MARINA MILITARE

Agenzia di Sicurezza

Disciplinare Interno per l'utilizzo dei servizi Non Classificati di posta elettronica ed accesso ad Internet

Edizione 2015

MARINA MILITARE

ATTO DI APPROVAZIONE

Approvo la direttiva "Disciplinare Interno per l'utilizzo dei servizi non classificati di posta elettronica ed accesso ad internet" - edizione 2015

ROMA Lì 28 AGO. 2015

IL CAPO DI STATO MAGGIORE DELLA MARINA

REGISTRAZIONE DELLE AGGIUNTE E VARIANTI

1	
2	
3	
4	
5	
6	
7	

INDICE

ELENCO DELLE APPENDICI

1. Premessa

La M.M. con la realizzazione della struttura informatica – denominata MARINTRANET (Intranet M.M.I.), si pone come obiettivo primario quello di consentire a qualunque utente della rete M.M., purché debitamente autorizzato, di poter accedere ai dati e alle procedure residenti nei sistemi informativi automatizzati del proprio Comando/Ente o di qualsiasi altro Comando/Ente dell'Amministrazione M.M., indipendentemente dalla dislocazione geografica e dal sistema operativo dei vari sistemi informatici allacciati alla stessa, sia che questi siano di un Comando/Ente terrestre che di Comando Navale (indifferentemente in porto o in navigazione).

L'architettura di rete realizzata consente inoltre l'interconnessione alla rete Internet e alle intranet delle altre FF.AA.

In tale contesto, allo scopo di armonizzare le diverse direttive in materia di sicurezza informatica e privacy, è necessario definire le modalità di accesso alle diverse risorse messe a disposizione dall'Amministrazione onde assicurare la funzionalità ed il corretto impiego di tali risorse da parte degli utenti, utilizzando al contempo idonee misure di sicurezza per garantire la disponibilità e l'integrità dei sistemi informativi stessi ed i relativi dati nonché prevenire eventuali utilizzi indebiti dello strumento.

2. Principi

Il presente disciplinare è stato predisposto nel rispetto della vigente normativa in materia di Privacy, con riguardo, alle norme del D. Lgs. 196/03 (Codice in materia di protezione dei dati personali, di seguito "Codice") che disciplinano il trattamento effettuato dai soggetti pubblici, nel rispetto del Provvedimento generale del Garante della privacy n° 13 del 1 marzo 2007, pubblicato sulla G.U. - Serie generale n. 58 del 10.03.2007 (di seguito "il Provvedimento"), rafforzato successivamente dalla direttiva 02/09 della Presidenza del Consiglio dei Ministri – Dipartimento della Funzione Pubblica, datata 26.05.2009, nel rispetto della Policy di sicurezza inerente l'utilizzo della posta elettronica e di internet.

Il Ministero della Difesa - Marina garantisce che il trattamento dei dati personali dei propri dipendenti, effettuato per verificare il corretto utilizzo della Posta elettronica e di Internet, si conforma ai seguenti principi:

a. il ***principio di necessità***, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 3 del Codice; par. 5.2 del Provvedimento);
b. il ***principio di correttezza***, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art. 11, comma 1, lett. a), del Codice) poiché le tecnologie dell'informazione, in modo più marcato rispetto ad apparecchiature tradizionali, permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa, anche all'insaputa o, comunque, senza la piena consapevolezza dei lavoratori (par. 3 del Provvedimento);
c. ***principio di pertinenza e non eccedenza*** (par. 6 del Provvedimento), in virtù del quale:
   - i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime

(art. 11, comma 1, lett. b) del Codice; par. 4 e 5 del Provvedimento);

- il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile";
- le attività di monitoraggio devono essere svolte solo da soggetti preposti (par. 8 del Provvedimento) ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza" (Parere n. 8/2001 del 13.09.2001, punti 5 e 12).

3. Informativa sulle modalità di utilizzo di Posta elettronica ed Internet

Il Ministero della Difesa - Marina informa i fruitori dei servizi in questione in merito alle modalità consentite di utilizzo di Posta elettronica ed Internet, attraverso la pubblicazione delle relative politiche d'uso, all'interno dei siti intranet dell'Amministrazione.

Il presente disciplinare riporta, di seguito, le politiche di uso di Posta elettronica ed Internet attualmente in vigore.

4. Posta elettronica

La presente direttiva disciplina l'utilizzo del servizio di posta elettronica (ovvero Servizio) del dominio **marina.difesa.it** in conformità alle leggi vigenti e alle ulteriori disposizioni emanate dallo Stato Maggiore Marina.

L'Amministrazione, anche sulla base delle direttive del Governo tese a promuovere la crescita delle comunicazioni in formato digitale e l'abbattimento di quelle cartacee, considera la posta elettronica uno strumento fondamentale, che viene messo a disposizione di tutti gli utenti.

La presente direttiva vale anche come informativa sulle finalità e modalità del trattamento dei dati personali, ricavabili dalle attività di controllo tecnico svolte sul servizio di posta elettronica, ai sensi dell'art. 13 della legge 196/2003.

4.1 Scopo

Scopo della presente direttiva è assicurare che:

a. gli utenti del servizio di posta elettronica siano informati delle disposizioni di legge vigenti e della giurisprudenza relativa alla disciplina dell'uso della posta elettronica;
b. il servizio di posta elettronica sia utilizzato dagli utenti in conformità a tali disposizioni;
c. gli utenti del servizio di posta elettronica siano informati in merito ai concetti di privacy e di sicurezza applicabili all'uso della posta elettronica;
d. il servizio di posta e altri servizi siano fruibili con la massima continuità ed affidabilità.

4.2 Destinatari

La presente direttiva si applica a:

- tutti i sistemi ed i servizi di posta elettronica afferenti il dominio **marina.difesa.it**;
- agli amministratori e fornitori di tali servizi;
- tutto il personale, militare e civile, dotato di una casella di posta elettronica, definita nel dominio **marina.difesa.it**;

- ogni altra categoria di personale come ad esempio fornitori, consulenti, personale estraneo all'Amministrazione M.M., cui venga fornito in modo temporaneo un account di posta elettronica per lo svolgimento delle proprie attività e/o esigenze operative.

Inoltre, si applica indifferentemente ai contenuti dei messaggi di posta e alle informazioni transazionali (header dei messaggi, indirizzi di posta, dati dei destinatari e dei mittenti) relative a tali messaggi.

4.3 Caselle di posta elettronica

Nel dominio **marina.difesa.it** sono stati definiti quattro tipi di caselle di posta elettronica con le seguenti caratteristiche:

1. **Nominativa** : la creazione e l'assegnazione della casella di posta elettronica nominativa avviene automaticamente all'atto dell'arruolamento del personale (sia come volontario in ferma prefissata che in S.P.E.) e comunque in concomitanza dell'emissione della Carta Multiservizi della Difesa (Mod. ATe), previa sottoscrizione della "liberatoria per l'uso del servizio e-mail" in allegato al presente Disciplinare. Successivamente, tale liberatoria, sarà sottoscritta dall'utente ogni 5 anni con modalità che verranno dettagliate con apposita normativa.

   Il Ministero della Difesa - Marina fornisce un codice Utente ed una password "standard" che dovrà essere obbligatoriamente modificata al primo collegamento. L'accesso al Servizio è consentito solo mediante tali identificativi.

   Al termine del servizio attivo o congedamento, la casella di posta elettronica nominativa sarà chiusa dai preposti Enti tecnici. Sarà cura del personale provvedere a salvare eventuali dati di interesse, fermo restando l'obbligo di riservatezza da ottemperare per le informazioni in essa contenuta.
2. **Posta Elettronica Istituzionale (P.E.I.)** : la casella di posta elettronica istituzionale (esempio: *maristat@marina.difesa.it*) è istituita per lo scambio di comunicazioni ufficiali, cioè per atti formalmente validi sotto il profilo giuridico-amministrativo che richiedono la relativa formale protocollazione. Si tratta della casella postale "*non certificata*", associata all' Area Organizzativa Omogenea ed impiegata nell'ambito del sistema di protocollo informatico. L'elenco delle P.E.I. sono pubblicate sul portale Marintranet.

   Tali caselle vengono create automaticamente e le relative credenziali di accesso sono assegnate al Titolare del Comando/Ente ed ai suoi delegati.
3. **Posta Elettronica Certificata (P.E.C.) :** la casella di posta elettronica certificata (esempio: *maristat@postacert.difesa.it*) è istituita per lo scambio di comunicazioni ufficiali, cioè per atti formalmente validi sotto il profilo giuridico-amministrativo che richiedono la relativa formale protocollazione. Si tratta della casella postale "*certificata*", associata all' Area Organizzativa Omogenea ed impiegata nell'ambito del sistema di protocollo informatico. L'elenco delle P.E.C. sono pubblicate nell'Indice delle Pubbliche Amministrazioni (www.indicepa.gov.it).

   Tali caselle vengono create automaticamente e le relative credenziali di accesso sono assegnate al Responsabile del servizio di protocollo.

4. **Funzionale :** sono caselle di posta create per esigenze specifiche della funzione collegata al servizio (esempio: *cyber.defence@marina.difesa.it*). Tali caselle sono associate ad una o più persone attraverso la casella nominativa. Le persone delegate all'utilizzo della casella funzionale possono inviare e ricevere messaggi a nome della casella stessa ed i messaggi sono condivisi a tutti i delegati.

4.4 Condizioni Generali

a. **Finalità del servizio di posta elettronica.** Il Ministero della Difesa - Marina incoraggia l'uso della posta elettronica per scambiare informazioni, migliorare le comunicazioni, scambiare idee e per rendere più efficaci ed efficienti i processi di lavoro a supporto della missione istituzionale dell'Amministrazione;
b. **Proprietà del Ministero della Difesa – Marina.** Il servizio di posta elettronica erogato tramite l'infrastruttura telematica del Centro Telecomunicazioni ed Informatica della Marina Militare di Roma (Maritele Roma), è di proprietà del Ministero della Difesa - Marina, pertanto ogni casella di posta elettronica associata al Ministero (nel dominio *marina.difesa.it*) o a suoi Comandi/Enti o assegnata a individui o funzioni del Ministero, sono di proprietà del Ministero della Difesa – Marina;
c. Anche agli utenti delle Capitanerie di Porto, viene assegnata all'atto dell'arruolamento una casella di posta elettronica del tipo *nome.cognome@marina.difesa.it*. Tale casella tuttavia verrà ridimensionata ad una capacita inferiore terminate le scuole di formazione (contestualmente alla creazione della casella nel dominio *mit.gov.it* da parte del Ministero delle Infrastrutture e dei Trasporti.
d. **Limitazioni di Responsabilità per l'Amministrazione.** Il Ministero della Difesa - Marina non può essere ritenuto responsabile per qualsiasi danno, diretto o indiretto, arrecato all'Utente ovvero a terzi e derivante:
   - dall'eventuale interruzione del Servizio;
   - dall'eventuale smarrimento di messaggi diffusi per mezzo del Servizio;
   - da messaggi inviati/ricevuti o da transazioni eseguite tramite il Servizio;
   - da accesso non autorizzato ovvero da alterazione di trasmissioni o dati dell'Utente.
e. **Restrizioni all'uso del Servizio.** Gli utenti del servizio di posta elettronica sono tenuti ad usarlo in modo responsabile, cioè, rispettando le leggi, la presente direttiva e altre norme e procedure del Ministero della Difesa - Marina e secondo normali standard di cortesia, correttezza, buona fede e diligenza professionale. L'accesso ai servizi di posta elettronica può essere totalmente o parzialmente limitato dall'Amministrazione, senza necessità di assenso da parte dell'utente e anche senza preavviso:
   - quando richiesto dalla legge e in conformità ad essa;
   - in caso di comprovati motivi che facciano ritenere la violazione della presente direttiva o delle disposizioni di legge vigenti;
   - al venir meno delle condizioni in base alle quali si ha facoltà di utilizzare il Servizio (ad es. cessazione per qualsiasi motivo del rapporto di lavoro con l'Amministrazione);
   - in casi eccezionali, quando richiesto per esigenze operative critiche e improcrastinabili.

Non è prevista alcuna forma di indennizzo per il venir meno del Servizio.

f. **Assenso e Conformità.** Il Ministero della Difesa - Marina è tenuto in generale ad ottenere l'assenso del titolare della casella di posta elettronica (nominativa) prima di ogni ispezione dei messaggi o accesso alle registrazioni o ai messaggi di posta elettronica, fatta eccezione per quanto disposto al punto e. D'altro canto, ci si attende che tutto il personale soddisfi eventuali richieste dell'Amministrazione riguardanti la fornitura di copie delle registrazioni di posta elettronica in suo possesso che riguardino le attività lavorative o richieste per soddisfare obblighi di legge, indipendentemente dal fatto che tali registrazioni risiedano o meno su computer di proprietà dell'Amministrazione. Il mancato rispetto di tali richieste può portare all'applicazione delle condizioni di cui al successivo punto g..

g. **Accesso senza assenso.** Il Ministero della Difesa - Marina non ispeziona e non accede ai messaggi di posta elettronica nominativa senza la sua autorizzazione. D'altro canto, il Ministero della Difesa - Marina potrà permettere l'ispezione, il monitoraggio o l'accesso alla posta elettronica nominativa, anche senza l'assenso del titolare della casella stessa, solamente nei seguenti casi:
   - su richiesta dell'Autorità Giudiziaria nei casi previsti dalla normativa vigente;
   - previo preavviso all'utente, per gravi e comprovati motivi[1] che facciano ritenere che siano state violate le disposizioni di legge vigenti o le direttive del Ministero della Difesa – Marina in materia di sicurezza;
   - per atti dovuti[2] ;
   - in situazioni critiche e di emergenza[3].

   Data la natura stessa delle caselle PEI, PEC e funzionali che non godono dell'esclusività del possesso e che sono utilizzate ai fini giuridico-amministrativi per lo svolgimento delle attività istituzionali, gli organi preposti del Ministero della Difesa - Marina possono effettuare controlli di corretto uso ed aderenza alle normative vigenti senza il consenso dei delegati all'utilizzo.

h. **Utilizzo di dispositivi personali e del servizio Push Mail.** Il Ministero della Difesa - Marina acconsente che gli utenti possano accedere alla propria casella di posta elettronica nominativa attraverso dispositivi personali su connessioni non dell'amministrazione. Ciò avviene collegandosi attraverso un qualsiasi browser all'indirizzo https://mail.marina.difesa.it.
   Inoltre tutti gli utenti in possesso di una casella di posta elettronica nominativa hanno attivo il servizio Push Mail che consente di poter accedere a tale casella attraverso il proprio dispositivo mobile su connessione dati personale.

   Per garantire un adeguato livello di sicurezza a tale modalità di accesso, è consigliabile:

   - Non mantenere l'archivio della propria casella di posta all'interno del

[1] ***Grave e comprovato motivo:*** evidenza oggettiva, non basata quindi su semplici sospetti o illazioni, che dimostra l'avvenuta violazione di disposizioni di leggi vigenti o delle politiche di sicurezza dell'Amministrazione.

[2] ***Atti dovuti:*** circostanze in base alle quali la mancanza di adeguate azioni può comportare danni significativi a cose o persone, perdita di informazioni di rilievo per l'Amministrazione o danni economici e di immagine per l'Amministrazione e per le persone che ne fanno parte

[3] ***Situazioni critiche o di emergenza***: circostanze in cui la tempestività d'azione è di fondamentale importanza al fine di evitare danni significativi a cose o persone, perdita di informazioni di rilievo per l'Amministrazione o danni economici e di immagine per l'Amministrazione e per le persone che ne fanno parte o l'interruzione dei servizi informatici e la continuità operativa dei processi dell'Amministrazione

dispositivo mobile. Ciò è possibile utilizzando la modalità IMAP di connessione al Server di posta che di fatto non scarica mai le e-mail sul dispositivo ma permette la gestione /consultazione direttamente sul Server Exchange.

- Proteggere il dispositivo dall'accesso non consentito attraverso l'inserimento di un codice di sblocco dalla modalità "salva schermo"
- Procedere all'immediato cambio della password dell'account di posta, non appena si ha consapevolezza della perdita o del furto del proprio dispositivo.

4.5 Avvertenze

Gli utenti del servizio di posta elettronica sono avvisati del fatto che:

a. La natura stessa della posta elettronica la rende meno sicura di quanto si possa immaginare. Ad esempio, i messaggi di posta elettronica spediti ad una persona possono essere facilmente inoltrati successivamente ad altri destinatari. Il Ministero della Difesa - Marina non può proteggere gli utenti da eventi come quelli descritti che esulano dalle proprie possibilità e compiti. Gli utenti pertanto devono esercitare la massima cautela nell'uso della posta elettronica per comunicare informazioni private o dati sensibili;
b. I messaggi di posta elettronica, creati e conservati sia su apparati elettronici forniti dall'Amministrazione che su altri sistemi, possono costituire registrazioni di attività svolte dall'utente nell'espletamento delle sue attività lavorative. E' possibile quindi che venga richiesto di accedere ai contenuti dei messaggi per un eventuale utilizzo nell'ambito di contenziosi che coinvolgano l'Amministrazione. Il Ministero della Difesa - Marina non darà corso automaticamente a tutte le richieste di accesso, ma le valuterà in relazione a precisi obblighi di legge quali la privacy ed altre normative applicabili. Gli utenti devono però tener presente che, per quanto detto, in nessun caso l'Amministrazione può garantire che non saranno accedute informazioni personali degli utenti presenti in messaggi di posta elettronica residenti sui sistemi dell'Amministrazione;
c. il Ministero della Difesa - Marina, in generale, non può e non intende porsi come valutatore dei contenuti dei messaggi di mail scambiati, né può proteggere gli utenti dalla ricezione di messaggi che possano essere considerati offensivi. Gli utenti sono comunque fortemente incoraggiati a usare nella posta elettronica le stesse regole di cortesia che adopererebbero in altre forme di comunicazione;
d. non vi è garanzia, a meno di utilizzare sistemi di posta certificata (firma digitale – Carta Multiservizi Difesa ed altre P.K.I formalmente riconosciute), che i messaggi ricevuti provengano effettivamente dal mittente previsto, poiché è piuttosto semplice per i mittenti mascherare la propria identità, anche se ciò costituisce, tra le altre cose, una violazione della presente direttiva. Inoltre i messaggi di posta che arrivano come "inoltro" di precedenti messaggi, potrebbero essere stati modificati rispetto all'originale. Pertanto, in caso di dubbi, chi riceve un messaggio di posta elettronica è tenuto a verificare con il mittente l'autenticità delle informazioni ricevute.

4.6 Limitazioni all'uso personale della casella di posta elettronica

a. Non è consentito l'utilizzo della propria casella nominale nel dominio

"**marina.difesa.it**" a fini privati e personali; l'indirizzo di posta elettronica (e-mail) assegnato, ancorché nella forma *nome.cognome@marina.difesa.it*, è di proprietà dell'Amministrazione e costituisce normale strumento di lavoro. In tale ambito l'amministrazione fornisce in automatico la configurazione formale della posta elettronica con uno specifico disclaimer (dichiarazione di esclusione di responsabilità) [4] automaticamente generato all'atto della stesura di un nuovo messaggio di posta elettronica. E' fatto divieto all'utente di cancellare il disclaimer di cui trattasi.

a. E' fatto divieto a tutti gli utenti di utilizzare il servizio di posta elettronica per inviare messaggi dannosi, di tipo offensivo o sconveniente, come ad esempio, a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di messaggio che possa arrecare danno alla reputazione del Ministero della Difesa - Marina. E' inoltre vietato l'uso del servizio di posta elettronica per diffondere messaggi che inducano il destinatario a produrre altre copie da spedire, a propria volta, a nuovi destinatari (e-mail che generano le cosiddette "catene di Sant'Antonio"), la partecipazione a dibattiti, forum o mailing list, ecc., a scopi commerciali o di profitto personale e per attività illegali e la fornitura a qualsiasi titolo, di qualunque lista o elenco degli utenti del servizio. E' proibito fornire le proprie credenziali di accesso a sistemi o procedure, così come rispondere a messaggi e-mail che facciano richiesta di questo tipo di informazioni. Chiunque riceva comunicazioni della natura sopra indicata dovrà segnalarlo al CERT T.C. [5] della MARINA (cert@marina.difesa.it) e per conoscenza a MARISTAT OCS – 6° Ufficio Sicurezza Cibernetica, Informatica e delle Comunicazioni (CERT C.C.[6] - cyber.defence@marina.difesa.it).

   E' altresì vietato utilizzare l'indirizzo di posta elettronica nominativa per l'iscrizione su siti web di qualsiasi natura (social forum, blog ecc.) a meno di quelli necessari al lavoro di ufficio (ad esempio siti governativi ed extranazionali come il sito NATO). La casella di posta elettronica può essere utilizzata per tutte quelle attività che a qualsiasi titolo rientrano nella sfera lavorativa, come ad esempio la registrazione presso alberghi durante le missioni. E' importante ricordare che ogni volta si effettua una registrazione dei propri dati presso un servizio WEB o un servizio tradizionale, bisogna negare il consenso alla trasmissione dei propri dati a società terze per fini di mercato (questa opzione è sempre presente in tutti i moduli di registrazione).

4.7 Sicurezza e riservatezza

a. Oltre a quanto indicato al par. 4.3, gli utenti devono tener presente che, nell'assolvimento dei propri compiti, il personale che gestisce i sistemi di elaborazione e le reti di telecomunicazione può avere, saltuariamente, la

---

[4] TESTO DISCLAIMER UTILIZZATO IN AMBITO MARINA: Questa e-mail e tutti i suoi allegati sono da intendersi inviati esclusivamente per motivi di servizio e sono da considerarsi quali USO ESCLUSIVO DI UFFICIO; come tali saranno soggetti alle relative restrizioni legali. Se non siete l'effettivo destinatario o avete ricevuto il messaggio per errore, siete pregati di cancellarlo dal vostro sistema e di avvisare il mittente. E' vietata la duplicazione, l'uso a qualsiasi titolo, la divulgazione o la distribuzione dei contenuti di questa e-mail a qualunque altro soggetto. Laddove fosse necessario il re-inoltro del messaggio, chi esegue l'operazione si assume in proprio gli oneri di tale estensione.

[5] C.E.R.T. T.C. : Computer Emergency Response Team Technical Center

[6] C.E.R.T. C.C. : Computer Emergency Response Team Coordination Center

necessità di analizzare i dati transazionali (database) dei messaggi di posta per garantire il corretto funzionamento del servizio e in queste occasioni è possibile che avvengano inavvertitamente accessi al contenuto stesso dei messaggi. Tale personale è tenuto comunque al rispetto di stretti vincoli di riservatezza qualora si verificassero i casi citati; l'accesso a tali dati avviene tramite postazioni dotate di *strong authentication* (uso contestuale di una duplice tecnologia di autenticazione) e tutte le operazioni effettuate dagli amministratori vengono memorizzate, come disposto dal Garante della Privacy nelle *"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"* (G.U. n. 300 del 24.12.2008).

b. il Ministero della Difesa - Marina si pone come obiettivo fondamentale, la fornitura di servizi di posta elettronica sicuri ed affidabili avvalendosi di personale qualificato. Va comunque ricordato, come già detto in precedenza, che la sicurezza e riservatezza della posta elettronica non possono essere garantite in ogni circostanza, in particolare per quanto concerne i messaggi di posta scaricati sul proprio personal computer. In questo caso è indispensabile che l'utente stesso provveda ad attuare le azioni adeguate a proteggere le informazioni usando tutti i mezzi disponibili, quali ad esempio password di accesso alle applicazioni ed alla propria postazione di lavoro e di bloccare (log-off) la propria postazione prima di allontanarsi dalla stessa.

4.8 Archiviazione e conservazione

L'archiviazione e la conservazione dei messaggi di posta elettronica avviene tramite l'infrastruttura telematica del Centro Telecomunicazioni ed Informatica della Marina Militare di Roma (MARITELE Roma) mediante procedure di backup giornaliero. Si evidenzia che il backup viene effettuato esclusivamente sui messaggi di posta elettronica giacenti sul server Exchange e non sui messaggi di posta eventualmente scaricati sul computer dell'utente (cartelle personali).

La riservatezza viene assicurata poiché il formato stesso del backup (Information Store Database) non consente la visualizzazione del singolo messaggio di posta elettronica se non al legittimo proprietario della casella e-mail che vi accede autenticandosi con username e password personali.

4.9 Violazioni

Il personale che contravviene alle norme indicate nella presente direttiva di sicurezza, stanti le responsabilità individuali di tipo civile e penale verso terze parti offese, potrà essere oggetto nei limiti previsti dalla legge, di azioni di accertamento delle responsabilità ed, eventualmente, delle conseguenti sanzioni.

In Appendice 3 è riportata una tabella di riferimento circa le eventuali sanzioni comminabili in funzione alla violazione commessa.

5. Internet

La presente direttiva disciplina l'utilizzo del servizio di accesso a Internet in conformità alle leggi vigenti e alle ulteriori disposizioni emanate dallo Stato Maggiore Marina. La possibilità d'uso di Internet (ove prevista e concessa) è consentita unicamente per incrementare l'efficienza e la produttività del proprio lavoro e deve essere sempre incentrata ai principi di Diligenza, Fedeltà e Correttezza.

L'accesso a Internet, per fare un esempio, è da intendersi alla stessa stregua di un qualsiasi altro strumento di lavoro messo a disposizione del dipendente dall'amministrazione (scrivania, automobili, Personal Computer, etc) e quindi valgono le stesse restrizioni, disposizioni e norme di buon senso che abitualmente vengono adottate verso le proprietà dell'amministrazione.

L'Amministrazione, anche sulla base delle direttive del governo tese a promuovere la crescita delle comunicazioni in formato digitale, intende utilizzare le risorse e le potenzialità messe a disposizione dallo strumento telematico "Internet" per fornire un moderno e potente mezzo di informazione a disposizione di tutti gli utenti autorizzati.

La presente direttiva vale anche come informativa sulle finalità e modalità del trattamento dei dati personali, ricavabili dalle attività di controllo tecnico svolte sul servizio di navigazione su Internet, ai sensi dell'art. 13 della legge 196/2003.

5.1 Scopo

Scopo della presente direttiva è assicurare che:

a. gli utenti del servizio di accesso ad Internet siano informati delle disposizioni di legge vigenti e della giurisprudenza relativa alla disciplina dell'uso del servizio di navigazione su Internet;
b. il servizio di navigazione su Internet sia utilizzato dagli utenti in conformità a tali disposizioni;
c. gli utenti del servizio di navigazione su Internet siano informati in merito ai concetti di privacy e di sicurezza applicabili all'uso del servizio;
d. il servizio di accesso ad Internet e altri servizi siano fruibili con la massima continuità ed affidabilità.

5.2 Destinatari

La presente direttiva si applica a:

a. tutti i sistemi ed i servizi afferenti il dominio di Marintranet;
b. agli amministratori e fornitori di tali servizi;
c. tutto il personale, militare e civile, formalmente autorizzato all'impiego del servizio;
d. ogni altra categoria di personale come ad esempio fornitori, consulenti, personale estraneo all'Amministrazione M.M., cui venga fornito in modo temporaneo un account di accesso al servizio Internet per lo svolgimento delle proprie attività e/o esigenze operative.

5.3 Condizioni Generali

a. **Finalità del servizio di accesso ad Internet.** Rendere disponibile agli utenti autorizzati, per scopi connessi al servizio, l'enorme patrimonio informativo presente sulla rete pubblica Internet costituendo inoltre, un ulteriore canale di comunicazione della F.A. alla stregua delle altre tradizionali modalità di comunicazione informale (telefonia, fax, ecc.).

   Viene ammesso in via eccezionale che l'accesso ad internet venga utilizzato anche per scopi non immediatamente correlati alla prestazione lavorativa, purché ciò avvenga nel rispetto dei principi di ragionevolezza e di buona fede (imprescindibili nella esecuzione del rapporto di lavoro) e, comunque, non metta a repentaglio l'integrità e la riservatezza dei dati, delle informazioni e

dell'intero sistema informatico dell' amministrazione. Il limite massimo di accesso ad Internet per motivi non immediatamente correlati alla prestazione lavorativa, non dovrà in ogni caso superare il **10** % del periodo lavorativo ordinario giornaliero (stimato in un massimo di **40 minuti**). Al fine di consentire una corretta informazione dell'utenza, sulle pagine Marintranet del CERT Marina è possibile prendere visione delle categorie dei siti internet la cui consultazione è di *default* considerata "non per uso d'ufficio".

b. **Proprietà del Ministero della Difesa – Marina.** Il servizio di accesso ad Internet delle postazioni informatiche, è erogato esclusivamente tramite l'infrastruttura telematica del Centro Telecomunicazioni ed Informatica della Marina Militare di Roma (MARITELE Roma) ed è di proprietà del Ministero della Difesa - Marina, il quale concede tale accesso a titolo gratuito ad ogni destinatario di cui al punto 5.2 . E' espressamente vietato collegare i PP.CC. dell'Amministrazione ad Internet sfruttando altre modalità di collegamento (cellulare, modem, ecc.), ed è vietato utilizzare strumenti software in grado di fornire connessioni diverse da quelle impostate dagli amministratori (proxy avoidance)[7] in quanto potrebbero compromettere, ovvero aggirare, i meccanismi di sicurezza implementati sulla rete telematica di F.A.
c. **Attivazione del Servizio.** Il servizio di accesso ad Internet viene attivato dal Comando/Ente di appartenenza ed ha la validità di cinque anni (a meno di trasferimenti dell'interessato). Nell'apposita procedura di abilitazione, dovranno chiaramente essere indicate le finalità di tale concessione, nonché le tipologie di siti web autorizzati in relazione alla finalità da conseguire. Contestualmente dovrà essere sottoscritta l'apposita liberatoria (allegata al presente disciplinare). Le modalità per la richiesta dell'abilitazione sono dettagliate in apposite disposizioni.

   Il Ministero della Difesa - Marina, dopo aver effettuato le opportune verifiche, potrà in ogni caso entrare nel merito della tipologia dei siti web autorizzati.

   Al fine di evitare l'utilizzo abusivo da parte di utenti non autorizzati è fatto divieto divulgare/condividere le proprie credenziali di accesso (username-password) con qualsiasi altro soggetto.
d. **Limitazioni di Responsabilità per l'Amministrazione**. Il Ministero della Difesa - Marina non può essere ritenuto responsabile per qualsiasi danno, diretto o indiretto, arrecato all'Utente ovvero a terzi e derivante:
   - dall'eventuale interruzione del Servizio;
   - da accesso non autorizzato ovvero da alterazione di trasmissioni o dati dell'Utente.
e. **Restrizioni all'uso del servizio.** Gli utenti del servizio Internet sono tenuti ad usarlo in modo responsabile, cioè, rispettando le leggi, la presente e altre direttive e procedure del Ministero della Difesa - Marina e secondo normali standard di cortesia, correttezza, buona fede e diligenza professionale. L'accesso ai servizi Internet può essere totalmente o parzialmente limitato dall'Amministrazione, senza necessità di assenso da parte dell'utente e anche

[7] Strumenti software in grado di permettere all'utente la navigazione su siti che altrimenti sarebbero bloccati dai sistemi Proxy dell'amministrazione

senza preavviso:

- quando richiesto dalla legge e in conformità ad essa;
- in caso di comprovati motivi che facciano ritenere la violazione della presente politica o delle disposizioni di legge vigenti;
- al venir meno delle condizioni in base alle quali si ha facoltà di utilizzare il servizio (ad es. cessazione per qualsiasi motivo del rapporto di lavoro con l'Amministrazione);
- in casi eccezionali, quando richiesto per esigenze operative critiche e improcrastinabili.

Non è prevista alcuna forma di indennizzo per il venir meno del servizio.

Inoltre, è espressamente vietato pubblicare informazioni attinenti il servizio svolto in Forza Armata o interi siti web a fini istituzionali (es. Sito del Comando, Sito del Reparto o del Progetto, etc) utilizzando risorse informatiche autonome; nel caso questo si renda necessario è obbligatorio interessare lo Stato Maggiore Marina – Rep. C4S che, se ritenuto opportuno, provvederà a soddisfare l'esigenza tramite appositi server residenti nel dominio *marina.difesa.it*.

Infine, per questioni di sicurezza, il Ministero della Difesa - Marina si riserva di valutare l'attivazione o meno di ciascun protocollo di comunicazione da impiegare verso Internet (es. HTTP, HTTPS, FTP, etc).

f. **Assenso e Conformità.** Il Ministero della Difesa - Marina è tenuto in generale ad ottenere l'assenso dell'utente all'accesso alle registrazioni informatiche, fatta eccezione per quanto disposto al successivo punto g). D'altro canto, ci si attende che tutto il personale soddisfi eventuali richieste dell'Amministrazione riguardanti la fornitura di copie di files e documenti in suo possesso che riguardino le attività lavorative o richieste per soddisfare obblighi di legge, indipendentemente dal fatto che tali files e/o documenti risiedano o meno su computer di proprietà dell'Amministrazione. Il mancato rispetto di tali richieste può portare all'applicazione delle condizioni di cui al successivo punto g..

g. **Accesso senza assenso.** Il Ministero della Difesa - Marina tratta i dati delle registrazioni (*files di log*)[8] per l'esecuzione di statistiche sull'utilizzo dei servizi. I dati contenuti nei file di log possono essere trattati, anche senza assenso dell'utente, nelle seguenti ipotesi:

- su richiesta dell'Autorità Giudiziaria nei casi previsti dalla normativa vigente;
- per gravi e comprovati motivi[9] che facciano ritenere che siano state violate le disposizioni di legge vigenti o le politiche del Ministero della Difesa - Marina in materia di sicurezza;
- per atti dovuti[10];
- in situazioni critiche e di emergenza[11].

---

[8] Direttiva n. 02 del 2009 della Presidenza del Consiglio dei Ministri paragrafo 3.

[9] ***Grave e comprovato motivo:*** evidenza oggettiva, non basata quindi su semplici sospetti o illazioni, che dimostra l'avvenuta violazione di disposizioni di leggi vigenti o delle politiche di sicurezza dell'Amministrazione

[10] ***Atti dovuti:*** circostanze in base alle quali la mancanza di adeguate azioni può comportare danni significativi a cose o persone, perdita di informazioni di rilievo per l'Amministrazione o danni economici e di immagine per l'Amministrazione e per le persone che ne fanno parte

[11] ***Situazioni critiche o di emergenza***: circostanze in cui la tempestività d'azione è di fondamentale importanza al fine di evitare danni

5.4 Avvertenze

Gli utenti del servizio Internet sono avvisati del fatto che:

a. La natura stessa di Internet, intesa come "rete mondiale" la rende meno sicura di quanto si possa immaginare. Ne consegue che, nonostante i meccanismi di sicurezza implementati sull'infrastruttura di F.A. (Marintranet) possano comunque verificarsi problematiche a livello applicativo con alcuni siti e servizi Internet malevoli (bugs del browser web, phishing, pharming[12], file infetti, ecc.). Il Ministero della Difesa - Marina non può proteggere gli utenti da fatti come quelli descritti che esulano dalle proprie possibilità e compiti. Gli utenti pertanto devono esercitare la massima cautela nell'uso di Internet durante l'utilizzo, evitando la navigazione in siti di dubbio contenuto;
b. la cronologia ed i contenuti dei siti web visitati, creati e conservati automaticamente sia su apparati informatici forniti dall'Amministrazione che su altri sistemi, possono costituire registrazioni di attività svolte dagli utenti nell'espletamento delle attività lavorative. E' possibile quindi che avvenga l'accesso a tali contenuti per un eventuale utilizzo nell'ambito di contenziosi che coinvolgano l'Amministrazione. Il Ministero della Difesa - Marina non darà corso automaticamente a tutte le richieste di accesso, ma le valuterà in relazione a precisi obblighi di legge. Gli utenti devono però tener presente che, per quanto detto, in nessun caso l'Amministrazione può garantire che non saranno accedute informazioni personali degli utenti residenti sui sistemi dell'Amministrazione;
c. il Ministero della Difesa - Marina, pur non intendendo porsi quale valutatore dell'attività svolta dai propri dipendenti nell'utilizzo della risorsa Internet, allo scopo sia di salvaguardare la propria risorsa informatica che tutelare l'utente dall'ingresso in siti web non consoni o penalmente rilevanti, si riserva di svolgere una preventiva attività di "filtro"[13] alla navigazione . Gli utenti devono comunque attenersi a norme di comportamento non contrastanti con i principi etici e morali che contraddistinguono gli appartenenti all'Amministrazione; inoltre, tutte le azioni intraprese con tale servizio non devono assolutamente costituire una minaccia per le risorse e servizi disponibili su Marintranet dal punto di vista dell'integrità e disponibilità.

   Il software installato sulle macchine connesse a Marintranet deve essere obbligatoriamente in regola con la normativa inerente la tutela del "diritto di autore" di cui alla Circolare SMM 1091 – edizione 1993, e conforme alle direttive emanate in materia dal Ministero Difesa – Marina. E' pertanto espressamente vietato scaricare/condividere/installare software non espressamente autorizzato. In ogni modo, qualsiasi installazione/disinstallazione deve avvenire attraverso apposite procedure tecniche messe in atto dall'organo tecnico centrale (MARITELE ROMA). Per quanto appena scritto, l'utente non deve assolutamente possedere i diritti di "Amministratore" della propria postazione. Qualora l'utente si accorga di possedere i diritti di

significativi a cose o persone, perdita di informazioni di rilievo per l'Amministrazione o danni economici e di immagine per l'Amministrazione e per le persone che ne fanno parte o l'interruzione dei servizi informatici e la continuità operativa dei processi dell'Amministrazione.

[12] Sofisticate tecniche di hacking che consentono di sottrarre informazioni sensibili alla vittima

[13] Vengono utilizzati strumenti informatici denominati "content/web filtering" che bloccano siti internet dai contenuti indesiderati/pericolosi per la sicurezza.

"Amministrazione" della propria postazione, deve immediatamente darne comunicazione al proprio responsabile informatico che provvederà a far ripristinare l'account con i diritti corretti. Nel Caso particolare in cui un "Account" debba necessariamente possedere i diritti di "Amministrazione" della postazione, ne dovrà essere fatta preventiva richiesta allo Stato Maggiore Marina – Agenzia di Sicurezza – 6° Ufficio Sicurezza Cibernetica, Informatica e delle Comunicazioni (cyber.defence@marina.difesa.it), che dopo averne vagliato l'effettiva necessità, provvederà all'autorizzazione.

Il Ministero della Difesa – Marina effettua controlli sulla rete atti a verificarne i flussi e l'utilizzo, in maniera tale da prevenire o individuare anomalie sia di natura tecnica che di natura malevola; inoltre controlla che sulle postazioni utente siano presenti solo i software espressamente autorizzati.

Il CERT CC ubicato presso l'Agenzia di Sicurezza – Sez. Cyber Defence mantiene costantemente aggiornata (sulla propria pagina del Portale Marintranet) la lista del software autorizzato sulle postazioni non classificate di F.A.
E' fatto assoluto divieto di cercare di forzare con qualsiasi mezzo, l'utilizzo di un software o di una applicazione WEB che è stata esclusa dalla rete MARINA. Il CERT, attraverso opportune tecnologie, potrà provvedere in maniera automatica alla rimozione dei software presenti sulle macchine degli utenti non conformi alle normative vigenti.

E' inoltre vietato utilizzare software che non necessitano di installazione (c.d. Portable).

d. Il CERT CC in collaborazione con il personale del CERT TC, esegue auditing costante sulla rete. Tale attività è svolta sia con sistemi automatici che con tecniche di "penetration test"[14], con lo scopo di verificare la situazione complessiva in atto, implementare nuove policies di sicurezza ed eliminare quelle non più efficaci.

5.5 Uso consentito

L'uso del servizio Internet del Ministero Difesa - Marina è soggetto alle seguenti condizioni:

a. **Proibizioni**. E' fatto divieto a tutti gli utenti di utilizzare il servizio di Internet per inviare messaggi dannosi, di tipo offensivo o sconveniente, come ad esempio, a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di attività e navigazione su Internet che possa arrecare danno alla reputazione del Ministero della Difesa – Marina. E' proibito inoltre fornire a qualsiasi soggetto (estraneo o meno all'Amministrazione M.M.), a sistemi o procedure, le proprie credenziali di accesso alla rete. Nel caso si renda necessario un intervento tecnico

[14] Le attività di penetration test vengono effettuate di massima senza prendere visone dei contenuti informativi dei computer assegnati agli utenti. In relazione alla normativa in vigore e segnatamente ai sensi dell'art. 19 della legge 675/1996, il personale che effettua attività di penetration test (ai fini dell'individuazione delle misure minime di sicurezza per il sistema informatico), è da considerarsi quale "personale incaricato di compiere le operazioni del trattamento dei dati dal titolare o dal responsabile e che operano sotto la loro diretta autorità" e conseguentemente non è necessario il consenso al trattamento dei dati personali da parte degli interessati.

tramite Call Center, gli operatori provvederanno ad autenticare l'interlocutore mediante procedure interne. In nessun caso verrà richiesto via e-mail di fornire al Call Center le proprie credenziali di accesso alla rete. Chiunque riceva comunicazioni della natura sopra indicata dovrà segnalarlo al CERT TC (cert@marina.difesa.it) e per conoscenza CERT CC presso lo Stato Maggiore Marina – Agenzia di Sicurezza – 6° Ufficio Sicurezza Cibernetica, Informatica e delle Comunicazioni (cyber.defence@marina.difesa.it).

b. **Uso Personale**. E' consentito l'utilizzo del servizio Internet a fini privati e personali, purché, in aggiunta a quanto indicato nei punti precedenti, tale utilizzo non sia causa, diretta o indiretta di disservizi dei sistemi elaborativi dell'Amministrazione.

   Tale uso è comunque limitato a quelle attività atte a facilitare l'utente nell'espletamento di pratiche che lo strumento informatico può innegabilmente velocizzare (pagamento di bollettini, iscrizione a servizi pubblici, consultazione di servizi previdenziali on-line, etc).

   Si rammenta comunque che tale uso deve essere limitato al minimo indispensabile e comunque nei limiti del rispetto di criteri di buon senso, onde non contravvenire alle disposizione dell'Art. 314 c.p. (peculato d'uso) il quale, oltre a tutelare il patrimonio della pubblica amministrazione, mira ad assicurare anche il corretto andamento degli uffici sulla base di un rapporto di fiducia e di lealtà con il personale dipendente e l'art. 1223 c.c. (lucro cessante) che si riferisce espressamente al tempo sottratto dal dipendente al lavoro per effettuare attività private. Il tempo massimo che comunque il dipendente non deve mai superare nell'utilizzo del servizio internet per scopi non strettamente correlati all'attività lavorativa è fissato al **10** % dell'orario lavorativo. Qualora l'utente ecceda tale limite l'Amministrazione provvederà ad informare singolarmente l' utente e nel caso i comportamenti dovessero reiterarsi, l'Amministrazione si riserva la facoltà di sospendere/revocare l'accesso ad internet.

c. **WI-FI**. Il Ministero della Difesa – Marina conscio del continuo sviluppo tecnologico e consapevole delle sempre maggiori necessità che tale sviluppo comporta, sta effettuando specifiche attività finalizzate a garantire una maggiore efficacia nella fruizione dei servizi presenti sulla rete. A tal fine saranno disponibili a breve tecnologie WI-FI su Marintranet, da utilizzarsi in modalità, tali da non arrecare problematiche di sicurezza sulla intera infostruttura. Appena tale capacità WI-FI sarà resa disponibile, sarà possibile accedere ad Internet da dispositivi sia personali (Rete Guest) che di servizio (Rete User Marina) secondo modalità e procedure che verranno dettagliate da apposita normativa.

   Nella connessione ad Internet in ambito lavorativo tramite WI-FI valgono le stesse disposizioni relative alla gestione, utilizzo e sicurezza descritte in questo disciplinare (anche nel caso di utilizzo di apparati personali).

   Nel caso in cui invece venga concessa la connessione WI-FI in ambienti non lavorativi (esempio: circoli, alloggi del personale, etc), vengono derogate le disposizioni di cui al punto b. di questo capitolo relative al tempo massimo di utilizzo del servizio internet per usi personali (10%) e della limitazione della navigazione ai soli siti autorizzati in fase di attivazione. Permangono ovviamente tutte le altre disposizioni.

5.6 Sicurezza e riservatezza

a. Oltre a quanto indicato al par. 5.4, gli utenti devono tener presente che, nell'assolvimento dei propri compiti, il personale che gestisce i sistemi di elaborazione e le reti di telecomunicazione può avere, saltuariamente, la necessità di analizzare i dati dei files di log per garantire il corretto funzionamento del servizio e in queste occasioni è possibile che avvengano inavvertitamente accessi al contenuto stesso. Tale personale è tenuto comunque al rispetto di stretti vincoli di riservatezza qualora si verificassero i casi citati e tutte le operazioni effettuate dagli amministratori vengono comunque registrate, come disposto dal Garante della Privacy nelle "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" (G.U. n. 300 del 24.12.2008).

a. il Ministero della Difesa - Marina si pone come obiettivo fondamentale, la fornitura di servizi telematici sicuri ed affidabili avvalendosi di personale qualificato. Va comunque ricordato, come già detto in precedenza, che la sicurezza e riservatezza della navigazione su Internet non possono essere garantite in ogni circostanza, in particolare per quanto concerne i files e le pagine web scaricate sui Personal Computer. In questo caso è indispensabile che l'utente stesso provveda ad attuare le azioni adeguate a proteggere tali informazioni usando tutti i mezzi disponibili, quali ad esempio password di accesso alle applicazioni ed alla propria postazione di lavoro e di bloccare (log-off) la propria postazione prima di allontanarsi dalla stessa.

5.7 Violazioni

Il personale che contravviene alle norme indicate nella presente direttiva di sicurezza, stanti le responsabilità individuali di tipo civile e penale verso terze parti offese, potrà essere oggetto nei limiti previsti dalla legge, di azioni di accertamento delle responsabilità ed, eventualmente, delle conseguenti sanzioni.

In Appendice 3 è riportata una tabella di riferimento circa le eventuali sanzioni comminabili in funzione alla violazione commessa.

Laddove si accerti una qualsiasi violazione al presente disciplinare, sarà valutata dal Ministero della Difesa – Marina la sospensione o la revoca del servizio stesso con segnalazione alla persona ed al Comando/Ente di appartenenza.

6. Responsabilità del Titolare del Comando/Ente

Il Titolare del Comando/Ente è tenuto a definire con apposito Ordine del Giorno il personale dipendente autorizzato ad utilizzare i servizi Internet.

E' responsabilità del Titolare del Comando/Ente accertarsi che l'utente, prima di essere autorizzato ad usufruire di tali servizi, abbia preso conoscenza della presente disciplinare di sicurezza, sia stato indottrinato sull'uso della rete e abbia sottoscritto la "liberatoria per uso del servizio Internet" con le modalità tecniche dettagliate da apposite disposizioni.

Nella procedura di abilitazione (Attuabile dallo stesso Titolare o suo Delegato tramite apposito sistema informatico) devono essere dettagliate le finalità dell'abilitazione stessa e la tipologia di siti web che l'utente può utilizzare per il raggiungimento dell'obiettivo.

Il Ministero della Difesa - Marina, dopo aver effettuato le opportune verifiche, potrà in ogni caso entrare nel merito della tipologia dei siti web autorizzati.

Qualora, a seguito di personale valutazione, venga a mancare la necessità di accesso ad Internet relativamente ad utenza precedentemente abilitata, il Titolare del Comando/Ente è tenuto a disabilitare immediatamente l'abilitazione.

Si rammenta infine, che, per ovvi motivi di sicurezza, è responsabilità del Titolare del Comando/Ente assicurarsi che l'accesso alla rete Marintranet da parte dei propri utenti, avvenga esclusivamente tramite dispositivi proprietari della F.A. e che non venga pertanto impiegato materiale informatico e/o modalità d'impiego non espressamente previste/autorizzate dalla stessa (access point, modalità wireless, varianti configurazioni switch e router, ecc.).

7. Misure di tipo organizzativo

In relazione all'adozione delle misure di tipo organizzativo di cui al punto 5.2. del Provvedimento (per le finalità segnatamente indicate alla lettera b) delle conclusioni del Provvedimento stesso) il Ministero della Difesa – Marina, tramite il proprio referente responsabile della gestione dei sistemi Informatici di F.A. Maritele Roma, ha provveduto ad un'attenta valutazione dell'impatto dei controlli implementati sui diritti degli utenti riguardo le procedure attuate. Sul punto specifico, per ciò che riguarda le tipologie di utenti cui è accordato l'utilizzo della Posta elettronica e l'accesso a Internet, si rinvia alle politiche sopra riportate.

In riferimento a quanto prescritto dal Provvedimento circa l'individuazione dell'ubicazione riservata alle postazioni di lavoro, al fine di ridurre il rischio di impieghi abusivi, si specifica che ogni dipendente riceve indicazione della postazione di lavoro a lui assegnata al momento dell'incarico, ovvero in caso di cambiamento della propria posizione. L'accesso a tali postazioni è protetto tramite sistema di autenticazione che richiede l'immissione di un apposito codice utente e della relativa password.

8. Misure di tipo tecnologico

Con riguardo alla navigazione in Internet, il Centro Telecomunicazioni ed Informatica della M.M. di Roma (Maritele Roma), al fine di ridurre il rischio di usi impropri della "navigazione" (ovvero quegli usi consistenti in attività non correlate alla prestazione lavorativa quali, a titolo esemplificativo, la visione di siti non pertinenti, l'upload o il download di file, l'uso di servizi di rete con finalità ludiche o, comunque, estranee alle proprie mansioni), adotta le seguenti misure tese a limitare nel maggior grado possibile controlli successivi che, in relazione ai dati personali che ne sono oggetto, potrebbero determinare il trattamento di informazioni personali, anche non pertinenti o idonee a rivelare convinzioni religiose, filosofiche o di altro genere, opinioni politiche, lo stato di salute o la vita sessuale (art. 8 l. n. 300/1970; artt. 26 e 113 del Codice; Provv. del Garante Privacy del 2 Febbraio 2006).

In particolare, sono state realizzate attività finalizzate:

- all'individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- alla predisposizione di liste di siti indesiderati (c.d. black list);
- alla configurazione di sistemi o utilizzo di filtri che prevengono determinate operazioni non correlate all'attività lavorativa (quali a titolo esemplificativo e non esaustivo: l'upload, l'accesso ai siti inseriti nella black list, il download di file o software aventi particolari caratteristiche dimensionali o di tipologia di dato);

- al trattamento di dati in forma anonima;
- alla conservazione nel tempo dei dati per il periodo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza ovvero in adempimento di obblighi previsti dalla legge.

9. Trattamenti esclusi

Il Centro Telecomunicazioni ed Informatica della M.M. di Roma (Maritele Roma) non effettua controlli prolungati, costanti o indiscriminati dell'uso di Internet e Posta elettronica da parte degli utenti.

Il Centro Telecomunicazioni ed Informatica della M.M. di Roma (Maritele Roma) non effettua, in nessun modo ed in nessun caso, trattamenti di dati personali mediante sistemi hardware e software che mirano al controllo a distanza degli utenti e che possano essere svolti tramite i seguenti mezzi:

- lettura e registrazione sistematica dei messaggi di posta elettronica degli utenti ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per fornire il servizio di Posta elettronica;
- riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dall'utente;
- lettura e registrazione dei caratteri inseriti dall'utente tramite la tastiera ovvero dispositivi analoghi a quello descritto;
- analisi occulta dei dispositivi per l'accesso ad Internet o l'uso della Posta elettronica messi a disposizione degli utenti.

10. Titolare del Trattamento dei dati

Il titolare del trattamento dei dati personali per tutto il personale MM (sia civile che militare) che insistono sull'infrastruttura di rete è identificato con il Direttore del Centro Telecomunicazioni ed Informatica della M.M. di Roma (Maritele Roma) che a sua volta designerà i responsabili del trattamento e gli incaricati, con apposito documento interno.

11. Monitoraggio e controlli

Il Ministero della Difesa - Marina si avvale di sistemi di controllo che hanno la finalità di acquisire informazioni statistiche sull'uso dei servizi telematici e garantire inoltre la sicurezza nel trattamento dei dati e nell'uso della dotazione informatica e pertanto, non mirano ad un controllo a distanza degli utenti.

Le attività sull'uso del servizio di accesso ad internet vengono automaticamente registrate in forma elettronica nel rispetto delle disposizioni di legge in materia e automaticamente cancellate dopo 12 mesi.

Il trattamento dei dati contenuti nei LOG può avvenire esclusivamente in forma anonima in modo tale da precludere l'identificazione degli utenti e/o delle loro attività.

I dati anonimi aggregati, riferibili all'intera struttura o a sue aree, sono mantenute presso il Centro Telecomunicazioni ed Informatica della M.M. di Roma (Maritele Roma) per i successivi 12 mesi e riguardano:

- per ciascun sito/dominio visitato le seguenti informazioni: il numero di utenti che lo visitano, il numero delle relative pagine richieste e della quantità di dati scaricati;
- I predetti controlli si svolgono nelle seguenti modalità in forma graduata:

a. In caso di mirata segnalazione il Centro Telecomunicazioni ed Informatica della M.M. di Roma (Maritele Roma) provvederà ad eseguire dei controlli su dati aggregati, riferiti all'intera struttura di Marintranet, ovvero a sue aree e dunque ad un controllo anonimo che si concluderà con un avviso generalizzato inerente l'eventuale utilizzo anomalo degli strumenti informatici.
b. In assenza di successive anomalie non si effettueranno controlli su base individuale;
c. Nel perdurare delle anomalie segnalate si procederà a controlli su base individuale o per postazioni di lavoro.
d. In caso di abusi singoli e reiterati si procederà all'invio di avvisi individuali (e per informazione il Comando/Ente di appartenenza) e si eseguiranno controlli nominativi o su singoli dispositivi e/o postazioni di lavoro

- Fermo restando quanto specificato nei punti precedenti, il Ministero della Difesa – Marina, tramite i preposti organi di controllo, effettuerà verifiche sull'aderenza della navigazione internet (dato aggregato) in relazione all'autorizzazione ricevuta all'atto dell'abilitazione.

In caso di riscontrato uso non conforme da parte di un utente delle risorse informatiche, il Ministero della Difesa – Marina valuterà la sospensione o la revoca del servizio stesso dandone conoscenza al Comando/Ente dell'utente per le conseguenti sanzioni.

In appendice al presente documento è riportato un vademecum non esaustivo relativo all'impiego dei servizi telematici e di posta elettronica.

12. Incidenti informatici

Si definisce *"Incidente Informatico"* :

"un evento che abbia come conseguenza l'alterazione del normale funzionamento (in senso strettamente tecnologico oppure di corretto uso) dei servizi erogati sulla rete della Difesa / Marina".

Qualora un utente abbia il sospetto che il suo sistema informatico (PC, server, apparato di rete, sistema di videoconferenza, etc.) possa essere oggetto di un incidente informatico deve :

- Scollegare immediatamente l'apparato dalla rete (dove fattibile);
- NON spegnere l'apparato;
- Avvisare immediatamente l' Ufficiale alla Sicurezza EAD / responsabile informatico del Comando/Ente;
- Aprire un Ticket presso il Call Center M.M. , con l'ausilio dell'Ufficiale alla Sicurezza EAD / responsabile informatico in maniera tale da poter fornire dettagliate informazione tecniche. Il Ticket può essere aperto telefonicamente (al num. 71-44444 o 06-36804444) o via web (https://callcenter.marina.difesa.it).
- Attendere di essere ricontattati dal personale preposto.

In caso di dubbi e per fornire informazioni riguardo problematiche di natura Cyber Defence, come ad esempio :

- Segnalare un sito malevolo;
- Segnalare un indirizzo e-mail che effettua SPAM sulla rete;
- Segnalare l'uso improprio di servizi internet / e-mail

scrivere un'e-mail all'indirizzo cert@marina.difesa.it (CERT Marina) info cyber.defence@marina.difesa.it (MARISTAT OCS – Sez. Cyber Defence).

13. Conclusioni

Il presente disciplinare viene, oltre ad essere sottoscritto dal singolo dipendente al momento dell'attivazione della propria utenza e postazione, pubblicato sul sito Intranet della Marina Militare e si ritiene conosciuto da tutto il personale militare e civile della Difesa a far data dalla predetta pubblicazione.
Il militare/dipendente civile dell'A.D. dovrà attenersi, nell'utilizzo e nella gestione delle risorse strumentali informatiche alle norme ed ai principi del presente disciplinare ed ai doveri stabiliti dalla normativa indicata nei riferimenti.
I comportamenti posti in essere da parte dei dipendenti o dagli addetti ai sistemi di manutenzione informatica, non conformi ai principi ed alle norme contenute nel presente disciplinare costituiranno violazione degli obblighi e dei doveri del militare e/o dipendente pubblico e, pertanto, in relazione alla gravità dell'infrazione, l'autorità a cui spetta la potestà sanzionatoria (dirigenti/Comandanti di Corpo) potrà:

- disattivare, in via cautelare o definitiva, i servizi internet;
- irrogare l'eventuale sanzione disciplinare di corpo;
- segnalare l'eventuale mancanza all'Autorità competente a disporre l'apertura di un'inchiesta formale per l'irrogazione di una sanzione disciplinare di stato;
- segnalare l'evento alla Procura della Repubblica e/o alla Corte dei Conti.

In particolare, come definito anche dalle Linee Giuda del Garante, si ribadisce che nell'ambito del presente disciplinare, sarà sempre garantito il rispetto della libertà e la dignità dei lavoratori in particolar modo per ciò che attiene al divieto di installare "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (art. 4, primo comma, L. n. 300/70), tra cui sono certamente comprese strumentazioni hardware e software mirate al controllo dell'utente di un sistema di comunicazione elettronica.

14. Riferimenti

a. S.M.M. 57/R – Vol. II ;
b. Circolare SMM 1091 – Edizione 1993;
c. Decreto Legislativo 27 ottobre 2009 n. 150;
d. Decreto Legislativo 15 marzo 2010 n. 66;
e. Decreto del Presidente della Repubblica 15 marzo 2010 n. 90
f. Legge 20 maggio 1970, n. 300 – Art. 8 ;
g. Garante privacy - Parere 8/2001 sul trattamento di dati personali nell'ambito dei rapporti di lavoro – adottato il 13 settembre 2001;

h. Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali;
i. Provvedimento del Garante della privacy del 2 febbraio 2006 – "Internet: proporzionalità nei controlli effettuati dal datore di lavoro";
j. Provvedimento generale del Garante della privacy n° 13 del 1 marzo 2007 (G.U. – Serie Generale n° 58 del 10 marzo 2007;
k. Provvedimento generale del Garante della privacy del 17 gennaio 2008 – Sicurezza dei dati di traffico telefonico e telematico (G.U. n° 30 del 5 febbraio 2008);
l. Provvedimento generale del Garante della privacy del 24 luglio 2008 – Recepimento normativo in tema di dati di traffico telefonico e telematico (G.U. n° 189 del 13 agosto 2008);
m. Provvedimento generale del Garante della privacy del 27 novembre 2008 – Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema (G.U. n° 300 del 24 dicembre 2008);
n. Decreto legislativo n° 82 del 7 marzo 2005 "Codice dell'Amministrazione digitale" – (modificato con D.Lgs. n.83 del 22/06/2012 e D.Lgs. n. 95 del 6/7/2012));
o. Art. 314 - Codice Penale Libro 2 Titolo II "Dei delitti contro la pubblica amministrazione";
p. Direttiva nr. 02/09 del 26.05.2009 – Presidenza del Consiglio dei Ministri – Dipartimento della Funzione Pubblica;
q. SMD – I - 013 "Procedure di risposta agli incidenti informatici riguardanti le reti telematiche della Difesa" – Ed. 2008

Appendice 1 – Modulo di richiesta accesso Internet e assunzione di responsabilità

MODULO DI RICHIESTA ACCESSO INTERNET E ASSUNZIONE DI RESPONSABILITA'

Io sottoscritto, …….. in servizio preso ……..……
(grado/qualifica cognome e nome)

assegnatario della casella di posta elettronica :…….

chiede :

l'abilitazione al servizio Internet erogato sulla rete non classificata di Forza Armata (MARINTRANET) per la seguente motivazione:

……
……

dichiara di essere a conoscenza che :

a) il PC eventualmente affidatogli dall'Amministrazione Marina deve essere utilizzato esclusivamente per adempiere alle sole esigenze d'istituto a lui demandate.
b) La possibilità d'uso di Internet (ove prevista e concessa) è consentita unicamente per incrementare l'efficienza e la produttività del proprio lavoro ed è limitata alla sola tipologia di siti web definiti dal Comando/Ente all'atto dell'attivazione, come stabilito ;
c) la navigazione Internet ad uso non strettamente collegato ai fini lavorativi (pagamenti on-line, visualizzazione servizi previdenziali on-line, etc.) non può in ogni caso superare il 10% della giornata lavorativa;
d) il Ministero della Difesa - Marina, può in ogni momento verificare il corretto impiego dello strumento Internet secondo quanto dichiarato dal Comando/Ente in fase di attivazione del servizio;
e) l'user-ID assegnato e la password di accesso devono essere custoditi e mantenuti strettamente riservati e non devono essere condivisi con altri utenti;
f) l'abilitazione dovrà essere rinnovata ad ogni cambio incarico/trasferimento e almeno ogni cinque anni; contestualmente dovranno essere accettate nuovamente le presenti "condizioni di utilizzo" mediante procedure possibilmente informatiche e dettagliate da apposite disposizioni;
g) non è consentito detenere dati personali sul PC in questione in quanto per motivi di sicurezza (ad esempio infezione da Virus), può esserne richiesta l'immediata riconsegna, senza la possibilità quindi di salvare i propri dati laddove presenti;
h) al fine di garantire un elevato livello di sicurezza, sulla rete agiscono sistemi di firewall, IDS, IPS, Url filtering, web security e di filtraggio della posta indesiderata (firewall-antispam) che analizzano in modo autonomo ed automatico il traffico Internet e della posta elettronica;
i) deve dare comunicazione immediata al MARITELE ROMA (tramite procedura GEIRMM) dell'eventuale perdita di riservatezza della password e al titolare del Comando/Ente;
j) è vietato immettere, trasmettere, diffondere qualsiasi materiale che non può essere distribuito legalmente via rete telematica;
k) è vietato modificare la configurazione del PC eventualmente in dotazione. Nel caso in cui si presentasse l'esigenza di utilizzare nuovo software, ciò può avvenire solo previa autorizzazione del proprio Capo Ufficio/Servizio, che ne valuterà l'effettiva necessità. Se autorizzata, l'installazione verrà effettuata dal responsabile informatico del Comando / Ente;
l) le disposizioni legislative sulla tutela giuridica del software considerano i programmi per elaboratore alla stregua di opere letterarie protette dalle vigenti leggi in materia;

m) la riproduzione permanente/temporanea, totale/parziale di software acquisito dal commercio o prodotto dall'Amministrazione deve essere autorizzata dai titolari dei diritti di proprietà sullo stesso;

n) chiunque abusivamente duplica software per uso su elaboratori o sapendo o, avendo motivo di sapere, che si tratta di copie non autorizzate, lo distribuisce, lo vende, lo detiene a scopi commerciali/personali, è soggetto alla pena prevista dalla vigente legislazione che comporta reclusione e sanzioni economiche. Alla stessa pena è soggetto chi mette in atto sistemi tendenti a facilitare la rimozione arbitraria e l'elusione funzionale dei dispositivi applicati a protezione dei software per uso su elaboratori;

o) lo scarico dalla rete (download) di opere protette dal copyright (musiche, filmati, programmi etc. etc.) non è consentito a nessun titolo ed è soggetto a sanzione in conformità dalle vigenti normative;

p) la detenzione sul proprio elaboratore di contenuti pedo-pornografici è vietata e soggetta a sanzione in conformità alle vigenti leggi;

q) non sono consentite azioni tendenti a nascondere la propria identità, a molestare o arrecare danno sull'attività degli elaboratori di altri utenti o ad acquisire dati/informazioni/privilegi a cui non si ha diritto.

r) l'Amministrazione effettua controlli sulla rete atti a verificarne i flussi, in maniera tale da prevenire o individuare anomalie sia di natura tecnica che di natura malevola, inoltre controlla che sulle postazioni utente siano presenti solo i software espressamente autorizzati.
Il CERT CC ubicato presso l'Agenzia di Sicurezza – Sez. Cyber Defence stila periodicamente una lista di software o di applicazioni web che per ragioni di Sicurezza o per il non necessario impiego da parte degli utenti della F.A. verranno esclusi dalla rete e quindi non potranno essere utilizzati/installati. La lista completa di tali software sarà pubblicata sul portale MARINTRANET nella pagina del CERT CC.
E' fatto assoluto divieto cercare di forzare con qualsiasi mezzo, l'utilizzo di un software o di una applicazione WEB che è stata esclusa dalla rete MARINA. Il CERT, attraverso opportune tecnologie, potrà provvedere in maniera automatica alla rimozione dei software presenti sulle macchine degli utenti non conformi alle normative vigenti.

s) E' inoltre vietato utilizzare software che non necessitano di installazione (c.d. Portable).

t) Il CERT CC in collaborazione con il personale del CERT TC, esegue auditing costante sulla rete (sia con sistemi automatici che con tecniche di "penetration test") allo scopo di valutare la situazione complessiva in atto al fine implementare nuove policies di sicurezza ed eliminare quelle non più efficaci.

u) L'amministrazione si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali al fine di verificare che la tipologia dei siti visitati non comporti malfunzionamenti della RETE MARINTRANET dovuti a software malevoli (virus, malware, trojan ecc.). Nel caso di riscontro di navigazioni verso siti internet illeciti, l'amministrazione provvederà ad informare singolarmente gli utenti e nel caso i comportamenti dovessero reiterarsi, l'amministrazione si riserva la facoltà di procedere nei confronti dell'utente a norma di legge.

Conferisce

il proprio consenso all'attività di verifica che l'Amministrazione si riserva di effettuare sulle attività di "navigazione" in Internet, al fine di verificare che le attività effettuate dal sottoscritto sono strettamente riconducibili nell'ambito dell'attività di Ufficio e non possano arrecare danni all'infrastruttura informatica della Marina Militare.

Si impegna inoltre a:

- rispettare le suddette norme;
- segnalare tempestivamente ai responsabili alla sicurezza ogni ipotesi di compromissione/infrazione anche accidentale delle suddette norme.

Qualsiasi inadempienza a quanto dichiarato nel presente documento provocherà l'immediata sospensione del servizio rete Internet (ove concesso). Il Ministero della Difesa - Marina può interrompere il servizio prestato al sottoscritto anche solo per palese impiego non in linea con i fini istituzionali.

Dichiaro altresì di aver interamente letto e compreso il ***"Disciplinare interno per l'utilizzo dei servizi Non Classificati di posta elettronica e accesso ad internet"***

I dati di questo modulo saranno utilizzati dal Ministero della Difesa - Marina, titolare del trattamento degli stessi, nel rispetto del D.Lgs. 196 in data 30/06/2003.

(Documento firmato elettronicamente ai sensi del C.A.D.)

Data : _____

Appendice 1 – Modulo di richiesta accesso Internet e assunzione di responsabilità

MODULO DI ASSUNZIONE DI RESPONSABILITA' SERVIZIO E-MAIL

Con il presente modulo d'assunzione di responsabilità il sottoscritto:

…….. in servizio preso ……..……

(grado/qualifica cognome e nome)

Codice Fiscale : ……

dichiara di essere a conoscenza che :

a) l'indirizzo di posta elettronica (e-mail) assegnatogli, ancorché nella forma nome.cognome@marina.difesa.it, non ha caratteristiche di privatezza ma costituisce normale strumento di lavoro e ne è vietato l'utilizzo per scopi non strettamente connessi con l'attività lavorativa. L'assegnatario è tenuto ad informare di tale caratteristica i terzi a cui comunica il citato indirizzo e-mail;
b) Qual'ora al proprio indirizzo di posta elettronica nominativo vengano associati anche altri tipi di indirizzi previsti dall'infrastruttura Marina (PEI, Funzionali), quest'ultimi non godono dei principi di riservatezza comunque garantiti della casella di posta nominativa;
c) l'utilizzo del servizio Push-Mail per la lettura e la gestione della casella di posta elettronica sottopone la casella stessa ad un sensibile abbassamento del livello di sicurezza;
d) al fine di garantire un elevato livello di sicurezza, sulla rete agiscono sistemi di firewall, IDS, IPS, Url filtering e di filtraggio della posta indesiderata (firewall-antispam) che analizzano in modo autonomo ed automatico il traffico Internet e della posta elettronica;
e) deve dare comunicazione immediata al MARITELE ROMA (tramite procedura GEIRMM) dell'eventuale perdita di riservatezza della password e al titolare del Comando/Ente;
f) è vietato immettere, trasmettere, diffondere qualsiasi materiale che non può essere distribuito legalmente via rete telematica;
g) la detenzione sulla propria e-mail di contenuti pedo-pornografici è vietata e soggetta a sanzione in conformità alle vigenti leggi;
h) non sono consentite azioni tendenti a nascondere la propria identità, a molestare o arrecare danno sull'attività di altri utenti;
i) Il CERT CC in collaborazione con il personale del CERT TC, esegue auditing costante sulla rete allo scopo di valutare la situazione complessiva in atto al fine implementare nuove policies di sicurezza ed eliminare quelle non più efficaci.

Qualsiasi inadempienza a quanto dichiarato nel presente documento provocherà l'immediata sospensione della casella e-mail. Il Ministero Lo Stato Maggiore della Marina può interrompere il servizio prestato al sottoscritto anche solo per palese impiego non in linea con i fini istituzionali.

Dichiaro altresì di aver interamente letto e compreso il ***"Disciplinare interno per l'utilizzo dei servizi Non Classificati di posta elettronica e accesso ad internet"***

I dati di questo modulo saranno utilizzati dallo Stato Maggiore Marina, titolare del trattamento degli stessi, nel rispetto del D.Lgs. 196 in data 30/06/2003.

(Documento firmato elettronicamente ai sensi del C.A.D.)

Data : _____

_____

VADEMECUM PER L'UTENTE DI SERVIZI INFORMATICI DELL'AMMINISTRAZIONE

1. non può in alcun caso visitare siti e/o memorizzare file che abbiano un contenuto contrario a norme di legge, all'ordine pubblico o al buon costume;
2. deve porre la massima attenzione al fine di evitare che il sistema informatico dell' amministrazione venga attaccato da programmi idonei (o potenzialmente idonei) a danneggiarlo (es. virus, trojan horses, etc.);
3. non può utilizzare la connessione fornita dall'Amministrazione per effettuare attività che possano provocare malfunzionamenti, causare la riduzione di efficienza del servizio o arrecare danni, ad altri utenti e/o a terzi;
4. non può installare software non necessari ai fini della prestazione lavorativa e programmi, di qualsiasi genere, senza la preventiva autorizzazione;
5. non può utilizzare software o altri strumenti per la condivisione (ad es. Peer-To-Peer) di file al di fuori di finalità esclusivamente di ufficio;
6. non può scaricare né produrre copie di software e/o file protetti da licenza d'uso;
7. non può modificare i parametri di configurazione forniti dal sistema di gestione per la navigazione internet, né aggirare o tentare di disabilitare i sistemi posti in essere dall'Amministrazione per bloccare l'accesso ad alcuni siti;
8. non può utilizzare modem/chiavette internet/ sistemi wi-fi per effettuare connessioni ad internet o ad altre reti informatiche esterne, da postazioni collegate alla rete di F.A., se non in casi autorizzati;

VADEMECUM PER L'IMPIEGO DEL SERVIZIO DI POSTA ELETTRONICA DELL'AMMINISTRAZIONE

1. in considerazione del fatto che la "posta esterna" può essere da chiunque intercettata, non può diffondere notizie a carattere riservato/sensibile , né inviare documenti di lavoro ad indirizzi di posta elettronica esterni alla rete informatica dell'AD, se non necessario per l'attività lavorativa;
2. non può inviare o memorizzare messaggi (e-mail o altra forma di messaggistica) o allegati a contenuto contrario a norme di legge, all'ordine pubblico o al buon costume;
3. non può inviare materiale protetto da copyright senza le necessarie preventive autorizzazioni;
4. nell'invio di e-mail deve verificare che i documenti elettronici non contengano testi o immagini nascoste, ed ogni altro elemento che consenta di ottenere informazioni diverse da quelle che si intende diffondere;
5. non può modificare i parametri di configurazione forniti dal sistema per l'utilizzo della posta elettronica;
6. non può utilizzare l'indirizzo di posta elettronica dell'AD per partecipare a richieste, petizioni o ad altre forme di mailing di massa non istituzionali;
7. non può utilizzare l'indirizzo di posta elettronica istituzionale per inviare (sia all'interno che all'esterno dell'Amministrazione) messaggi pubblicitari o promozionali, a meno che ciò non rientri nello svolgimento delle proprie mansioni o, comunque, messaggi che possano arrecare danno o intralciare l'utilizzo della posta elettronica da parte dei destinatari degli stessi o causare la riduzione di efficienza del servizio;
8. non può utilizzare la posta elettronica istituzionale per le iscrizioni a siti internet, social forum, blog ed altro, a meno che ciò non rientri nelle proprie mansioni.

Tipizzazione condotte disciplinarmente rilevanti
Accesso con credenziali di altri utenti
Installazione software non autorizzato
Possedere i diritti di Amministrazione della postazione senza autorizzazione
Accesso ad Internet attraverso connessioni non previste
Registrazione su social network o siti non attinenti al servizio, utilizzando la casella di posta personale (@marina.difesa.it)
Divulgazione di informazioni Non Classificate Controllate in rete
Divulgazione delle proprie credenziali
Sincronizzazione dati PC Utente con Share Pubblici (DropBox, OneDrive, etc) o privati
Scansioni non autorizzate (host, port, vulnerability, ping, traceroutes, DNS zone transfer, OS fingerprinting, banner grabbing) sulle reti istituzionali
Sniffing di rete (cattura di traffico di rete non diretto all'utente stesso)
Utilizzo di software (crack) in grado di alterare la licenza di software coperto da copyright
Diffusione di email cosiddette "catene di S.Antonio"
Download di materiale protetto da copyright (films, musica, libri ecc.)
Manomissione hardware
Utilizzo di USB, hard disk ed altri sistemi di storage non autorizzati
Manomissione configurazione client (cambio di proxy, dns, parametri di rete)
Dual boot con sistemi non autorizzati (Windows/Linux)
Manomissione del BIOS
Boot da CD/USB o comunque da altro dispositivo diverso da quello prescritto
Connessione in rete di un qualsiasi dispositivo personale, se non diversamente specificato (laptop/pc/telefono/tablet ecc.)
Disattivazione antivirus e altri sistemi di sicurezza (Endpoint Firewall, DLP ecc.)
Creazione di VPN personali tra PC Marintranet e risorse personali non dell'amministrazione
Accesso a sistemi di rete non autorizzati (Server, Switch, Data Base, etc)
Superamento del limite giornaliero di navigazione consentito per scopi personali

Note:

Obiettivo del presente disciplinare è tutelare e proteggere la rete informatica della Marina Militare, a tal proposito sono state di massima tipizzate le suddette condotte che, in concreto verranno valutate disciplinarmente dall'Autorità Competente alla luce delle necessità connesse alla specificità ed alle esigenze correlate all'attività lavorativa prestata dal dipendete civile/ militare nell'ambito dell'A.D.

In tutti i casi in cui la condotta posta in essere dagli utenti integri gli estremi di un reato ai

sensi dell'art. 347 c.p.p. il Titolare del Comando / Ente provvederà a dare notizia all'Autorità Giudiziaria.