenti su supporto informatico bisogna descrivere i sistemi utilizzati per proteggere i documenti dall'accesso non autorizzato, dalla distruzione o modifica degli stessi (es. pdf file).

Le registrazioni sono tutte in lingua italiana/inglese.

Il Company Security Officer e lo Ship Security Officer sono responsabili di effettuare l'archiviazione delle registrazioni in accordo a questo capitolo.

In alcuni casi le registrazioni delle attività avvengono a mezzo moduli che sono identificati da un codice e/o titolo e dal numero e data di revisione

Il Company Security Officer fornisce ad ogni nave un fascicolo contenente la lista dei forms e, quando necessario, le istruzioni per la loro compilazione.

Chiunque ritenga che i moduli esistenti debbano essere modificati o che altri moduli debbano essere aggiunti, dovrà darne comunicazione al Company Security Officer che provvederà come appropriato.

Nessuno è autorizzato a modificare o predisporre moduli di sua iniziativa. Eventuali informazioni non considerate dal modulo esistente, potranno essere fornite per mezzo di una nota scritta.

I moduli superati devono essere eliminati.

4.2 Registrazioni

4.2.1 Nave (Ship Security Officer)

- *Formazione, addestramento ed esercitazioni*
- *Incidenti e violazioni della Security*
- *Cambiamenti del livello di Security*
- *Comunicazioni relative alla security della nave e/o del porto/impianto portuale dove la nave si trova, e o si trovava*
- *Registrazioni relative alla prova, manutenzione, calibratura e sostituzione delle dotazioni ed equipaggiamenti per le attività di security e relativo inventario materiale di rispetto*
- *Minacce sulla security*
- *Dichiarazioni di Security*
- *Registrazioni degli approdi nave (ultimi dieci approdi)*
- *Rapporti audits interni*
- *Riesami periodici Valutazione Security e Piano Security e revisioni*

Emesso da	Approvato da	Data	Revisione 0	Pagina 2 di 3
PIANO SECURITY(NAVE) REGISTRAZIONI E DOCUMENTAZIONE <i>Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				CAP. 4

4.2.2 Compagnia (Company Security Officer)

- *Formazione, addestramento ed attestati degli Ship Security Officers*
- *Incidenti di Security*
- *Cambiamenti del livello di Security*
- *Comunicazioni relative alla security della nave e/o del porto/impianto portuale dove la nave si trova, e o si trovava*
- *Minacce sulla security*
- *Registrazioni degli approdi nave (ultimi dieci approdi)*
- *Rapporti audit esterni/interni*
- *Riesami periodici Valutazione Security e Piano Security e revisioni*
- *Comunicazioni di security con Amministrazioni e Governi Contraenti.*

4.3 Conservazione ed archiviazione

Le registrazioni sulla security sono documenti che devono essere conservati per almeno un anno e passato il periodo devono essere distrutti.

Per l'archiviazione e la protezione vale quanto indicato al Capitolo "Audits e Revisioni Piano security".

4.4 Documentazione

I documenti della Security definiti dalla Compagnia sono:

- *Piano Security Nave*
- *Valutazione Security nave comprendente "visita a bordo" e relativa rapportazione*
- *Rapporto analisi del rischio*
- *Riesami periodici Piano e Valutazione Security*
- *Certificato nave secondo ISPS Code*
- *Continuous Synopsis Record (SOLS Cap. XI-1 Reg.5)*
- *Rapporti Amministrazione*
- *Dichiarazioni Security*
- *Forms*
- *Altri.....*

4.5 Norme internazionali, europee e nazionali

Devono essere inseriti i riferimenti nazionali, europei ed internazionali relativi alla Security (in analogia a quelli gestiti secondo il Manuale ISM) come ad es.:

La nave e la Compagnia devono osservare le seguenti norme nazionali ed internazionali riguardanti la security delle navi e degli impianti portuali:

- (i) *Convenzioni e codici internazionali come emendati e per quanto applicabili*
- 1 *Convenzione Internazionale per la Salvaguardia della Vita Umana in Mare (SOLAS 74), ,*
 - 2 *ISPS Code,*
 - 3 *Altri (vedasi Risoluzioni IMO e Circolari MSC)*

Emesso da	Approvato da	Data	Revisione 0	Pagina 3 di 3
PIANO SECURITY(NAVE) REGISTRAZIONI E DOCUMENTAZIONE				CAP. 4
<i>Riferimento:</i> SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)				

(ii) Regolamento CE sulla Security (quando emanato)

(iii) Norme nazionali

Come applicabile

Emesso da	Approvato da	Data	Revisione 0	Pagina 1 di 7
PIANO SECURITY(NAVE) LIVELLI SECURITY				CAP. 5
<i>Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				

I livelli di security devono tenere conto di quanto indicato nell'ISPS Code Parte A Sez. 7 tenendo conto della guida fornita nella parte B dal sottopar. 9.14 al 9.17 e della guida "Metodologia di base per la trasposizione dell'assessment nel piano security nave".

5.1 Generalità

I livelli di Security sono il principale comune strumento per la gestione della security a bordo e per la struttura portuale che accoglie la nave. La nave deve operare allo stesso livello, definito dal Governo Contraente, della struttura portuale in cui opera se questo è più alto di quello definito dall'Amministrazione di bandiera. La nave può operare ad un livello più alto, ma non inferiore a quello della struttura portuale.

Fermo restando il livello di security stabilito dall'Amministrazione, il Comandante e/o lo Ship Security Officer è/sono responsabili di elevare il livello di Security della nave per fronteggiare situazioni contingenti. La Dichiarazione della Security (DoS-Declaration of Security) tra nave e porto deve essere preparata come applicabile tenendo stretti contatti con il Port Facility Security Officer. Le DoS devono essere firmate da entrambe le parti. L'Autorità competente può richiedere in un qualsiasi momento un innalzamento del Livello di Security (per maggiori dettagli vedere Capitolo ("Dichiarazione di Security)).

Nel caso di operazioni tra nave e nave (es.: tra Supply Vessel e Mobile Offshore Unit) lo Ship Security Officer prenderà contatti con la nave per poter avere informazioni circa la security applicata da quest'ultima. Egli valuterà l'opportunità di utilizzare una DoS e, in questo caso, la invierà per le opportune azioni allo Ship Security Officer della nave con cui si interfaccia.

Nel caso di un innalzamento di Livello di Security durante il periodo di validità della DoS, deve essere preparata una nuova DoS e concordata come sopra indicato.

La nave dovrà sempre comunicare all'Amministrazione l'avvenuta ricezione di ogni cambiamento di livello 2 e 3 richiesto, unitamente alla conferma del cambiamento di livello effettuato.

I livelli di Security definiscono i compiti al fine di:

- *Assicurare l'effettuazione di tutti i compiti previsti per la Security*
- *Monitorare l'accesso alla nave*
- *Monitorare le aree del ponte ed intorno alla nave*

Emesso da	Approvato da	Data	Revisione 0	Pagina 2 di 7
PIANO SECURITY(NAVE) LIVELLI SECURITY				CAP. 5
<i>Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				

- *Monitorare l'imbarco delle persone e dell'eventuale bagaglio/attrezzature ecc. che viaggiano con loro*
- *Supervisionare l'imbarco del carico, qualunque esso sia, e delle provviste di bordo*
- *Assicurare la pronta comunicazione con le autorità competenti della security dell'impianto portuale come applicabile.*

Come la minaccia per la Security cambia, anche il livello deve essere cambiato. Sono stati definiti Tre Livelli di Security come segue:

- *Livello di security 1, livello normale: livello di security corrispondente al funzionamento normale di navi e impianti portuali.*
- *Livello di security 2, livello elevato: livello di security applicabile fintantoché persiste un rischio maggiore di incidente per la security.*
- *Livello di security 3, livello eccezionale: livello di security applicabile per il lasso di tempo durante il quale il rischio di incidente per la security è probabile o imminente.*

5.2 Livelli di Security

Di seguito vengono indicati i requisiti minimi richiesti dalla guida "Metodologia di base per la trasposizione dell'assessment nel piano security nave":

Efficacia delle attività di security a bordo

	<i>Livello di Sicurezza</i>		
	<i>1</i>	<i>2</i>	<i>3</i>
Misura protettiva			
<i>Tutti i membri dell'equipaggio normalmente ricontrollano e rivedono i propri compiti di security mediante esercitazioni ed addestramenti</i>	<i>SI*</i>	<i>SI*</i>	<i>SI*</i>
<i>Fornire a tutti i membri dell'equipaggio e al personale di security le informazioni che comprendono il livello di sicurezza ed altre informazioni specifiche sulle minacce</i>	<i>Opzionale</i>	<i>SI</i>	<i>SI</i>
<i>L'ufficiale responsabile della security della nave (SSO) dovrebbe normalmente comunicare con le installazioni di terra per coordinare le misure protettive</i>	<i>SI</i>	<i>SI[#]</i>	<i>SI[#]</i>
<i>* Esercitazioni e prove dovrebbero essere condotti mensilmente</i>			
<i># Coordinare ulteriori misure protettive</i>			

Emesso da	Approvato da	Data	Revisione 0	Pagina 3 di 7
PIANO SECURITY(NAVE) LIVELLI SECURITY				CAP. 5
<i>Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				

La Compagnia può considerare necessarie anche le seguenti azioni:

- Fornire ordini scritti al personale designato alla Security su tutti gli aspetti a carattere non contingente, che non sono inclusi nel seguente piano
- Sistemare avvisi sulla Security applicata sulla nave (es.: Avvisi Divieto Entrata Aree ad Accesso Limitato o Informazioni alle persone autorizzate ad entrare a bordo su eventuali limitazioni di accesso a determinate aree ecc.)

Controllo delle Aree ad Accesso Limitato (Restricted Areas) per garantire l'ingresso solo alle persone autorizzate:

Misura protettiva	Livello di Sicurezza		
	1	2	3
Chiudere o serrare l'entrata alle aree ad accesso limitato @	Opzionale	SI	SI
Impiego di personale per guardie e perlustrazioni	Opzionale	SI*	SI#
L'aumento della frequenza e della cura dei dettagli nel monitoraggio delle aree ad accesso limitato può includere: * Dedicare personale al controllo e alla perlustrazione delle aree ad accesso limitato # Disporre personale per il controllo continuo delle aree ad accesso limitato e/o assegnarlo alla perlustrazione continua delle stesse aree e delle zone vicine @ E' richiesto che le porte lungo i percorsi di sfuggita debbano poter essere aperte, senza chiavi, nel verso del percorso individuato per la fuga			

Emesso da	Approvato da	Data	Revisione 0	Pagina 4 di 7
PIANO SECURITY(NAVE) LIVELLI SECURITY				CAP. 5
<i>Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				

Controllo degli accessi della nave

Misura protettiva	Livello di Sicurezza		
	1	2	3
I punti d'accesso sono normalmente serrati [@] o continuamente controllati per prevenire l'ingresso non autorizzato	SI	SI [#]	SI [#]
Le maniche a vento sui ponti esposti, i locali deposito e le entrate in aree generalmente non presidiate (come magazzini, locali macchine ausiliarie, ecc.) devono essere serrate [@] o devono essere adottate precauzioni per prevenire l'accesso non autorizzato	SI	SI	SI
Limitare l'entrata alla nave ad un numero minimo di punti d'accesso ⁺	Opzionale	SI	SI [*]
Coordinarsi con le port facilities per estendere il controllo degli accessi anche oltre l'area in prossimità della nave	Opzionale	SI	SI
<p>* Limitare l'entrata ad un unico punto d'accesso</p> <p>[@] Le porte lungo i percorsi di sfuggita devono poter essere aperte senza l'ausilio di chiavi nel verso del percorso individuato per la fuga</p> <p>⁺ Ma non ridurre i punti d'uscita dalla nave in caso d'emergenza</p> <p>[#] Assegnare personale aggiuntivo agli appropriati punti d'accesso, come stabilito nello SSP</p>			

- La Compagnia può considerare necessarie anche le seguenti azioni:*
- *Incrementare la percentuale di controllo (in funzione del Livello di Security) dell'eventuale bagaglio non accompagnato tramite esame visivo esterno/interno identificandolo opportunamente*
 - *Eseguire controlli a spot da parte del Ship Security Officer o dell'Ufficiale di Guardia per verificare l'applicazione della security ai punti di accesso nave*
 - *Prevedere eventuale coordinamento con l'impianto portuale per la definizione delle aree di controllo accesso esterne alla nave, ove applicabile*

Emesso da	Approvato da	Data	Revisione 0	Pagina 5 di 7
PIANO SECURITY(NAVE) LIVELLI SECURITY				CAP. 5
<i>Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				

Monitoraggio dei ponti e delle aree circostanti la nave

Misura protettiva	Livello di Sicurezza		
	1	2	3
Impiegare vedette e/o ronde per la security	Opzionale	SI	SI*
Effettuare ispezioni a mezzo imbarcazioni per il controllo del lato mare	Opzionale	Opzionale	SI*
Usare sommozzatori per ispezionare la parte immersa della banchina prima dell'arrivo e durante la sosta della nave nonchè quando ritenuto necessario	Opzionale	Opzionale	SI
* Aumentare il numero e la frequenza di: <ol style="list-style-type: none"> 1. ronde di security per garantire un monitoraggio continuo; 2. ronde con imbarcazioni per assicurare il controllo continuo 			

La Compagnia può considerare necessarie anche le seguenti azioni:

- *illuminare i ponti e le zone lato terra/mare attorno alla nave durante la notte*

Emesso da	Approvato da	Data	Revisione 0	Pagina 6 di 7
PIANO SECURITY(NAVE) LIVELLI SECURITY				CAP. 5
<i>Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				

Controllo dell'imbarco delle persone e dei loro effetti

Misura protettiva	Livello di Sicurezza		
	1	2	3
Verificare i motivi dell'imbarco sulla nave attraverso biglietti, pass, ordinativi di lavoro o altro	SI	SI	SI
Identificare chiaramente i membri dell'equipaggio, i passeggeri, i fornitori, i visitatori e altro personale prima di ogni imbarco	SI	SI	SI
Controllare che l'equipaggio imbarcante sia autorizzato per l'impiego a bordo	SI	SI	SI
Ispezionare persone, bagagli, articoli trasportati ed apparecchiature personali per la ricerca di armi, sostanze incendiarie e/o esplosive	SI [#]	SI [@]	tutti
Prima della partenza, fornire informazioni di security a tutti i passeggeri su specifiche minacce e sulla necessità di vigilare e riportare al personale addetto eventuali notizie su persone, oggetti o attività sospette.	Opzionale	SI	SI*
Assegnare personale di guardia nelle aree di ispezione in aggiunta a quello già designato a svolgere i controlli	Opzionale	SI	SI
Limitare l'accesso solo ai passeggeri, all'equipaggio ed ai pubblici ufficiali nell'esercizio dei propri compiti	Opzionale	Opzionale	SI
Scortare i fornitori e le altre persone di servizio richieste dal bordo per fornire servizi essenziali alla nave	Opzionale	Opzionale	SI
<p>* Le informazioni sulla security sono generalmente fornite a tutti i passeggeri prima dell'imbarco e sbarco</p> <p># Quest'operazione può essere effettuata con ispezioni a campione, pari al 5-25% o utilizzando altri metodi stabiliti nel Security Plan della nave</p> <p>@ Aumentare la frequenza, pari al 25-50%, e dettagliare le ispezioni</p>			

La Compagnia può considerare necessarie anche le seguenti azioni:

- stabilire le procedure (chi, cosa e quando) affinché al bordo venga fornito l'elenco delle persone autorizzate ad avere l'accesso alla nave (es. personale agenzie, tecnici acc.)

Emesso da	Approvato da	Data	Revisione 0	Pagina 7 di 7
PIANO SECURITY(NAVE) LIVELLI SECURITY				CAP. 5
Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)				

Supervisione al maneggio del carico ed ai depositi nave

Misura protettiva	Livello di Security		
	1	2	3
Verificare il carico non containerizzato con la polizza di carico	SI [#]	Tutti	Tutti
Verificare i numeri d'identificazione dei container imbarcati con la polizza di carico	Tutti	Tutti	Tutti
Verificare i numeri d'identificazione dei container vuoti con la polizza di carico	SI [#]	Tutti	tutti
Ispezionare le forniture e le provviste della nave	SI [#]	SI ⁺	tutti
[#] Quest'operazione può essere effettuata con verifica a campione, pari al 5-25% del carico			
⁺ Aumentare la frequenza e il dettaglio delle ispezioni, pari al 25-50%			

La Compagnia può considerare necessarie anche le seguenti azioni:

- adottare eventuali azioni di security particolari nei casi di trasporto di merci pericolose (es.: esplosivi, armi ecc.)

Assicurare che le comunicazioni di security con il porto siano prontamente disponibili

Misura protettiva	Livello di Sicurezza		
	1	2	3
Effettuare regolari controlli alle comunicazioni	Opzionale	SI	SI
Fornire mezzi di comunicazione di riserva	Opzionale	SI	SI [#]
[#] Fornire mezzi di comunicazione ridondanti e multipli			

5.3 Attività non contemplate dall' ISPS Code

Dovrebbe essere indicato quali misure la nave adotta, nel caso di attività non contemplate dal ISPS Code, tenendo conto della guida fornita nella Parte B para. 9.51:
Il piano di sicurezza della nave deve precisare le procedure e le misure di sicurezza che la nave deve applicare quando:

- si trova nel porto di uno Stato che non è un Governo Contraente;

Da tenere presente che al riguardo potrebbero essere imposte condizioni particolari dall'Amministrazione di bandiera.

Emesso da	Approvato da	Data	Revisione 0	Pagina 1 di 2
PIANO SECURITY(NAVE)				CAP.
INTERFACCE CON AUTORITA', PORTI, IMPIANTI PORTUALI ED ALTRE NAVI				6
Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)				

I collegamenti e relative modalità di comunicazione tra il Company Security Officer, il Comandante, lo Ship Security Officer, l'impianto portuale, un'altra nave ed ogni autorità coinvolta nella gestione della Security deve essere conforme a quanto richiesto dal ISPS Code Parte A Sez. 7.6 al 7.9 e tenendo conto della guida fornita nella Parte B come ad es.:

6.1 Generalità

La Compagnia riconosce che una efficace interfaccia a tutti i livelli è di primaria importanza per una sicura ed efficiente gestione delle navi e deve essere effettuata con opportuni mezzi di comunicazione.

Ciò include sia le interfacce tra la compagnia e le navi gestite, con i Governi Contraenti (incluso l'Amministrazione di bandiera), le Autorità competenti della security portuale, gli impianti portuali e le altre navi.

Ulteriori istruzioni concernenti le comunicazioni (formato dei messaggi, ecc) vengono date nel (es.: Manuale della Compagnia, lettera circolare, ecc).

Il Company Security Officer provvede a fornire e mantenere aggiornato un elenco contenente i dati relativi ai contatti con le Autorità competenti degli Stati Costieri con i quali la nave può interfacciarsi. Questo elenco è allegato a(da completare)

Egli inoltre provvede a fornire alla nave e mantenere aggiornati i dettagli (vedere anche Capitolo "Dettagli Nave") relativi a:

- *parti incaricate di designare il personale di bordo, quali la compagnia di gestione marittima, le agenzie di assunzione, i contraenti, i concessionari (ad esempio, negozi, casinò, ecc.);*
- *parti incaricate di decidere l'uso della nave, compresi i noleggiatori a tempo o scafo nudo o altre parti che agiscono in tale qualità; e*
- *nei casi di contratto di noleggio della nave, gli estremi dei punti di contatto delle parti, compresi i noleggiatori a tempo o a scafo nudo.*

6.2 Governi Contraenti ed Amministrazione di Bandiera

Il Company Security Officer fornisce alla nave un elenco con tutti i punti di contatto dei Governi Contraenti e dell'Amministrazione di Bandiera. Egli provvede inoltre, unitamente allo Ship Security Officer a comunicare tutte le informazioni richieste per le misure di security da applicare o applicate. Quando un governo contraente fissa i livelli di sicurezza e provvede a comunicare le informazioni alla nave che opera nelle sue acque territoriali o ha comunicato l'intenzione di entrarvi, la nave comunica immediatamente alla propria amministrazione e a tutti gli Stati costieri nelle vicinanze qualsiasi informazione di cui venga a conoscenza e che possa avere un impatto sulla sicurezza marittima dell'area.

Emesso da	Approvato da	Data	Revisione 0	Pagina 2 di 2
PIANO SECURITY(NAVE)				CAP.
INTERFACCE CON AUTORITA', PORTI, IMPIANTI PORTUALI ED ALTRE NAVI				6
Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)				

6.3 Porti

Prima dell'arrivo della nave in un porto, lo Ship Security Officer provvede a compilare il form.....

Il form deve contenere le informazioni richieste SOLAS Cap. XI-2 Regola 9 paragrafo 2 , tenendo conto della guida fornita dal ISPS Code Parte B para 4.37 e successivi 4.38 e 4.39.

6.4 Impianti Portuali

E' responsabilità dello Ship Security Officer mettersi in contatto non appena possibile con il Port Facility Security Officer dell'impianto portuale in cui la nave intende recarsi per determinare il livello di security applicabile alla nave in questione in tale impianto portuale. Una volta in relazione con la nave, il Port Facility Security Officer dell'impianto portuale deve comunicare ogni eventuale cambiamento del livello di security dell'impianto portuale e fornire alla nave tutte le informazioni pertinenti riguardanti la security. La Dichiarazione di Security di cui all'Appendice 1 dell'ISPS Code (ParteB) può essere utilizzata al riguardo. E' responsabilità dello Ship Security Officer riportare ogni situazione negativa riscontrata nella gestione della security da parte dell'impianto portuale al Company Security Officer, che eventualmente farà segnalazione all'autorità competente per la security del porto e dell'Amministrazione.

6.5 Operazioni con altre navi

Nel caso di operazioni con altre navi, è responsabilità dello Ship Security Officer chiedere informazioni circa il livello di security applicato. Nel caso di un livello più alto, la nave si deve adeguare a tale livello, comunicando l'avvenuto adeguamento. Se si ritiene applicabile, può essere preparata una Dichiarazione di Security (Vedi relativo capitolo).

6.6 Attività non contemplate dal ISPS Code

Devono essere indicate quali misure la nave adotterà, nel caso di attività non contemplate dal ISPS Code, tenendo conto della guida fornita nella Parte B para. 9.51:

- effettua attività di interfaccia con piattaforme fisse o galleggianti o con una piattaforma mobile di perforazione in stazionamento; o
- effettua attività di interfaccia con una nave o un impianto portuale non assoggettato alle disposizioni del capitolo XI-2 e dall'ISPS Code.

6.7 Comunicazioni in situazioni di emergenza

Il Comandante e lo Ship Security Officer si assicurano che tutti i dettagli relativi ai contatti che possono essere utilizzati in caso di minaccia o emergenza per la security della nave siano disponibili. Le minacce possono essere ad esempio quelle relative ad attacchi di pirateria, attacchi criminali (es. furti a mano armata) ed attacchi di tipo terroristico.

La procedura da seguire per le comunicazioni tiene conto anche di quella prevista dal Manuale ISM.

Emesso da	Approvato da	Data	Revisione 0	Pagina 1 di 2
PIANO SECURITY(NAVE) DICHIARAZIONE DI SECURITY				CAP. 7
<i>Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				

La Dichiarazione di Security (Declaration of Security (DoS) deve essere gestita in conformità a quanto previsto dall'ISPS Code Parte A Sez. 5, tenendo conto della guida fornita nella Parte B medesimo paragrafo.

7.1 Generalità

La Dichiarazione di Security contiene i requisiti di security che possono essere ripartiti tra gli impianti portuali e la nave (o tra navi), con espressa dichiarazione delle responsabilità di ciascuno. La Dichiarazione di Security, quando richiesta, è un pre-requisito per l'entrata in porto o l'inizio delle operazioni nave/nave.

Le dichiarazioni devono essere archiviate a cura del Comandante e rese non accessibili al personale non autorizzato.

Il modulo da utilizzare è allegato a(può essere quello allegato come Appendice alla Parte B dell'ISPS Code).

7.2 Governi Contraenti

I Governi Contraenti decidono quando sia necessaria una dichiarazione di security, valutando il rischio che l'interfaccia nave/porto o l'attività nave/nave rappresenta per persone, beni o per l'ambiente. Alla ricezione di una richiesta in tal senso lo Ship Security Officer di concerto con il Comandante compila come richiesto la parte di competenza nave ed avvia tutte le azioni richieste dal relativo Livello di Security o altre azioni previste informando dell'avvenuta effettuazione di quanto richiesto. Lo Ship Security Officer informa il Company Security Officer, che a seguito delle informazioni ricevute provvederà a rendere disponibili le eventuali risorse aggiuntive che si dovessero rivelare necessarie ed informerà l'Amm.ne di bandiera come applicabile.

7.3 Nave

La nave può richiedere il rilascio di una dichiarazione di security quando:

- *la nave opera a un livello di security più elevato dell'impianto portuale o di un'altra nave con cui è in interfaccia;*
- *esiste un accordo sulla dichiarazione di security tra governi contraenti riguardo a determinati viaggi internazionali o a navi specifiche che effettuano tali viaggi;*
- *si è verificata una minaccia o un problema di security riguardante la nave o gli impianti portuali, ove applicabile;*
- *la nave è in un porto o presso un impianto portuale per i quali non è previsto esservi un piano approvato di security;*
- *la nave sta conducendo attività nave/nave per la quale non è necessario avere od attuare un piano approvato di security della nave.*

L'impianto portuale e la nave interessata devono rendere nota l'avvenuta ricezione delle richieste di dichiarazione di security fatte ai sensi della presente sezione.

La dichiarazione di security deve essere redatta:

- .1 *dal comandante della nave o dallo Ship Security Officer per conto della nave o delle navi;*

Emesso da	Approvato da	Data	Revisione 0	Pagina 2 di 2
PIANO SECURITY(NAVE) DICHIARAZIONE DI SECURITY <i>Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				CAP. 7

- .2 *dal Port Facility Security Officer o, se il governo contraente stabilisce diversamente, da qualunque altro ente responsabile della security a terra, per conto dell'impianto portuale.*

Emesso da	Approvato da	Data	Revisione 0	Pagina 1 di 2
PIANO SECURITY(NAVE) SISTEMI DI COMUNICAZIONE				CAP. 8
<i>Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				

Devono essere indicati i mezzi utilizzati per i collegamenti e relative modalità di comunicazione tra il Company Security Officer, il Comandante, lo Ship Security Officer, l'impianto portuale e ogni autorità coinvolta nella gestione della Security come richiesto nel ISPS Code Parte A Sez. 7.2.7, tenendo conto della guida fornita nella Parte B para. 9.7.2.

8.1 Generalità

La Compagnia riconosce che una efficace comunicazione a tutti i livelli è di primaria importanza per una sicura ed efficiente gestione delle navi.

Ciò include sia le comunicazioni tra la terra e le navi e viceversa che quelle sulla nave.

I mezzi di comunicazione disponibili a bordo sono:

Da completare con l'elencazione e tenendo presente l'Automatic Identification System (AIS) SOLAS Cap. V Reg. 19 e lo Ship Security Alert System SOLAS Cap.XI-2 Reg.6.

8.2 Responsabilità delle comunicazioni

ITU - Regolamento delle Radiocomunicazioni 1994 - Capitolo XI - Articolo 54:

§ 1 *Il servizio di una stazione di nave è posto sotto la suprema autorità del Comandante, o della persona responsabile della nave, o altro tipo di natante, sulla quale la stazione è installata.*

§ 2 *La persona che detiene tale autorità deve accertarsi che ogni operatore si attenga al presente Regolamento, e che la stazione di nave della quale l'operatore è responsabile, venga sempre utilizzata in accordo con il presente Regolamento.*

Tutte le comunicazioni in arrivo o in partenza da bordo, effettuate dagli ufficiali che svolgono il servizio GMDSS, avvengono sempre e comunque sotto l'autorità e la responsabilità del Comandante, che deve autorizzare tutti i messaggi in partenza.

Gli Ufficiali che svolgono il servizio GMDSS hanno il dovere di sottomettere al Comandante tutto il traffico in arrivo ed in partenza, sia esso commerciale o di carattere privato.

8.3 Segretezza delle comunicazioni

ITU - Regolamento delle Radiocomunicazioni 1994 - Capitolo XI - Articolo 54:

§ 3 *Il Comandante, o la persona responsabile, come pure tutte le persone che siano a conoscenza del testo, o anche soltanto dell'esistenza, di un messaggio radio, o di ogni altra informazione comunque ottenuta per mezzo del servizio di radiocomunicazione, hanno l'obbligo di osservare e di assicurare la segretezza della corrispondenza.*

L'ubicazione degli apparati GMDSS sul ponte di comando, fa sì che non possa sempre essere assicurata la necessaria riservatezza delle comunicazioni in arrivo o in partenza, siano esse commerciali o di carattere privato.

L'Ufficiale responsabile del GMDSS e, in sua assenza, l'Ufficiale di Coperta di guardia, hanno l'obbligo di sorvegliare che nessun estraneo al servizio, di qualsiasi grado, possa prendere visione o venire a conoscenza di messaggi o informazioni ricevute o inviate per mezzo degli apparati esistenti sul ponte di comando. Essi hanno l'obbligo di mantenere il segreto su tutte le comunicazioni delle quali vengono necessariamente a conoscenza.

Emesso da	Approvato da	Data	Revisione 0	Pagina 2 di 2
PIANO SECURITY(NAVE) SISTEMI DI COMUNICAZIONE				CAP. 8
<i>Riferimento:</i> SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)				

8.4 Radiocomunicazioni interne a bordo

Devono essere redatte le procedure (individuazione apparecchiature e relativo elenco, frequenze/canali, codici ecc.) che consentano la comunicazione, anche a carattere continuativo, tra il personale avente compiti di security.

Emesso da	Approvato da	Data	Revisione 0	Pagina 1 di 1
PIANO SECURITY(NAVE)				CAP.
DOTAZIONI ED EQUIPAGGIAMENTI PER LA SECURITY				9
Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)				

Le dotazioni ed equipaggiamenti per l'attività di security devono essere gestite in accordo a quanto indicato dall'ISPS Code Parte A Sez. 9.4.15 a 9.4.18 tenendo conto della guida fornita nella Parte B para 9.7.3. Eventualmente le dotazioni dovranno essere indicate nei piani nave (vedi Capitolo "Dettagli Nave"). Esempio:

9.1 Generalità

Tutte le dotazioni ed equipaggiamenti forniti alla nave devono essere gestiti dallo Ship Security Officer il quale provvederà ad effettuare tutte le operazioni di prova, ispezione, calibratura e manutenzione con la frequenza indicata nell'istruzione (scheda) che accompagna ogni dotazione/equipaggiamento e che è comprensiva delle istruzioni sull'uso. Egli manterrà un inventario di quanto indicato nei seguenti paragrafi e provvederà al loro immagazzinamento (per le dotazioni non fisse), quando non in uso.

Nel caso vi siano malfunzionamenti, manomissioni e smarrimenti (come applicabile) nelle dotazioni/equipaggiamenti sotto indicate il Ship Security Officer provvederà ad informare il Company Security Officer per le appropriate azioni. In caso detta dotazione pregiudichi una qualsiasi attività relativa alla security, il Ship Security Officer di concerto con il Comandante ed eventualmente il Company Security Officer ed il Port Facility Security Officer, stabilirà soluzioni alternative che non pregiudichino le sopradette attività, informando il personale addetto alla security come applicabile e registrando quanto sopra (vedi Capitolo Registrazioni)

9.2 Dotazioni ed equipaggiamenti

Le dotazioni nave ed equipaggiamenti sono i seguenti:

- Ship Security Alert System (vedi Capitolo "Dettagli Nave" e "Sistemi di Comunicazione")
- Impianto CCTV
- Metal detector fisso e portatile
- X-Ray bagaglio
- Explosive detector
- Card passeggeri ed equipaggio
- Allarmi
- Cercapersone, sensori
- Illuminazione Security (vedi Capitolo "Dettagli nave")
- Chiavi per Security (es.: chiave per chiusura aree ad accesso limitato, ecc.)
- Piombi/adesivi rilevazione apertura di porte accesso aree di cui sopra
- Altri.....

La combinazione delle dotazioni ed equipaggiamenti di security necessari deve scaturire dalle valutazioni fatte nello Ship Security Assessment

Emesso da	Approvato da	Data	Revisione 0	Pagina 1 di 4
PIANO SECURITY(NAVE) CONTROLLO ACCESSI				CAP. 10
Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)				

Gli accessi alla nave per l'attività di security devono essere identificati e gestiti in accordo a quanto indicato dall' ISPS Code Parte A Sez. 9.4.3 tenendo conto della guida fornita nella Parte B dal para 9.8 al 9.17 e devono essere indicati nei piani nave (vedi Capitolo "Dettagli nave"). Fare inoltre riferimento alla guida "Metodologia di base per la trasposizione dell'assessment nel piano di security per la nave". Esempio:

10.1 Generalità

Tutti gli accessi alla nave devono essere protetti e controllati al fine di garantire la security.

Di seguito vengono elencati tutti i punti di accesso alla nave e relativi controlli da effettuare (indicati nei piani di cui al Capitolo 1).

I punti di accesso, quando non utilizzati come deciso dal Comandante e dallo Ship Security Officer, devono essere chiusi e non più utilizzati se non previa loro formale autorizzazione.

10.2 Punti di accesso

I punti di accesso alla nave sono i seguenti:

- Scalandroni lato.....
- Passerelle lato..... (da considerare anche quelle per operazioni nave/nave)
- Biscagline
- Portelloni laterali per imbarco provviste e bunkeraggio nr..
- Rampe
- Cavi ormeggio e catene ancore
- Gru e picchi
- Oblò/finestroni
- Pick-up area (operazioni con elicottero)
- Nastri trasportatori e/o manichette del carico
- Pontili
- Altri.....

Per tutti i punti di cui sopra, dovranno essere indicate le procedure per il controllo e/o sorveglianza, la limitazione dell'accesso ed i divieti di accesso per ogni livello di sicurezza.

10.3 Controllo accessi

L'estensione dei controlli ed azioni da effettuare sono in funzione del Livello di Security da adottare (vedi Cap."Livelli Security") e comprendono:

- *Il comandante con lo Ship Security Officer devono stabilire i punti di accesso nave da utilizzare*
- *Lo Ship Security Officer deve stabilire il personale addetto al controllo dei punti di accesso*
- *Lo Ship Security Officer deve stabilire con l'impianto portuale le aree stabilite per il controllo di persone, carico e provviste prima dell'ingresso alla nave*
- *I punti di accesso alla nave diversi da quelli stabiliti per l'utilizzo devono essere assicurati chiusi o non accessibili*
- *L'identità di qualsiasi persona deve essere verificata prima di permettergli l'accesso a bordo*
- *Il carico e le provviste di bordo devono essere controllate prima dell'imbarco*
- *Devono essere stabilite ronde per il controllo degli accessi non utilizzati*

Emesso da	Approvato da	Data	Revisione 0	Pagina 2 di 4
PIANO SECURITY(NAVE) CONTROLLO ACCESSI				CAP. 10
<i>Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				

- *Limitare l'accesso alle Aree ad accesso Limitato solo a personale autorizzato*
- *Verificare che le persone già a bordo, non appartenenti all'equipaggio, siano state debitamente autorizzate*

10.4 Controllo persone all'imbarco incluso bagagli e bagaglio non accompagnato

L'estensione dei controlli ed azioni da effettuare sono in funzione del Livello di Security da adottare (vedi Cap. "Livelli Security") e comprendono:

10.4.1 Passeggeri e relativi bagagli

I controlli previsti sono i seguenti:

- *Controllo biglietto imbarco e relativo documento personale e rispondenza Elenco passeggeri imbarcanti*
- *Utilizzo Metal Detector fisso o portatile per persona*
- *Utilizzo X-Ray screening bagagli e relativa identificazione degli stessi*
- *Fornire al passeggero la card magnetica di identificazione (se prevista) o altra card di riconoscimento*
- *Fornire eventuale brochure sulla Politica della Security della nave*
- *Informare prontamente il Ship Security Officer nel caso di rifiuto del passeggero ai controlli di cui sopra e non permetterne l'entrata.*

10.4.1.1 Bagagli non accompagnati

- *Fornire dati sul proprietario del bagaglio, motivi dell'imbarco e modalità di identificazione e sistemazione bagaglio non accompagnato sulla nave*
- *Utilizzo X-Ray screening bagagli e relativa identificazione degli stessi*
- *Esame visivo interno (se previsto come scelta alternativa all' X-Ray screening)*
- *Prepararsi alla limitazione o alla sospensione della movimentazione dei bagagli non accompagnati*

10.4.2 Personale di Agenzie, tecnici

- *Verificare identità e motivi, controllare la corrispondenza con elenco entrata persone nave previsto*
- *Ispezionare il relativo bagaglio personale (possono utilizzarsi le dotazioni per il controllo dei passeggeri))*
- *Assegnare card identificazione*
- *Fornire informazioni sulla security di bordo (es.: identificazione e relativo divieto per aree ad accesso limitato)*
- *Registrare entrata/uscita*
- *Accompagnare la persona o vietarne l'ingresso in funzione del livello di Security*

10.4.3 Autorità

- *Verificare identità e motivi*
- *Fornire informazioni sulla security di bordo (es.: identificazione e relativo divieto ad aree ad accesso limitato)*
- *Registrare entrata/uscita*
- *Accompagnare la persona*

Emesso da	Approvato da	Data	Revisione 0	Pagina 3 di 4
PIANO SECURITY(NAVE) CONTROLLO ACCESSI				CAP. 10
Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)				

- *Garantire l'accesso rapido alle autorità preposte che devono rispondere alle minacce o all'incidente di security*

10.4.4 Personale addetto al carico

- *Chiarire con l'impianto portuale il sistema di identificazione del personale*
- *Informare il personale di bordo addetto ai controlli di security sul sistema di individuazione*
- *Informare il personale di terra sulle limitazioni previste per le Aree ad Accesso Limitato*
- *Controllare il personale come previsto dai Livelli di Security*

Nel caso una persona intenzionata a salire a bordo rifiuti di farsi identificare, gli deve essere negato l'accesso a bordo e si dovrà informare lo Ship Security Officer il quale provvederà a darne comunicazione immediata all'Autorità competente per la security dell'impianto portuale.

10.5 Controllo Scalandroni

L'estensione dei controlli ed azioni da effettuare sono in funzione del Livello di Security da adottare (vedi Cap."Livelli Security") e comprendono:

- *Assegnare personale di guardia*
- *Chiudere l'accesso e monitorare quelli non in uso (controllo visivo del personale di guardia o impianto CCTV)*
- *Controllare durante le ronde quelli non utilizzati*

10.6 Controllo Biscagline

L'estensione dei controlli ed azioni da effettuare sono in funzione del Livello di Security da adottare (vedi Cap."Livelli Security") e comprendono:

- *Assicurarsi che le biscagline non siano disponibili all'utilizzo quando non in uso*
- *Assegnare personale quando la biscaglina viene utilizzata, dotandolo di apposito apparecchio di radio comunicazione con il Ponte di Comando (es. Pilota)*
- *Attivare eventuale illuminazione prevista per la Security*
- *Controllare sistemazione biscagline durante le ronde stabilite*

10.7 Controllo Portelloni laterali

L'estensione dei controlli ed azioni da effettuare sono in funzione del Livello di Security da adottare (vedi Cap."Livelli Security") e comprendono:

- *Assegnare personale di guardia quando in uso dotandolo di apposito apparecchio di radio comunicazione con il Ponte di Comando (es. Pilota)*
- *Verificare che personale esterno non possa accedere previa effettuazione di quanto previsto per l'imbarco persone*
- *Verificare le operazioni da effettuare come indicato dallo Ship Security Officer (es.: imbarco acqua, combustibili, viveri)*

10.8 Controllo Rampe

Emesso da	Approvato da	Data	Revisione 0	Pagina 4 di 4
PIANO SECURITY(NAVE) CONTROLLO ACCESSI				CAP. 10
<i>Riferimento:</i> SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)				

L'estensione dei controlli ed azioni da effettuare sono in funzione del Livello di Security da adottare (vedi Cap. "Livelli Security") e comprendono:

- *Assegnare personale di guardia quando in uso*
- *Chiudere o rendere inaccessibili quando non in uso*
- *Monitorare visivamente*
- *Attivare Impianto CCTV (se previsto)*
- *Controllare durante le ronde*

Segue come applicabile secondo quanto indicato al paragrafo 10.2

Emesso da	Approvato da	Data	Revisione 0	Pagina 1 di 3
PIANO SECURITY(NAVE)				CAP.
AREE AD ACCESSO LIMITATO E MONITORAGGIO				11
Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)				

Le aree ad accesso limitato sono quelle definite dall'ISPS Code Parte A Sez. 9.4.2 tenendo conto della guida fornita nella Parte B para. 9.18-9.21 e devono essere indicate nei piani nave (vedi Capitolo "Dettagli nave"). Fare inoltre riferimento alla guida "Metodologia di base per la trasposizione dell'assessment nel piano di security per la nave".

11.1 Generalità

Le Aree ad Accesso Limitato ed i Punti Vulnerabili come definiti nei seguenti paragrafi sono stabiliti per controllare le zone ritenute "chiave" per le operazioni, controllo e sicurezza della nave. Dette aree e punti devono essere accessibili solo al personale di bordo o alle persone debitamente autorizzate. A seguito della valutazione della Security della nave sono stati inoltre identificati dei punti vulnerabili che vengono indicati nei successivi paragrafi.

I punti di ingresso alle aree ad accesso limitato e i punti vulnerabili devono essere chiusi e serrati a meno che il Comandante decida che per ragioni operative questi non possono essere chiusi.

Le aree ad accesso limitato ed i punti vulnerabili vengono controllati durante le ronde eventualmente istituite in relazione ai Livelli di Security.

Le aree ad accesso limitato sono tutte identificate opportunamente con il seguente cartello:

AREA AD ACCESSO LIMITATO – VIETATO L'INGRESSO

CONSENTITO L'INGRESSO AL SOLO PERSONALE AUTORIZZATO

L'ENTRATA AUTORIZZATA IN QUESTA AREA AD ACCESSO LIMITATO PUO' AVVENIRE SOLO PREVIA ISPEZIONE

11.2 Aree ad Accesso Limitato (Restricted Areas)

Le aree ad accesso limitato sono le seguenti (vedi anche Capitolo "Valutazione Security Nave"):

- Ponte di Comando
- Stazione Radio (se non nel Ponte di Comando)
- Sala Macchine
- Sala controllo Macchine (se non inclusa nel locale macchine)
- Le vie di sfuggita dalla Sala Macchine
- Locale timoneria
- Locali elica prodiera
- Locale Impianti Antincendio e VF
- Locale Diesel Emergenza
- Locali garage (quando in navigazione)
- Pick-up area per operazioni con elicottero (per come tecnicamente fattibile)
- Locali controllo carico
- Locali pompe del carico
- Locali per l'imbarco ed accesso ai serbatoi acqua potabile, fuel, olio, pompe e collettori
- Locali equipaggio
-

Emesso da	Approvato da	Data	Revisione 0	Pagina 2 di 3
PIANO SECURITY(NAVE)				CAP.
AREE AD ACCESSO LIMITATO E MONITORAGGIO				11
Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)				

Altre aree ad accesso limitato possono essere definite con l'autorità competente della security nel porto o nell'impianto portuale nel caso di un aumento del livello di security. In tal caso dette aree devono essere gestite dal Ship Security Officer in accordo alle decisioni concordate ed informando opportunamente il personale di bordo addetto ai compiti di security. Il Company Security Officer deve essere debitamente informato al fine della valutazione della necessità di eventuali risorse aggiuntive.

11.3 Punti vulnerabili

Sono stati definiti i seguenti Punti Vulnerabili (vedi considerazioni Capitolo "Valutazione Security nave"):

- Locali ventilazione
- Locali batterie
- Locali per stivaggio sostanze pericolose (es.pitture)
- Stazioni Elettriche
- Locali macchinari ascensori
- Locali bombole ossiacetileniche
- Zona estrema prodiera e poppiera
-

11.4 Sistemi di chiusura accessi

In base al livello di Security applicato, per la chiusura degli accessi vengono utilizzate serrature e relative chiavi oppure lucchetti, mentre per le vie di sfuggita viene assicurato che queste possano essere aperte dal lato della fuga.

L'utilizzo delle chiavi e dei lucchetti viene gestito a discrezione del Comandante e dello Ship Security Officer che provvede a fornirle al personale di bordo in accordo ai relativi compiti come applicabile e mantiene un elenco di distribuzione.

Ad ogni membro dell'equipaggio viene fornita una chiave del proprio alloggio.

Nel caso di perdita o di sottrazione delle chiavi di cui sopra, ne deve essere informato subito lo Ship Security Officer chiarendone le cause.

Nel caso lo Ship Security Officer valuta che la chiave sia stata sottratta volontariamente, egli provvederà ad informare il Comandante il quale valuterà le opportune azioni (cambio serratura etc.).

Possono essere utilizzati sistemi di chiusura quali key-cards, piombatura o speciali nastri adesivi dal cui esame visivo si può dedurre facilmente che gli stessi sono stati aperti da personale non autorizzato. Questo ultimo sistema può essere utilizzato anche per le vie di sfuggita **non** dal lato di fuga. In tutti i casi si dovranno prevedere istruzioni di comportamento da parte del personale di bordo.

11.5 Monitoraggio Aree ad Accesso Limitato

L'estensione dei controlli ed azioni da effettuare sono in funzione del Livello di Security da adottare (vedi Capitolo "Livelli Security") e comprendono:

- Stabilire personale di guardia o ronda definendo numero persone, turni e frequenza ronde e modalità
- Attivare illuminazione prevista per la security ed eventuale illuminazione di terra
- Prevedere continua sorveglianza e/o attivazione di impianti fissi di rilevazione

Emesso da	Approvato da	Data	Revisione 0	Pagina 3 di 3
PIANO SECURITY(NAVE) AREE AD ACCESSO LIMITATO E MONITORAGGIO <i>Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				CAP. 11

- *Chiudere a chiave tutte le porte di accesso ai Punti Vulnerabili definiti al par. 11.3.*
- *Assicurare che l'accesso alle aree sia ristretto solo al personale autorizzato*
- *Verificare l'autorizzazione delle persone presenti nelle aree*
- *In caso di nave all'ancora stabilire personale di guardia dotandolo di mezzo di comunicazione con il Ponte di Comando*
- *Effettuare ricerche di persone o altri elementi che minacciano la security nelle aree*

Emesso da	Approvato da	Data	Revisione 0	Pagina 1 di 1
PIANO SECURITY(NAVE) CONTROLLO OPERAZIONI DEL CARICO				CAP. 12
<i>Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				

Le misure di security per il carico devono essere definite in conformità a quanto indicato dall'ISPS Code Parte A Sez.7 tenendo conto della guida fornita nella Parte B para. B 9.25 e 9.26. . Fare inoltre riferimento alla guida "Metodologia di base per la trasposizione dell'assessment nel piano di security per la nave".

12.1 Generalità

Il controllo delle operazioni di caricazione della nave devono permettere di evitare manomissioni dolose dello stesso e l'imbarco di carico non previsto.

Di seguito vengono elencati i controlli da effettuare sul carico.

12.2 Controllo operazioni del carico

L'estensione dei controlli ed azioni da effettuare sono in funzione del Livello di Security da adottare (vedi Cap. "Livelli Security") e comprendono:

- *Fornire polizze del carico, piano caricazione ed informazioni come appropriato al personale addetto al controllo*
- *Stabilire con l'impianto portuale come avviene l'identificazione del carico (es.: marcatura con adesivi dedicati o altro)*
- *Stabilire con l'impianto portuale le aree da utilizzare per il controllo prima dell'imbarco di auto, autoarticolati, moto, contenitori ed altri carichi*
- *Informarsi circa eventuali sistemi di controllo da parte del porto/impianto portuale per la security con i quali prevedere di coordinarsi*
- *Nel caso di operazioni nave/nave fornire istruzioni specifiche concordate al personale di controllo*
- *Controllare spazi carico prima/dopo caricazione*
- *Controllare il carico e/o attivare gli impianti fissi di rilevazione*
- *Verificare rispondenza carico con polizza di carico fornita*
- *Verificare numeri matricola contenitori*
- *Controllare identificazione carico*
- *Verificare integrità carico trasportato mezzo esame visivo o.....*
- *Ispezionare carico (es. auto) mezzo.....*
- *Verifica merci e sostanze pericolose*
- *Sospensione delle operazioni di carico*

Emesso da	Approvato da	Data	Revisione 0	Pagina 1 di 2
PIANO SECURITY(NAVE)				CAP.
CONTROLLO OPERAZIONI IMBARCO FORNITURE DI BORDO				13
Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)				

Le misure di security per il controllo delle forniture di bordo da imbarcare devono essere definite in conformità a quanto indicato dall'ISPS Code Parte A Sez. 7 e tenendo conto della guida fornita nella Parte B para. 9.33 e 9.34. . Fare inoltre riferimento alla guida "Metodologia di base per la trasposizione dell'assessment nel piano di security per la nave". Esempio:

13.1 Generalità

Il controllo delle operazioni di imbarco delle forniture di bordo della nave quali provviste, bunker, materiali di rispetto, di consumo devono permettere di evitare manomissioni dolose, di imbarcare forniture non ispezionate e non previste.

Di seguito vengono elencati i controlli da effettuare sulle forniture di bordo.

13.2 Controllo operazioni forniture di bordo

L'estensione dei controlli ed azioni da effettuare sono in funzione del Livello di Security da adottare (vedi Cap. "Livelli Security") e comprendono:

13.2.1 Bunkeraggi

- *Fornire dati sul fornitore, sulle modalità di conferimento e sui quantitativi da imbarcare al personale di controllo durante l'imbarco*
- *Informarsi circa eventuali sistemi di controllo da parte del porto/impianto portuale per la security con i quali provvedere a coordinarsi*
- *Attivare impianti CCTV se presenti*
- *Illuminare la zona imbarco*
- *Identificare il personale addetto all'imbarco*
- *Nel caso di imbarco da bettolina informarsi di quali controlli di security applica il Comandante della stessa*
- *Stabilire tipo di comunicazione con il personale di terra/bettolina*
- *Permettere l'ingresso alla nave da parte del personale di terra/bettolina per il solo tempo necessario alle operazioni*
- *Verificare le quantità imbarcate*
- *Sospendere l'imbarco*

13.2.3 Provviste di bordo

- *Fornire dati sul fornitore, sulle modalità di conferimento e sui quantitativi da imbarcare al personale di controllo durante l'imbarco*
- *Informarsi circa eventuali sistemi di controllo da parte del porto/impianto portuale per la security con i quali provvedere a coordinarsi*
- *Nel caso di operazioni nave/nave fornire istruzioni specifiche concordate al personale di controllo*
- *Mantenere aggiornata inventari nave (per le merci e sostanze pericolose anche la relativa ubicazione a bordo)*
- *Controllare spazi dedicati alle provviste prima/dopo caricazione*
- *Attivare impianti CCTV se presenti*
- *Verificare rispondenza provviste con Richieste bordo previste*
- *Controllare identificazione provviste*

Emesso da	Approvato da	Data	Revisione 0	Pagina 2 di 2
PIANO SECURITY(NAVE) CONTROLLO OPERAZIONI IMBARCO FORNITURE DI BORDO <i>Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				CAP. 13

- *Verificare integrità imballaggi forniture con mezzo esame visivo o(es.: controllo al Metal detector, utilizzo di cani ecc.)*
- *Sospensione delle operazioni di imbarco forniture*

Emesso da	Approvato da	Data	Revisione 0	Pagina 1 di 1
PIANO SECURITY(NAVE) MONITORAGGIO SECURITY NAVE				CAP. 14
<i>Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				

Le procedure per il monitoraggio dei ponti e delle aree circostanti la nave sono quelle indicate dall'ISPS Code Parte A Sez.7.2.5 e tenendo conto della guida fornita nella Parte B para. 9.42. Fare inoltre riferimento alla guida "Metodologia di base per la trasposizione dell'assessment nel piano di security per la nave".

14.1 Generalità

La nave è dotata dei mezzi necessari che permettono di assicurare il monitoraggio delle aree di ponte e delle aree circostanti la nave per individuare ed applicare misure preventive contro minacce o violazioni della security.

I mezzi utilizzati, alcuni dei quali indicati nei piani di cui al Capitolo 1, comprendono:

- *Impianti di illuminazione ponti e aree circostanti la nave*
- *Impianti CCTV (come applicabile)*
- *Personale di guardia e ronda*
- *Sistemi di rilevazione intrusione*

Riportare le specifiche tecniche basilari, se non già indicate nei piani di cui al Capitolo 1.

Mentre per gli accessi nave e relativo controllo si rimanda a quanto contenuto nel capitolo "Controllo Accessi" e per le aree ad accesso limitato a quanto contenuto nel capitolo "Aree ad accesso limitato e monitoraggio", per il monitoraggio della security nave sono state definite tre principali aree:

- *Aree dei ponti*
- *Area circostante la nave lato mare*
- *Area circostante la nave lato terra*

14.2 Controlli

L'estensione dei controlli ed azioni da effettuare sono in funzione del Livello di Security di riferimento (vedi Cap."Livelli Security") e comprendono, come applicabile alle varie aree:

- *Stabilire personale di guardia o ronda definendo numero persone, turni e frequenza ronde e relative modalità di monitoraggio*
- *Attivare illuminazione prevista per la security ed eventuale illuminazione di terra di concerto con il porto/impianto portuale*
- *Attivare impianti CCTV e prevedere continua sorveglianza*
- *Coordinare con il porto/impianto portuale la guardia alle aree circostanti alla nave lato terra e mare*
- *Organizzare ispezioni subacquee allo scafo*
- *Organizzare ronde lato banchina e mare (con imbarcazioni)*
- *Definire ulteriori aree in prossimità della nave da monitorare*
- *Effettuare ricerche di persone o altri elementi che minacciano la security nelle aree*

Emesso da	Approvato da	Data	Revisione 0	Pagina 1 di 2
PIANO SECURITY(NAVE)				CAP.
PROCEDURE PER RISPONDERE ALLE MINACCE E VIOLAZIONE DELLA SECURITY				15
<i>Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				

Le procedure per rispondere alle minacce o violazione della security sono quelle indicate dall'ISPS Code Parte A Sez. 9.4.4 e 9.4.6 e tenendo conto della guida fornita nella Parte B para. 8.9 relativo alle eventuali minacce. Da identificare quali di queste procedure sono anche previste dal manuale ISM e come gestire le procedure nel loro insieme.

15.1 Generalità

La Compagnia ha stabilito le procedure in risposta a minacce o violazioni della security della nave che comprendono un danno, la perdita o la distruzione della proprietà, della perdita della vita e qualsiasi atto illegale.

Qualsiasi persona, un gruppo di persone o un gruppo militare o paramilitare può iniziare la minaccia.

La Compagnia consapevole di quanto sopra, ha sviluppato una serie di procedure per rispondere a queste minacce ed eventuali violazioni della security comprese disposizioni per garantire le operazioni fondamentali dell'interfaccia nave/porto e per l'evacuazione della nave.

Queste procedure comprendono:

- *Minaccia di una bomba*
- *Piano di ricerca*
- *Individuazione di una bomba o un pacco sospetto*
- *Incendio doloso*
- *Sabotaggio o vandalismo*
- *Dirottamento o sequestro della nave o delle persone a bordo*
- *Manomissioni dolose alla nave ed al carico*
- *Immigranti illegali/clandestini*
- *Trasporto di droga e contrabbando di armi o apparecchiature*
- *Utilizzo della nave per trasportare persone intenzionate a causare un incidente di security, incluso l'utilizzo della stessa come arma per causare danni o distruzioni*
- *Atti di pirateria in mare aperto, all'ancora ed all'ormeggio*
- *Scomparsa di un membro dell'equipaggio*
- *Movimenti sospetti di un'altra nave (Attacco dal mare)*
- *Movimenti aereomobili sospetti (tenendo conto della Pick-up Area)*
- *Altri casi.....*

Devono essere elencate le azioni da effettuare per ogni caso previsto.

15.2 Rapportazione

In caso di uno qualsiasi dei casi previsti di cui sopra, lo Ship Security Officer secondo le indicazioni del Comandante deve rapportare l'accaduto alle competenti Autorità di security e relazionare, con la massima sollecitudine possibile, al Company Security Officer che informerà, se del caso, l'Amministrazione.

Emesso da	Approvato da	Data	Revisione 0	Pagina 2 di 2
PIANO SECURITY(NAVE)				CAP.
PROCEDURE PER RISPONDERE ALLE MINACCE E VIOLAZIONE DELLA SECURITY				15
<i>Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				

Il Rapporto di Atto illegale/minaccia o violazione della Security dovrebbe contenere:

- *Individuazione nave*
- *Data, ora e posizione nave come applicabile*
- *Breve descrizione dell'accaduto*
- *Individuazione dati e contatti PFSO e/o Autorità intervenute, come pertinente*
- *Mezzi utilizzati per l'atto illegale (particolari) e relativi metodi per introdurli sulla nave o nell'impianto portuale*
- *Numero dei presunti colpevoli dell'atto e dettagli*
- *Numero presunte vittime e dettagli*
- *Tipi di danni subiti dalle vittime*
- *Proposte di misure protettive preventive derivanti da quanto rapportato*

Nei casi di incidenti relativi alla Security, dovranno comunque essere messe in atto, a giudizio del Comandante, le seguenti azioni:

- *Proibire/restringere l'entrata nell'area coinvolta*
- *Restringere l'entrata sulla nave alle sole persone che dovranno reagire a quanto accaduto e che concorrono a ristabilire il livello di security*
- *Applicare le misure appropriate relative al livello di security superiore*
- *Notificare l'emergenza all'Autorità, all'Impianto Portuale o ad altra nave*
- *Informare il personale di bordo sull'esigenza di vigilare e su quanto è accaduto*
- *Evacuare la nave se necessario*

Emesso da	Approvato da	Data	Revisione 0	Pagina 1 di 4
PIANO SECURITY(NAVE) AUDITS E REVISIONI DEL PIANO SECURITY NAVE				CAP. 16
Riferimento : SOLAS 74 Capitolo XI-2 e del Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)				

Il piano deve essere conforme quanto indicato nell'ISPS Code Parte A Sez. 9.4, tenendo conto della guida fornita nella Parte B medesimo paragrafo.
Devono essere indicate le procedure per la revisione del Piano, il riesame e le procedure per l'effettuazione degli audit interni.

16.1 Generalità

Il Piano della Security (questo piano) soddisfa gli scopi sotto elencati:

1. *contribuisce alla prevenzione di atti illegali contro la nave, il suo equipaggio, i passeggeri ed il carico*
2. *chiarisce la politica della Compagnia per una sicura ed efficiente condotta delle navi gestite a nome dei clienti della Compagnia..... (se la Compagnia è una Società di Gestione navale);*
3. *chiarisce come la nave/Compagnia risponde a eventi pianificati e non pianificati relativi alla security e che possono accadere; e*
4. *rappresenta il riferimento per tutte le attività relative alla security a bordo della nave.*

*Il Piano contiene le istruzioni e le procedure utilizzate dalla nave e dalla compagnia per soddisfare gli standards internazionali per una sicura gestione e operatività della nave in conformità al Capitolo XI-2 della Solas ed al ISPS Code **"Codice Internazionale per la Sicurezza delle Navi e degli Impianti Portuali"**.*

Nel Piano viene utilizzato il termine inglese "security" per poter meglio evidenziare la differenza dal termine "sicurezza" (safety) utilizzato nel Manuale per il ISM Code.

Il Piano descrive inoltre come la politica della Compagnia è applicata e rappresenta una guida di riferimento per tutto il personale coinvolto nelle attività sulla nave ed in Compagnia.

Le procedure descritte in questo piano devono essere seguite da tutto il personale di terra e di bordo coinvolto

Il Piano è di proprietà della nave ed il suo uso è ristretto alla Compagnia ed alla nave stessa nelle persone del Comandante e del Ship Security Officer e non può essere distribuito a nessuno senza l'autorizzazione del Company Security Officer.

Il Piano è approvato dall'Amm.ne di bandiera o da un ente da essa riconosciuto (Organizzazione di Security Riconosciuta), incluso le relative revisioni. Gli unici piani approvati sono quelli con evidenza in originale dell'approvazione come sopra indicato.

Al momento della richiesta per le verifiche a bordo al fine dell'ottenimento del certificato conforme alla SOLAS Cap. XI-2 e al ISPS Code Parte A, il presente piano deve essere già stato approvato e devono già essere state attuate le misure di sicurezza previste, altrimenti la nave non potrà ricevere il certificato internazionale di sicurezza della nave.

Emesso da	Approvato da	Data	Revisione 0	Pagina 2 di 4
PIANO SECURITY(NAVE) AUDITS E REVISIONI DEL PIANO SECURITY NAVE				CAP. 16
<i>Riferimento</i> : SOLAS 74 Capitolo XI-2 e del Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)				

Per i contenuti del piano si rimanda ai relativi capitoli.

16.2 Lista di distribuzione controllata

Compagnia	Nave	Amministrazione
<i>Company Security Officer</i>	<i>Ship Security Officer</i>	<i>Autorità che procede all'approvazione dello Ship Security Plan</i>
		<i>L'Autorità che assicura il coordinamento operativo delle varie attività per la Maritime Security delle navi nazionali</i>

Il Piano deve essere tenuto sotto controllo e protetto da parte degli interessati e non deve essere reso accessibile alle persone non coinvolte nelle attività indicate in questo piano. Il piano è strettamente confidenziale. Nella copertina del Piano viene indicato il nr. della copia e a chi è stata consegnata. Per le revisioni vedasi paragrafo successivo.

E' esplicitamente vietato fare qualunque fotocopia del piano completo e relativi allegati.

Si deve definire come viene gestita la documentazione su supporto informatico, compreso hardware e software (es. files in pdf.file per evitarne la modifica, password ecc.)

Generalmente il Piano non è soggetto a controllo da parte dei Governi Contraenti a meno che non esistano fondati motivi per cui un ufficiale debitamente autorizzato dal Governo Contraente ritenga che la nave non sia conforme ai requisiti imposti dalle pertinenti norme. In tal caso funzionari, con la debita autorizzazione, possono accedere al Piano per verificare i requisiti sulla security per individuare le eventuali appropriate azioni correttive.

Per maggiori dettagli si rimanda a quanto stabilito nell'ISPS Code Parte A Sez. 9.8 e 9.8.1.

16.3 Riesame

Il Piano viene riesaminato almeno annualmente e sulla base delle valutazioni effettuate dal Company Security Officer e dallo Ship Security Officer (vedi anche capitolo 17) al fine di garantirne la dovuta efficacia, a seguito dei risultati relativi a:

- *Verifiche effettuate dall'Amministrazione di bandiera, e da Governi Contraenti degli Stati dei porti di approdo*
- *audit interni,*
- *esperienze a seguito di esercitazioni o addestramenti svolti a bordo sulla security ed eventuali problematiche emerse*

Emesso da	Approvato da	Data	Revisione 0	Pagina 3 di 4
PIANO SECURITY(NAVE) AUDITS E REVISIONI DEL PIANO SECURITY NAVE <i>Riferimento : SOLAS 74 Capitolo XI-2 e del Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				CAP. 16

- incidenti relativi alla security occorsi alla nave o rapporti di incidenti avvenuti su altre navi
- esperienze acquisite nel tempo in materia di security o in risposta a nuovi requisiti

Le modifiche del Piano devono essere validate dal Company Security Officer ed approvate dall'Amministrazione.

Quando le parti revisionate vengono inviate alle persone indicate nella lista di distribuzione, queste devono provvedere a:

1. Accertarsi che il plico contenente la documentazione non sia stato manomesso (nel caso deve essere avvisato subito il Company Security Officer)
2. Aggiornare il piano con le parti revisionate registrando quanto effettuato nel foglio Revisioni contenuto nel piano
3. Distruggere le parti sostituite.

E' responsabilità del Company Security Officer provvedere, a seguito delle modifiche apportate al Piano, l'invio dei relativi aggiornamenti debitamente approvati come applicabile, alla nave.

16.4 Audit Interni

Gli audits interni hanno lo scopo di determinare se:

- Il sistema di gestione per la security della nave è conforme alle disposizioni stabilite
- Il sistema di gestione per la security è efficacemente messo in atto e mantenuto
- Le attività sono svolte in conformità ai requisiti dell'ISPS Code ed ad eventuali ulteriori requisiti imposti dall'Amministrazione di bandiera

La responsabilità della pianificazione degli audits è del Company Security Officer.

La periodicità degli audits interni è almeno annuale.

Gli audits interni sono svolti da auditors debitamente qualificati dalla Compagnia e sono indipendenti rispetto alle attività auditate.

Gli audits interni vengono eseguiti utilizzando la modulistica.....

Gli audits interni prevedono la verifica di eventuali azioni messe in atto per correggere eventuali rilievi da audits precedenti o da verifiche effettuate dall'Amministrazione.

I risultati degli audits sono registrati nel modulo....., che contiene eventuali rilievi, documentazione di supporto e le conclusioni dell'auditor. Detti risultati sono portati all'esame del Comandante, dello Ship Security Officer e del Company security Officer.

I documenti relativi agli audits interni sono conservati dallo Ship Security Officer a bordo e dal Company Security Officer in Compagnia e devono essere resi disponibili durante le verifiche esterne previste.

16.5 Gestione rilievi

Emesso da	Approvato da	Data	Revisione 0	Pagina 4 di 4
PIANO SECURITY(NAVE) AUDITS E REVISIONI DEL PIANO SECURITY NAVE				CAP. 16
<i>Riferimento</i> : SOLAS 74 Capitolo XI-2 e del Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)				

Per la gestione dei rilievi e le azioni da effettuare fare riferimento, eventualmente, anche a quanto contenuto nel Manuale ISM. Tenere in considerazione anche la guida fornita nel ISPS Code Parte B para 4.33.

Nel caso di rilievi relativi ad anomalia nel funzionamento delle apparecchiature o dei sistemi di sicurezza, o di sospensione di una misura di sicurezza per qualsivoglia motivo, le temporanee misure di sicurezza equivalenti che sono state adottate, sono notificate dal Company Security Officer all'Amministrazione di bandiera e da essa approvate.

Emesso da	Approvato da	Data	Revisione 0	Pagina 1 di 2
PIANO SECURITY(NAVE) VALUTAZIONE SECURITY NAVE				CAP. 17
<i>Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				

Per le considerazioni sulla valutazione della security della nave si rimanda al documento "Security Assessment per la Nave". Lo SSA deve comprendere anche un'ispezione in loco (On scene-survey).

17.1 Valutazione Security nave

La valutazione è il primo scalino per sviluppare il Piano per la Security. E' responsabilità del Company Security Officer assicurare che l'effettuazione della valutazione della security sia eseguita da personale competente con la professionalità richiesta per poter valutare la security della nave.

Per l'effettuazione delle operazioni sotto indicate devono essere utilizzati i moduli.....

La valutazione di sicurezza comprende i seguenti elementi:

- *identificazione di possibili minacce alle principali operazioni di bordo della nave e della probabilità che si verifichi un problema, per la definizione delle misure di security e la determinazione del loro ordine di priorità;*
- *identificazione dei punti deboli, fattore umano compreso, delle infrastrutture, politiche e procedure.*
- *identificazione e valutazione delle principali operazioni di bordo della nave che è importante proteggere;*
- *identificazione delle attuali misure, procedure ed operazioni di security;*

La valutazione della security dovrebbe comprendere gli elementi indicati nella Parte B del Codice ISPS par. 8.3 e cioè:

- *sicurezza fisica;*
- *integrità strutturale;*
- *sistemi di protezione individuale;*
- *procedure generali;*
- *sistemi di radio e telecomunicazioni, compresi reti e sistemi informatici;*
- *altri elementi che, se danneggiati o utilizzati per osservazioni illecite, possono rappresentare un rischio per le persone, i beni o le operazioni a bordo della nave o all'interno dell'impianto portuale.*

La visita a bordo (on-scene security survey) è parte integrante della valutazione ed ha lo scopo di esaminare e valutare le misure, le procedure e le operazioni di protezione per:

- *garantire che tutte le operazioni di security della nave siano effettuate;*
- *sorvegliare le zone ad accesso ristretto per accertare che solo le persone autorizzate vi abbiano accesso;*
- *controllare l'accesso alla nave, compresi eventuali sistemi di identificazione;*
- *sorvegliare il ponte e la zona attorno alla nave;*
- *controllare l'imbarco delle persone e dei loro effetti personali (bagagli a mano, bagagli non accompagnati ed effetti personali del personale della nave);*
- *sorvegliare la movimentazione del carico e la consegna delle provviste di bordo; e*

garantire che i sistemi di comunicazione di security, le informazioni relative alla security e le apparecchiature di security della nave siano rapidamente disponibili.

Per raggiungere i requisiti sopra elencati l'approccio dovrebbe essere quello dell'effettuazione di una analisi del rischio per la nave per identificare le minacce e gli specifici scenari che il Piano dovrà contemplare ed una visita a bordo per definire le vulnerabilità ed identificare le misure da adottare per tali vulnerabilità. Tra i punti vulnerabili si possono segnalare. stazioni Aria condizionamento e ventilazione, locali batteria, locale CO2, locali ascensori, sottostazioni elettriche, locali pitture.

Emesso da	Approvato da	Data	Revisione 0	Pagina 2 di 2
PIANO SECURITY(NAVE) VALUTAZIONE SECURITY NAVE				CAP. 17
<i>Riferimento: SOLAS 74 Capitolo XI-2 e Codice Internazionale per la Sicurezza delle navi e degli impianti portuali (ISPS Code)</i>				

17.2 *Riesame*

La valutazione Security nave con il relativo rapporto è riesaminata ed approvata dal Company Security Officer ed è parte integrante, con le relative registrazioni (es.: analisi del rischio e valutazione vulnerabilità, risultati della On-scene survey e considerazioni), di questo Piano ed è pertanto un documento confidenziale che deve essere gestito analogamente come indicato al Capitolo 16.

Eventuali effettuazioni di valutazioni supplementari dovranno essere gestite come sopra indicato.