Marsh S.p.A. - Marsh Risk Consulting Services S.r.l.

Procedura per l'uso dell'informatica aziendale

(Personal computer e altri dispositivi elettronici aziendali, internet e posta elettronica)

Doc. Id.:		**N. pagine:**	17
Redatto da:	HR	Maddalena Rigo	**Il:** 01/07/2013
	Legal	Lara Didolani	
	Operations	Alessandro Crivelli	
	MGTI	Massimo Fiammeni	
Approvato da:	Amministratore Delegato	Flavio Piccolomini	**Il:** 01/07/2013
	Marsh S.p.A.	Giovanni Turci	
	Presidente Marsh S.p.A.		

STORIA DELLE MODIFICHE		
Versione Modificata		**Descrizione modificata**
1.00	24/07/08	Nuova emissione
2.00	01/07/2013	Modifica

Indice

1

Introduzione

1.1 Obiettivo

La presente procedura definisce le modalità di accesso e di uso corretto dei PERSONAL COMPUTER (d'ora innanzi, "PC"), BlackBerry e di altri dispositivi elettronici aziendali nonché di Internet e della posta elettronica utilizzati dai dipendenti per lo svolgimento delle mansioni assegnate. Un uso dei PC (inclusi portatili e BlackBerry) e di altri dispositivi elettronici nonché dei servizi di Internet e della posta elettronica, difforme dalle regole contenute nella presente procedura potrebbe esporre Marsh S.p.A., Marsh Risk Consulting Services S.r.l. (di seguito, in generale, la SOCIETA') ad aumentare la minaccia di accessi non autorizzati al sistema informatico aziendale, a furti o divulgazioni di informazioni riservate, nonché a furti o danneggiamenti del sistema informatico della SOCIETA' e/o malfunzionamenti in generale dell'intero sistema informatico.

La presente procedura viene consegnata ai dipendenti anche ai fini e per gli effetti previsti dall'art. 13 del D. Lgs. 196/2003 ("Codice Privacy").

1.2 Definizioni

TECNOLOGIA DELLA SOCIETA': la tecnologia della società comprende, in via esemplificativa e non esaustiva:

- l'hardware di elaborazione della SOCIETÀ (mainframe, servers, Pc desktop e laptop);
- il software (applicazioni che supportano i flussi di lavoro, i sistemi operativi, i software di utilità);
- reti e applicazioni di rete (PDA, sistemi telefonici, VoiceMail, posta elettronica, fax);
- i servers di collegamento alle borse per la ricerca dei dati di mercato e l'invio degli ordini.

PC: il sistema informatico consegnato al dipendente, incluse le periferiche, gli accessori ed il SOFTWARE.

SOFTWARE: applicativo utilizzato dal PC che ne consenta il funzionamento e/o l'elaborazione delle informazioni o lo svolgimento di specifici compiti o funzioni, o che sia necessario per aumentare o diminuire la funzionalità di altri applicativi o del sistema operativo stesso.

FILE: qualunque tipo di documento elettronico, in qualsiasi formato, contenente dati, testo, immagini, suoni o un insieme degli stessi.

INTERNET: la rete informatica che consente, a livello mondiale, il collegamento e lo scambio di informazioni tra PC.

POSTA ELETTRONICA: SOFTWARE che consente l'invio di messaggi (e-mail) e documenti elettronici da un PC ad un altro, utilizzando INTERNET.

LOGIN: identificazione dell'utente.

PASSWORD: il codice segreto individuale che permette l'autenticazione e l'accesso alla rete, a un PC, o più in generale a un sistema informatico protetto. È severamente vietato divulgare la password individuale a terzi.

DOWNLOAD: l'operazione che permette di trasferire un SOFTWARE o un FILE sul proprio PC prelevandolo dalla rete INTERNET o da altro PC o da un qualsiasi supporto magnetico, ottico o di qualunque altro tipo.

LAN: rete locale.

SERVER: il PC che utilizza SOFTWARE di gestione di altri PC, fornendo ad essi servizi su una rete, e gestione di FILE, stampanti, internet, dati.

CHAT: servizio di conversazione contemporanea tra utenti in tempo reale tramite lo scambio di messaggi di testo su rete locale o su internet.

BACKUP: copia di riserva di dati, di una serie di cartelle, di FILE effettuata su una memoria di massa o su qualsiasi altro supporto diverso dall'originale.

CRACKING PROGRAMS: SOFTWARE idonei a violare le protezioni o le PASSWORDS di altri SOFTWARE.

INTERNET SERVICE PROVIDER: fornitore del servizio di accesso alla rete.

INFORMAZIONI RISERVATE: al fine della presente procedura, per INFORMAZIONI RISERVATE si intendono in via esemplificativa e non esaustiva:

- le informazioni relative ai clienti o fornitori della SOCIETÀ e in particolare ai servizi richiesti da essi alla SOCIETÀ e/o ai documenti finanziari che li riguardino;
- le informazioni relative alle procedure, prodotti, organizzazione, gestione, progetti futuri, organizzazione del personale e documenti di proprietà della SOCIETÀ;
- informazioni relative a tutti i lavoratori autonomi o subordinati o agli amministratori della SOCIETÀ, comprese le informazioni riguardanti la loro retribuzione e il loro preavviso.

IT: dipartimento della SOCIETÀ che si occupa della gestione, amministrazione e funzionamento delle infrastrutture informatiche**.**

CODICE PRIVACY: Decreto Legislativo 30 giugno 2003, n.196 Codice in materia di protezione dei dati personali

BYOD (Bring Your Own Device): programma cui hanno accesso alcuni dipendenti della Società secondo il quale il dipendente utilizza strumenti di sua proprietà (es. smartphone, laptop ecc.) sul quale vengono installati software aziendali che consentono la connessione a Internet e l'accesso alla casella di posta elettronica aziendale.

2

Modalità d'uso

2.1 Composizione del sistema informativo aziendale

Il sistema informativo aziendale è composto da un insieme di unità server centrali e macchine client connessi ad una rete locale (LAN), che utilizzano diversi sistemi operativi e applicativi.

2.2 Casi di esclusione di utilizzo degli strumenti informatici

Hanno diritto all'utilizzo degli strumenti informatici e ai relativi accessi solo i dipendenti che per funzioni lavorative ne abbiano un effettivo e concreto bisogno. Le esclusioni dall'utilizzo degli strumenti informatici sono strettamente connesse alla destinazione aziendale lavorativa degli strumenti stessi nonché al principio di necessità di cui al Codice Privacy.

I casi di esclusione possono riguardare:

- utilizzo del PC
- utilizzo della posta elettronica
- accesso ad internet.

I casi di esclusione saranno comunicati individualmente e potranno riguardare uno o più dei casi sopra descritti.
Tali esclusioni hanno la finalità di ridurre, a titolo cautelativo e preventivo, i pericoli e le minacce esposti nell'introduzione del presente documento, in ottemperanza con quanto previsto dal Provvedimento del Garante 1° marzo 2007 con il quale il datore di lavoro è chiamato ad adottare ogni misura in grado di prevenire il rischio di utilizzi impropri, così da ridurre controlli successivi sui lavoratori.

2.3 Modalità d'utilizzo del PC

Il PC che viene consegnato al dipendente contiene tutti i SOFTWARE necessari a svolgere le mansioni affidate. L'accesso al SOFTWARE installato sul proprio PC è regolato mediante l'inserimento di una PASSWORD. Per ogni necessità aziendale, il dipartimento IT, utilizzando la propria LOGIN con privilegi di Amministratore e la PASSWORD di Amministratore, potrà accedere sia alla memoria di massa locale che al SERVER aziendale nonché, previa comunicazione al dipendente, accedere al PC in remoto.

La PASSWORD posta a protezione del PC è strettamente riservata. In caso di assenza dell'utilizzatore abituale, il superiore gerarchico/responsabile, qualora sia necessario accedere al PC potrà richiedere all'IT - previa autorizzazione dell'HR- di modificare la password ai fini dell'accesso.

Il dipendente ha l'obbligo di utilizzare solo ed esclusivamente le aree di memoria del SERVER denominate «disco X » (individuale) e quelle di gruppo di lavoro, ed ivi creare e registrare FILE o archivi dati.

La SOCIETÀ si riserva il diritto di controllare che nessun FILE o SOFTWARE o archivio dati sia registrato sulla memoria di massa del PC consegnato al dipendente, attraverso periodiche verifiche.

2.4 Comportamenti vietati

Al dipendente non è consentito:

a) registrare alcun FILE o SOFTWARE o archivio dati nel disco fisso o memoria di massa del PC consegnato al dipendente. È consentito utilizzare solo ed esclusivamente le aree di memoria del SERVER denominate «*X* » (individuale) e quelle di gruppo di lavoro, ed ivi registrare FILE o archivio dati.

b) Modificare le configurazioni già impostate sul PC consegnato.

c) Utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta del diretto superiore gerarchico del dipendente e dell' IT.

d) Installare alcun SOFTWARE di cui la SOCIETÀ non possieda la licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul PC (portatile, BlackBerry o altro dispositivo elettronico) consegnato, senza l'espressa autorizzazione dell' IT.

e) Fare copia del SOFTWARE installato al fine di farne un uso personale.

f) Caricare alcun documento, gioco, FILE musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate.

g) Aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, PCMCIA, firewall ecc.) o periferiche (telecamere, macchine fotografiche, chiavi USB, ecc.) diversi da quelli consegnati, senza l'autorizzazione espressa dell' IT.

h) Creare o diffondere programmi idonei a danneggiare il sistema informatico della SOCIETÀ, quali per esempio virus, trojan horses, ecc.

i) Accedere, rivelare, o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte.

Dal momento che la violazione delle regole di cui sopra potrebbe esporre la SOCIETÀ al rischio di danneggiamento del sistema informatico o eventualmente a responsabilità penale in caso di uso di programmi senza licenza, il loro rispetto potrebbe essere oggetto di controllo attraverso periodiche verifiche del contenuto della memoria di massa del PC consegnato al dipendente (si vedano i paragrafi 3.1 e 3.2 della presente procedura).

2.5 Modalità d'utilizzo di INTERNET

La connessione ad INTERNET dai PC aziendali (inclusi portatili e BlackBerry) e tutti gli accessi alla rete INTERNET vengono registrati nel proxy SERVER per motivi di sicurezza ed integrità del sistema informativo aziendale. La connessione ad INTERNET dai PC aziendali (portatili, BlackBerry) è ammessa esclusivamente per motivi attinenti all'attività lavorativa e pertanto ne è vietato l'utilizzo per scopi personali.

2.6 Comportamenti vietati

Al dipendente non è consentito:

a) Accedere a siti dal contenuto non attinente allo svolgimento dell'attività lavorativa e in tutti i casi in cui la navigazione sia idonea a rivelare dati sensibili ai sensi del Codice Privacy.

b) Accedere a siti INTERNET evitando l'azione o comunque superando o tentando di superare o disabilitando i sistemi adottati dalla SOCIETÀ per bloccare l'accesso ad alcuni siti ed in ogni caso utilizzare siti o altri strumenti (es. CRACKING PROGRAMS) che realizzino tale fine.

c) Effettuare il DOWNLOAD di SOFTWARE gratuito (freeware) o messo a disposizione in rete per essere provato (shareware, demo), e comunque il DOWNLOAD di qualsiasi SOFTWARE senza l'espressa autorizzazione dell' IT.

d) Accedere a siti INTERNET che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.

e) Accedere, attraverso le apparecchiature della SOCIETÀ, a qualsivoglia gruppo di discussione o conferenza in rete (CHAT *lines* o altro) o banche dati esterne, con la sola esclusione di quelli espressamente autorizzati.

f) Promuovere utile o guadagno personale.

g) Utilizzare INTERNET in violazione delle norme in vigore dell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, d.lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248).

h) Creare Siti web personali sui sistemi della SOCIETÀ.

i) Collegarsi a siti web al fine di ascoltare musica e/o stazioni radio e/o visionare filmati/video non inerenti l'attività professionale.

Dal momento che la violazione delle summenzionate regole potrebbe esporre la SOCIETÀ al rischio di danneggiamento o mal funzionamento del sistema informatico, il rispetto di tali regole potrà essere oggetto di controllo anche mediante accesso in remoto, attraverso periodiche verifiche del contenuto della memoria di massa del SERVER e del PC consegnato al dipendente (si vedano i paragrafi 3.1 e 3.2 della presente procedura).

2.7 Modalità d'utilizzo della POSTA ELETTRONICA

A ciascun dipendente che ne abbia necessità ai fini dello svolgimento dell'attività lavorativa, è attribuito un indirizzo di posta elettronica aziendale individuale, configurato come segue: nome.cognome@marsh.com

Altresì la Società può predisporre un indirizzo di posta elettronica aziendale condiviso tra più dipendenti appartenenti allo stesso dipartimento.

Utilizzando gli indirizzi di POSTA ELETTRONICA aziendale, il dipendente è a conoscenza e consapevole che:

1. tutti i messaggi in entrata e in uscita dagli indirizzi di POSTA ELETTRONICA aziendale sono di proprietà della SOCIETÀ;
2. il messaggio di POSTA ELETTRONICA aziendale, sia individuale che condiviso si configura come corrispondenza aperta che potrebbe essere letto da chiunque durante il suo percorso sulla rete INTERNET fino al destinatario nonché dagli addetti IT sul SERVER aziendale che gestisce il servizio stesso;
3. l'uso degli indirizzi di POSTA ELETTRONICA aziendale è ammesso esclusivamente per motivi attinenti all'attività lavorativa; l'uso per motivi personali è pertanto espressamente vietato. Nessuna aspettativa di tutela del proprio diritto alla privacy, relativa ai messaggi di POSTA ELETTRONICA in entrata ed in uscita utilizzando l'indirizzo aziendale, potrà, dunque, essere pretesa dal dipendente;
4. il messaggio di POSTA ELETTRONICA potrebbe essere letto da destinatari diversi da quelli a cui era diretto, e ciò potrebbe determinare danni anche gravi alla SOCIETÀ;

5. i falsi o errati messaggi di POSTA ELETTRONICA scritti per conto e nel nome della SOCIETÀ potrebbero essere spediti per errore sia all'interno che all'esterno della SOCIETÀ;
6. i messaggi di POSTA ELETTRONICA spediti potrebbero non essere recapitati, essere distrutti o subire ritardi;
7. le informazioni inviate attraverso la POSTA ELETTRONICA non possono essere fermate o richiamate, una volta che siano state spedite all'esterno della SOCIETÀ;
8. le comunicazioni di POSTA ELETTRONICA sono considerate a tutti gli effetti posta in partenza e pertanto gli utenti dovranno verificare quanto scritto per ottenere la firma di persone autorizzate ad impegnare la SOCIETÀ;
9. in caso di assenza programmata dal lavoro (ad es. ferie, attività di lavoro fuori ufficio, etc.), il dipendente ha l'obbligo di attivare il servizio di risposta automatica (*Out of office*), seguendo le istruzioni ricevute dall' IT, utilizzando il messaggio concordato con il proprio superiore gerarchico. Per effettive ragioni di continuità dell'attività lavorativa, in caso di prolungata assenza dal lavoro, sia essa programmata o non prevista, il dipendente che non abbia conferito l'accesso al proprio account di posta elettronica ad apposito delegato deve comunicare, a richiesta del Responsabile IT e/o del Direttore del Personale o di loro incaricati, la propria password di accesso all'account di posta elettronica (o la password di rete se l'account di posta non prevede una specifica password). Successivamente al suo ritorno dall'assenza, il dipendente deve modificare la password. Qualora il dipendente assente sia irraggiungibile, o comunque in caso di effettiva urgenza, nei limiti di quanto necessario al fine di assicurare la continuità dell'attività aziendale e/o per effettuare interventi per garantire la sicurezza del sistema informatico, il Responsabile IT potrà altresì accedere alla posta elettronica del dipendente mediante le proprie credenziali di amministratore, previa semplice informazione al dipendente.
10. in caso di assenza non programmata dal lavoro (ad es. malattia etc.), il dipendente ha l'obbligo di attivare o far attivare il servizio di risposta automatica (*Out of office*), seguendo le istruzioni ricevute dall' IT.

Posta elettronica con l'esterno

Gli utenti abilitati all'uso della POSTA ELETTRONICA dovranno attenersi alle direttive di archiviazione che saranno impartite dai responsabili degli uffici e da Casa Madre.

Posta elettronica all'interno della SOCIETÀ

È possibile usare la posta elettronica anche all'interno dell'azienda, tra colleghi, seguendo le istruzioni ricevute dall' IT.

2.8 Comportamenti vietati

In ogni caso di uso della posta elettronica aziendale, sia con l'esterno che all'interno della SOCIETÀ, al dipendente non è consentito:

a) Utilizzare gli indirizzi di POSTA ELETTRONICA aziendale per inviare o ricevere messaggi a carattere personale;

b) Utilizzare gli indirizzi di POSTA ELETTRONICA contenenti il dominio della SOCIETÀ (@marsh.com) per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta della SOCIETÀ, nonché per partecipare a qualunque genere di petizione, catene di Sant'Antonio o, in generale, a qualunque pubblico dibattito su qualsivoglia tema.

c) Promuovere utile o guadagno personale.

d) Redigere messaggi di POSTA ELETTRONICA diretti a destinatari esterni alla SOCIETÀ senza il rispetto delle seguenti regole:

   – per i procuratori, l'indicazione del nome, cognome, carica e ufficio sotto la ragione sociale della società;

   – per gli altri, la sola indicazione del nome, cognome e ufficio.

e) Utilizzare il servizio di POSTA ELETTRONICA per trasmettere a soggetti esterni alla SOCIETÀ, INFORMAZIONI RISERVATE o comunque documenti aziendali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte.

f) Trasmettere messaggi a gruppi numerosi di dipendenti (es. a tutto un ufficio o ad un'intera divisione) senza l'autorizzazione necessaria.

g) Accedere a caselle di POSTA ELETTRONICA personali attraverso la rete e le apparecchiature della SOCIETÀ. Il dipendente non potrà, peraltro, inoltrare automaticamente i messaggi ricevuti all'indirizzo di POSTA ELETTRONICA aziendale su indirizzi personali.

h) Creare, archiviare o spedire, anche all'interno della rete aziendale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) in nessun modo connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto utilizzando l'indirizzo aziendale.

i) Sollecitare donazioni di beneficenza o altre voci non legate al lavoro.

j) Inviare, tramite la POSTA ELETTRONICA, anche all'interno della rete aziendale, alcun materiale a contenuto violento, sessuale o comunque offensivo dei principî di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico. Inviare messaggi di POSTA ELETTRONICA, anche all'interno della rete aziendale, che abbiano contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap. Qualora il dipendente riceva messaggi aventi tali

contenuti, è tenuto a cancellarli immediatamente e a darne comunicazione tempestiva al Responsabile dell' IT.

k) Spedire una e-mail con allegato un FILE eseguibile (.exe) senza la previa autorizzazione scritta del diretto superiore gerarchico e dell'IT.

l) Utilizzare la POSTA ELETTRONICA aziendale in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, d.lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248).

m) Inviare a indirizzi di posta elettronica privata e-mail con allegati documenti aziendali o, anche senza allegati, e-mail di contenuto attinente all'attività lavorativa.

2.9 Gestione dell'account di posta elettronica successivamente alla cessazione del rapporto di lavoro

Successivamente alla cessazione del rapporto di lavoro la casella di posta elettronica sarà disattivata. Sarà inoltre predisposto temporaneamente un sistema di risposta automatica per informare il mittente dell'avvenuta disattivazione dell'account di posta elettronica e dare indicazione del nuovo referente aziendale.

Il contenuto degli account di posta elettronica disattivati sarà registrato in un file di backup. Successivamente alla cessazione del rapporto di lavoro, la Società potrà liberamente accedere al contenuto del file di backup, del personal computer nonché alla casella di posta elettronica assegnata al lavoratore durante il rapporto di lavoro per ragioni di continuità dell'attività della Società, per finalità di sicurezza del sistema informatico, nonché quando ciò sia necessario nei casi di cui all'Articolo 3.1.2 (a) e 3.1.2(b).

2.10 Accesso alla posta elettronica nell'ambito del programma BYOD

Le regole stabilite dagli Articoli 2.7, 2.8, 2.9 della presente procedura sono applicabili, in relazione alle sole applicazioni aziendali, anche per l'utilizzo della posta elettronica nell'ambito del programma BYOD.

2.11 Modalità di uso del PC portatile, BlackBerry o altri dispositivi elettronici

Il PC portatile, BlackBerry o altri dispositivi elettronici possono essere concessi in uso dalla SOCIETÀ ai dipendenti che durante gli spostamenti sul territorio necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete della SOCIETÀ.

La richiesta del PC portatile o del BlackBerry deve essere presentata al superiore gerarchico per l'autorizzazione.

Circa l'uso del PC portatile, BlackBerry o altri dispositivi elettronici, il dipendente è informato che:

a) Il PC portatile o il BlackBerry può essere facilmente rubato o smarrito se non se ne ha particolare cura. La perdita del PC portatile o del BlackBerry, oltre il suo valore intrinseco, può provocare la perdita di informazioni importanti per la SOCIETÀ, e quindi costituisce sempre un danno economico per la stessa. Si richiede, quindi, particolare diligenza nella custodia del PC portatile o del BlackBerry.
b) In caso di furto o smarrimento del PC portatile o del BlackBerry, il dipendente deve denunciare l'accaduto alle competenti autorità di Pubblica Sicurezza e comunicare immediatamente l'user ID all'IT, in modo da impedire ad altri di utilizzarli. Copia della denuncia deve essere consegnata, entro tre giorni dall'evento, all'Ufficio Legale della SOCIETA'.
c) A discrezione della SOCIETÀ, in caso di smarrimento fuori dall'azienda, il dipendente potrà essere ritenuto responsabile del risarcimento del danno pari al valore di mercato del bene al momento dell'accaduto. In caso di danneggiamento, a discrezione della SOCIETA', potranno essere addebitate le spese di riparazione.
d) In caso di cessazione del rapporto e in tutti gli altri casi in cui ciò sia richiesto dalla SOCIETÀ (quali ad esempio il venir meno delle ragioni di servizio che avevano determinato l'assegnazione, la sua sostituzione con altro portatile o BlackBerry), il PC portatile e/o il BlackBerry dovranno essere restituiti all' IT nella loro interezza, comprese eventuali periferiche interne ed esterne.

L'assegnazione del PC portatile o del BlackBerry o di altro dispositivo elettronico può, comunque, essere revocata dalla SOCIETÀ.

2.12 Modalità di uso dei telefoni cellulari aziendali

Qualora la SOCIETÀ abbia deciso di dare in dotazione ai dipendenti, in via fiduciaria, telefoni cellulari di sua proprietà, confida nel fatto che essi ne facciano un uso corretto e di buona fede, secondo quanto precisato qui di seguito:

a) È fatto divieto di utilizzare i telefoni cellulari aziendali dati in dotazione per fini diversi da quelli legati allo svolgimento della prestazione lavorativa e degli altri espressamente consentiti, in contrasto con disposizioni di legge o regolamenti e comunque in contrasto con gli usi e la buona fede.
b) Le comunicazioni telefoniche eseguite o ricevute per motivi professionali devono intendersi effettuate esclusivamente nell'interesse della SOCIETÀ.
c) Il telefono cellulare può essere rubato o smarrito: a tal fine occorre proteggerlo dai furti mediante l'inserimento del PIN.

d) Il dipendente è tenuto ad un uso corretto del telefono cellulare che non dovrà essere utilizzato per scaricare dati di alcun genere (loghi, suonerie, servizi informativi) se non su specifica autorizzazione da parte della SOCIETÀ.

3

Controlli

3.1 Controllo sul rispetto delle modalità di utilizzo di INTERNET e della POSTA ELETTRONICA

Marsh promuove ogni opportuna misura organizzativa, tecnologica e di sicurezza volta a prevenire il rischio di utilizzi indebiti che possono essere fonti di responsabilità, a "minimizzare" l'uso di dati riferibili ai lavoratori e a garantire la disponibilità e l'integrità dei sistemi informativi e dei dati; allo scopo, la Società ha adottato strumenti tecnici e organizzativi volti a prevenire trattamenti illeciti sui dati trattati con strumenti informatici, come illustrato nella presente procedura.

Marsh informa di aver adottato sistemi che evitano interferenze ingiustificate sui diritti e sulle libertà fondamentali dei lavoratori e dei soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata, nel rispetto del principio di pertinenza e non eccedenza, con esclusione di qualunque registrazione o monitoraggio sistematico e di analisi occulta.

Premesso che l'uso del PC aziendale, di INTERNET e dell'indirizzo di POSTA ELETTRONICA aziendale, attraverso le apparecchiature aziendali, è consentito solo per motivi di lavoro e nell'interesse esclusivo della SOCIETÀ, mentre ne è vietato l'uso personale, e che l'utilizzo dei sistemi informatici non conforme alle regole di cui alla presente Policy può comportare delle serie minacce alla sicurezza informatica e alla corretta conservazione dei dati essenziali per l'attività di Marsh nonché il rischio di sanzioni civili, amministrative e penali sia per Marsh sia per lo stesso lavoratore, la SOCIETÀ si riserva espressamente il diritto di esercitare controlli (ad esempio per fini di manutenzione, per esigenze di sicurezza, e/o per verificare il rispetto delle modalità di utilizzo da parte dei dipendenti degli strumenti informatici in dotazione, nonché al fine di prevenire e/o accertare la commissione di atti che possono costituire reati o comunque atti illeciti).

I controlli possono avvenire secondo due livelli, denominati rispettivamente "ordinario" e "straordinario", secondo le modalità di seguito descritte agli Articoli 3.1.1 e 3.1.2

3.1.1 Controllo Ordinario

Il primo livello di controllo "ordinario" viene svolto in maniera anonima e in caso di elusione dei filtri preventivi preimpostati che riducono al minimo l'esigenza del controllo successivo. Il sistema di Firewall per l'accesso a siti Internet di contenuto illecito o comunque non attinente all'attività lavorativa nonché il sistema di filtraggio automatico delle mail (anti-spam, quarantena di files riconosciuti come non sicuri ecc.) possono infatti subire elusioni. In questo caso il sistema genera automaticamente degli avvisi di anomalia ("*alert*" relativi a, in via esemplificativa, scarico di files pirata, navigazioni da cui sia derivato il download di virus informatici, ecc.) che vengono visualizzati dal personale IT. La finalità del controllo relativamente agli accessi a Internet è verificare se dai dati di connessione non risultino anomalie quali la violazione o l'elusione del sistema di blocco (Firewall) dei siti a contenuto illecito (es. siti a contenuto violento, discriminatorio, pornografico ecc.) o comunque non attinenti all'attività lavorativa . La finalità del controllo relativo alla posta elettronica è verificare che l'e-mail aziendale venga utilizzata in conformità con le regole di condotta stabilite nella presente Policy e quindi che non venga utilizzata per ricevere notifiche di messaggi da server esterni, non sicuri o comunque non attinenti all'attività lavorativa, per inviare a soggetti o indirizzi di posta elettronica non autorizzati informazioni e documenti riservati (es. invio di files a propri account di posta elettronica privati), per effettuare operazioni on-line non sicure e potenzialmente dannose non solo per Marsh ma per lo stesso lavoratore (es. acquisti su siti Internet, download di files audio/video in violazione della legge sul copyright ecc.).

In caso di avviso di anomalia, Marsh effettuerà un controllo anonimo sui dati aggregati riferito all'intera struttura aziendale oppure a sue aree, in modo da poter individuare l'area aziendale da richiamare al rispetto delle regole procedurali. Il controllo anonimo potrà concludersi con un avviso generalizzato relativo all'utilizzo anomalo di strumenti aziendali, con l'invito ad attenersi scrupolosamente alle istruzioni impartite a mezzo della presente procedura. Qualora il comportamento anomalo dovesse ripetersi o comunque nei casi di maggiore gravità (es. accesso a siti illegali o a contenuto discriminatorio o violento), Marsh potrà effettuare controlli su base individuale ("Controllo Straordinario").

3.1.2 Controllo Straordinario

Il secondo livello di controllo denominato "straordinario" viene attuato nei seguenti casi:

a) nel caso in cui all'esito del controllo ordinario emergano comportamenti anomali ripetuti o comunque di particolare gravità (es. accesso a siti illegali o a contenuto discriminatorio o violento);

b) nel caso vi sia l'esigenza di svolgere indagini di natura difensiva ovvero nel caso in cui sia necessario accertare, anche nel quadro della normativa di cui al D. Lgs. 8 giugno 2001, n. 231, comportamenti che possano costituire reato o che siano comunque illeciti o non conformi alla presente Policy e, in genere, ai regolamenti aziendali di Marsh, posti in essere mediante l'utilizzo

del personal computer, di Internet e della posta elettronica aziendale.

Nei suddetti casi, Marsh potrà, per mezzo del proprio personale IT, previo coinvolgimento dell'HR Manager verificare il contenuto dei file presenti sui SERVER. A tal fine deve essere inoltrata apposita richiesta all'MGTI (MMC Global Technology Infrastructure) con sede a Londra da parte dell'IT locale di concerto con l'HR. Il controllo straordinario potrà avvenire, laddove la natura dell'indagine lo richieda, anche mediante accesso diretto al PC del dipendente che, su richiesta, dovrà consegnarlo al Responsabile IT.

Il controllo straordinario potrà altresì avvenire con la collaborazione di professionisti esterni (quali società di auditing, avvocati, consulenti informatici ecc.), mediante accesso al server e/o alla memoria di massa del computer dato in dotazione al dipendente. Marsh dovrà, in ogni caso, provvedere alla nomina di un responsabile del procedimento. In mancanza di nomina specifica il responsabile del procedimento sarà il Direttore del Personale. Il controllo straordinario non potrà avere ad oggetto un arco temporale eccedente i sei mesi precedenti la data in cui esso viene effettuato, salva la necessità di estendere l'indagine oltre tale periodo in ragione della natura del comportamento oggetto di indagine e/o in conseguenza di fatti emersi nel controllo relativo ai sei mesi precedenti la data dell'indagine. Del suddetto controllo, verrà redatto processo verbale che dovrà riportare la data di inizio dell'indagine, il motivo dell'indagine, una descrizione sintetica delle attività di indagine svolta, il relativo arco temporale, la data della chiusura dell'indagine, se la conclusione dell'indagine richiede o meno l'instaurazione di un procedimento disciplinare. Il verbale di indagine dovrà essere sottoscritto dal responsabile del procedimento. Qualora non sia necessaria l'instaurazione di un procedimento disciplinare, sarà conservata copia del verbale di indagine mentre i relativi documenti cartacei (es. stampa delle e-mail, stampa dei siti internet visitati ecc.) dovranno essere distrutti, salvo che tali documenti siano necessari al fine di difendere un diritto della Società nei confronti di soggetti diversi dal dipendente. Tale eventuale necessità di conservare i documenti cartacei di indagine anche in mancanza di procedimenti disciplinari dovrà essere indicata e motivata nel verbale di indagine. Qualora si ritenga di dover instaurare un procedimento disciplinare, i documenti raccolti nel corso dell'indagine potranno essere conservati sia su sopporto informatico sia su supporto cartaceo, per il tempo necessario al fine di difendere i diritti di Marsh, connessi al procedimento disciplinare stesso e al suo esito.

In caso di indagine da effettuarsi per ordine di una Pubblica Autorità, potranno essere effettuati controlli anche al di fuori della procedura di cui al presente Articolo 3.1.2, secondo le modalità e con le procedure eventualmente prescritte dalla stessa Pubblica Autorità.

Resta inteso che entro 15 giorni dal completamento dell'indagine sarà data comunicazione alle RSA e al lavoratore.

3.2 Controlli sulla posta elettronica nell'ambito del programma BYOD

Le regole stabilite dagli Articoli 3.1.1 e 3.1.2 della presente procedura sono applicabili, in relazione alle sole applicazioni aziendali, anche ai controlli della posta elettronica nell'ambito del programma BYOD.

3.3 Rappresentanti dei lavoratori nell'ambito del Controllo Straordinario

Le RSA avranno la facoltà di verificare i verbali di indagine secondo la procedura di seguito stabilita.

Con cadenza biennale, la Società, in apposito incontro da organizzarsi a richiesta delle RSA, fornirà una informativa sui controlli straordinari conclusi nei 24 mesi precedenti. A richiesta delle RSA, da inoltrarsi per iscritto (anche mediante e-mail) al Direttore del Personale, la Società dovrà concedere la consultazione dei verbali di indagine alle RSA. Entro sette giorni lavorativi dalla richiesta di consultazione la Società dovrà mettere a disposizione un locale e copia dei verbali di indagine relativi ai 24 mesi precedenti per la consultazione. Non è consentita la copia di alcun verbale di indagine, salvo diverso accordo con la Società. Nei sette giorni lavorativi successivi alla avvenuta consultazione le RSA potranno chiedere, per iscritto, un incontro con il responsabile del procedimento o i responsabili dei procedimenti che hanno sottoscritto i verbali di indagine oggetto di consultazione. Nella richiesta scritta di incontro dovranno essere sommariamente indicati i chiarimenti che le RSA intendono ottenere. Nei 7 giorni lavorativi successivi alla richiesta di incontro, la Società dovrà incontrare le RSA per fornire i chiarimenti che saranno richiesti. Decorsi 7 giorni lavorativi dalla data dell'incontro per i chiarimenti la procedura si intende esaurita senza alcun ulteriore obbligo per la Società. Con il consenso di entrambe le parti possono essere stabiliti di volta in volta, termini diversi, superiori o inferiori.

Tali modalità di Controllo Straordinario consentono di evitare che i controlli suddetti siano svolti con finalità di profilazione delle abitudini dei dipendenti o con finalità di controllo a distanza degli stessi

Le informazioni di cui la Società venisse a conoscenza a seguito del controllo straordinario, non potranno essere utilizzate per accertamenti circa l'obbligo di diligenza del lavoratore, né per finalità di valutazione della prestazione, né per l'adozione di provvedimenti disciplinari, salvi i casi di dolo e/o colpa grave.

Ai dipendenti sarà consegnata copia della suddetta procedura.

3.4 Trattamento di dati personali

Le procedure di controllo di cui alla sezione 3. della presente procedura nonché gli accessi, successivi alla cessazione del rapporto di lavoro, al contenuto del personal computer, ai file di backup, nonché alla casella di posta elettronica di dipendenti ed ex dipendenti possono comportare il trattamento di dati personali ai sensi del D. Lgs. 30 giugno 2003, n. 196.

Le finalità e modalità del trattamento, nonché i soggetti all'interno della Società che possono venire a conoscenza dei dati sono indicati ai precedenti Articoli 3.1.1 e 3.1.2.

Il titolare del trattamento è la Società. I responsabili del trattamento sono il Responsabile IT e il Direttore del Personale.

I dati non saranno diffusi. Potranno essere comunicati a società del gruppo Marsh, professionisti esterni, consulenti della Società, quali avvocati, consulenti informatici, auditors, Pubbliche Autorità, per le finalità di cui agli Articoli 3.1.1 e 3.1.2. La comunicazione potrebbe altresì avvenire anche con la finalità di difendere in giudizio un diritto di Marsh e/o di società del gruppo Marsh.

Il trattamento dei dati oggetto di controllo straordinario non potrà essere superiore a quello necessario agli scopi per i quali la stessa documentazione è stata raccolta e successivamente trattata, ai sensi dell'art. 11, comma 1, lett. e), Codice Privacy nonché dell'art. 6 dell'Autorizzazione Generale n. 1/2005 del 21 dicembre 2005 e paragrafo 6.2 della deliberazione n. 13 del 1 marzo 2007 dell'Autorità Garante della Privacy, al termine del quale l'IT dovrà provvedere alla cancellazione dei dati.

In qualità di interessato al trattamento, ciascun lavoratore ha facoltà di esercitare i diritti di cui all'Articolo 7 del D. Lgs. 30 giugno 2003, n. 196 ovvero:

- il diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano e la loro comunicazione, l'aggiornamento, la rettificazione e l'integrazione dei dati, la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge.

- il diritto di ottenere gli estremi identificativi aggiornati del titolare nonché l'elenco aggiornato dei responsabili e di tutti i soggetti cui i dati sono comunicati.

- il diritto di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati che lo riguardano.

I diritti di cui sopra, potranno essere esercitati dal lavoratore in qualsiasi momento, anche successivamente alla cessazione del rapporto di lavoro con Marsh, mediante invio di semplice richiesta scritta al Direttore del Personale.

Il riscontro alle richieste di esercizio di tali diritti sarà fornito secondo quanto stabilito dalla normativa di tempo in tempo in vigore, nell'ambito del principio del bilanciamento di interessi, salve le esclusioni previste dalla legge e avuto riguardo ad eventuali esigenze di confidenzialità e/o di tutela della riservatezza di terzi, che di volta in volta dovranno essere valutate a cura della Società.

Al fine di verificare la correttezza dei controlli effettuati, il log degli accessi dell’account dedicato viene conservato per un periodo di tempo non inferiore a tre anni.