Modena settembre 2010
Allegato 1)

Piano di razionalizzazione dell'utilizzo delle dotazioni strumentali, anche informatiche, che corredano le stazioni di lavoro nell'automazione d'ufficio;(aggiornamento)

Monitoraggio dell'assegnazione di apparecchiature di telefonia mobile

Dotazioni strumentali

L'azienda dispone di 1800 personal computer all'interno di questo parco macchine vi sono 197 pc portatili.
L'assegnazione utilizzo / dei 197 portatili si può ulteriormente suddividere rilevando che circa 120 postazioni (2 – 3 per struttura complessa) sono destinati al supporto del giro visita e sono fisicamente installati su carrelli con lucchetto di sicurezza.

I restanti 77 circa sono assegnati in via diretta e nominale ad operatori dell'azienda secondo i seguenti criteri

Operatori che per motivi di servizio sono impegnati in frequenti missioni al di fuori del campus aziendale
Operatori che per motivi di servizio sono potenzialmente impegnati in servizi di reperibilità (h24 x 365) e pertanto necessitano di strumenti remoti necessari a fruire delle risorse elaborative dell'azienda.
Componenti dell' Alta Direzione e del collegio di direzione

Tale dotazione – considerata a regime – è stata costruita nel tempo mediante l'adesione alle convenzioni nazionali e regionali stipulate grazie all'azione delle centrali di acquisto (consip, intercenter)

Negli ultimi due anni non sono state acquisite nuove attrezzature di questo tipo il cui indice di turn-over è di 7 anni.

Razionalizzazione nell'uso delle stampanti.

L'unica tecnologia adottata in questa materia (salvo rarissime accezioni) è Laser B/N con opzione fronte retro.

L'azione dell'ultimo biennio è stata impostata nell'ottica di centralizzare, per gruppi di lavoro, le risorse di stampa a favore di sistemi in rete multifunzione (stampa, fotocopia, scanner, fax). Tale azione ha consentito di non acquistare nell'ultimo biennio laser b/n ad utilizzo individuale , salvo garantire con l'acquisto di 40 unità, il tourn over dei sistemi di stampa che per motivi logistici non possono essere rimpiazzati da soluzioni centralizzate (esempio tipico in questo senso sono gli ambulatori all'interno delle aree di degenza).

Anche in questo caso l'unico canale di acquisto è stato quello messo a disposizione delle già citate centrali nazionali e regionali.

Eliminazione fax e fotocopiatrici di proprietà

I fax e le fotocopiatrici di proprietà , dichiarati fuoriuso per eccessiva onerosità della riparazione, sono stati man mano sostituiti con fotocopiatrici multifunzioni.
Grazie all'adesione alle convenzioni stipulate dallecentrali di committenza nazionale e regionale, l'azienda ha in dotazione circa 80 fotocopiatrici a noleggio e ha adottato la politica dell'accentramento, dove possibile, della doppia funzione (fotocopiatrice ï fax) eliminando i costi di manutenzione, delle parti di ricambio e dei toner.

Apparecchiature di telefonia Mobile

L'azienda dispone di 86 telefoni mobili, i criteri di distribuzione sono essenzialmente correlati ai servizi di reperibilità e pronta disponibilità. In generale gli apparati sono assegnati alla funzione e non alla persona che in una determinata fascia oraria assolve alla funzione.
Questo consente di assicurare il medesimo servizio con un numero di apparati molto inferiore.

Sia gli apparati sia i contratti e le tariffe d'uso delle sim discendono dalle convenzioni regionali già citate.

Sul tema più ampio dei controlli e della responsabilizzazione degli operatori si riporta a seguire il regolamento adottato e diffuso nello scorso 2009 dal quale si evince l'impostazione generale che norma l'utilizzo delle attrezzature informatiche e telefoniche.

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Ospedaliero - Universitaria di Modena
Policlinico

Disciplinare sull'utilizzo degli strumenti informatici e di telefonia

Sommario

Premessa 2
Istruzioni 2
Accesso al sistema informatico aziendale e più in generale agli ausili tecnologici messi a disposizione dall'Azienda 2
Utilizzo dei supporti di memorizzazione 4
Buon uso della rete di comunicazione e delle attrezzature aziendali di comunicazione 5
Virus 5
Internet 6
Posta elettronica 7
Utilizzo dei sistemi di comunicazione in fonia – telefoni fissi, telefoni mobili, ecc… -..... 8
Ulteriori istruzioni 9
Utilizzo di fax 9
Utilizzo di fotocopiatrice e stampante 9
Tutela del diritto d'autore 9
Servizio deputato ai controlli 10
Facoltà dell'Azienda 10

Revisione	Data	Note / aggiornamenti
01	Maggio 2009	Prima Adozione

Premessa

Il presente disciplinare è stato redatto sulla base delle indicazioni contenute nel provvedimento del Garante per la protezione dei dati personali del 01.03.2007 "Lavoro. Le linee guide del garante per posta elettronica e internet".

L'Azienda garantisce che per nessuna ragione i dati informatizzati gestiti dall'Azienda, i sistemi di elaborazione dati e gli strumenti di telecomunicazioni saranno utilizzati per il controllo a distanza dei lavoratori (artt. 113, 114 e 184, comma 3, del Codice; artt. 4 e 8 l. 20 maggio 1970, n.300).

Il documento opera nei confronti di ogni dipendente dell'Azienda e di tutti coloro che a vario titolo si trovino ad utilizzare il sistema informativo dell'Azienda.

Sarà cura dell'operatore accertarsi se siano state pubblicate nuove versioni della presente linea guida e adottare comportamenti congrui a quanto prescritto relativamente ai propri ambiti specifici di competenza e di attività. Qualora l'operatore lo desideri potrà ottenere una copia a stampa del presente documento recandosi in un qualsiasi ufficio del Servizio Tecnologie dell'Informazione.

È comunque indispensabile che chiunque tratti dati personali o sensibili prenda visione del vigente DPS – Documento Programmatico sulla Sicurezza –. Copia del DPS è reperibile presso gli uffici del Servizio Tecnologie dell'Informazione Aziendale

Istruzioni

Le seguenti istruzioni sono parte del sistema di sicurezza che l'Azienda adotta al fine di gestire, nel rispetto della vigente normativa, i dati trattati.

Accesso al sistema informatico aziendale e più in generale agli ausili tecnologici messi a disposizione dall'Azienda

- tutti coloro che per ragioni di lavoro devono avere accesso al sistema informatico aziendale devono essere intestatari di un nome di utente all'interno del dominio di sicurezza aziendale; possono richiedere l'accesso ad Internet che sarà autorizzato o meno – in base alla mansione e a considerazioni organizzative – dal responsabile del trattamento di riferimento;
- la parola chiave di accesso alla postazione informatica e agli applicativi aziendali deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi;
- la parola chiave di accesso alla postazione informatica e agli applicativi aziendali deve essere modificata a cura dell'incaricato con cadenza almeno trimestrale.
- la parola chiave non deve contenere riferimenti facilmente riconducibili all'incaricato;
- l'incaricato è responsabile di ogni utilizzo indebito o non consentito della parola chiave di cui sia titolare;
- ai soli fini di controlli tecnici e di sicurezza gli accessi al dominio aziendale ed alle risorse informative (applicazioni) abilitate dall'accesso al dominio sono registrati su specifici archivi di log accessibili solo agli amministratori di dominio. Tutti i log sopra citati vengono conservati dall'Azienda per un massimo di 2 anni solari;. Le operazioni di cancellazione avvengono nel mese di gennaio di ogni anno. Eventuali approfondimenti sui log che si rendessero necessari saranno condotti nel pieno rispetto delle leggi vigenti ponendo particolare attenzione ai i criteri della pertinenza e non eccedenza rispetto al fine di controllo; qualora le verifiche portino all'accertamento della violazione delle presenti regole o più in generale all'accertamento di

utilizzi impropri, l'Azienda si riserva di adottare le opportune misure disciplinari e amministrative;

- tutti i PC hanno il programma antivirus installato e configurato per l'aggiornamento automatico; nel caso in cui si verifichi la non rispondenza della stazione di lavoro a tale requisito si è pregati di rivolgersi al Servizio Tecnologie dell'Informazione;
- in caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure atte a escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni riservate o accedere alle banche dati, ad esempio scollegandosi o attivando un salvaschermo protetto da password;
- il solo personale addetto alla manutenzione, al controllo e alla sicurezza delle infrastrutture tecnologiche è autorizzato a compiere le attività che garantiscano, oltre al buon funzionamento delle infrastrutture aziendali, il perseguimento dei fini istituzionali nei limiti e nel rispetto della normativa vigente;
- gli strumenti di comunicazione aziendali e gli strumenti di produttività personale in genere – telefono fisso, telefono cellulare, stazioni informatizzate di lavoro, fax, stampanti, ecc… - concessi in uso dovranno essere utilizzati per fini esclusivamente istituzionali e connessi alla propria mansione e attività di servizio; nessun altro uso di tali strumenti è consentito se non espressamente autorizzato anche se nelle potenzialità della strumentazione concessa in uso ed eventualmente abilitata; a questo proposito è bene precisare che talvolta non è possibile disabilitare determinate funzionalità da alcuni apparati tecnologici, o che questo, anche se tecnicamente possibile, può essere organizzativamente oneroso per l'Azienda; ciò posto la disponibilità di una determinata funzionalità non autorizza il consegnatario di un bene all'utilizzo della stessa se non espressamente autorizzato e comunque se non necessario all'espletamento delle proprie mansioni e riconducibile ad attività istituzionali;
- nessun dispositivo personale potrà essere collegato alla rete dell'Azienda e/o utilizzato per trattare dati istituzionali aziendali; qualora l'Azienda, per l'espletamento della propria attività istituzionale si avvalga di attrezzature la cui gestione in sicurezza ricada sotto la responsabilità di personale non dipendente o a questi assimilabile, dovrà essere formalmente definito un Responsabile/Incaricato Esterno che si faccia garante degli aspetti di sicurezza e di rispondenza alla normativa vigente in tema di trattamento dei dati personali per tutti i trattamenti che avvengono su tali attrezzature;
- l'Azienda si riserva di verificare l'utilizzo degli strumenti aziendali concessi in uso – ad esempio il telefono, le stazioni di lavoro informatizzate, i palmari, ecc… - qualora si evidenzino volumi anomali di traffico o vi siano altri elementi che indichino un uso non conforme alle presenti indicazioni;
- l'Azienda vieta di memorizzare e/o trattare dati a fini personali di qualsiasi tipo per mezzo o all'interno degli strumenti aziendali concessi in uso. Il personale tecnico dell'Azienda, o il personale delle Aziende che in nome e per conto dell'Azienda effettuano attività di manutenzione sugli strumenti aziendali - attrezzature di produttività personale, sistemi di comunicazione, ecc… - potranno accedere a detti strumenti per compiti connessi alla rispettiva funzione e mansione. Non potrà essere addotto come impedimento all'accesso il fatto che siano presenti dati utilizzati a fini personali in forza del suddetto divieto di gestire dati non connessi alla propria mansione e/o attività istituzionale –;
- in particolare è fatto espresso divieto di memorizzare sui file server aziendali, foto, filmati, brani musicali, etc.etc. che non abbiano attinenza ed utilità rispetto alle proprie mansioni. Nell' ambito dei controlli sui dati aggregati ove risulti un'occupazione di spazio disco superiore alla media, il personale che effettua i controlli ha facoltà di segnalare al responsabile della articolazione organizzativa od al singolo utente la presenza di materiale di "dubbio" contenuto istituzionale.
- modalità da seguire per l'accesso ai dati in caso di prolungata assenza dell'incaricato – in ottemperanza a quanto prescritto al punto 10 dell'allegato B del d.lvo 196/2003-:

- è necessario distinguere due diversi casi:
  a) il caso in cui i dati sono accessibili da più di un operatore;
  b) il caso in cui i dati sono accessibili da parte di un unico operatore;

  (a) sarà necessario adottare le misure di seguito descritte solo nel caso in cui tutti gli operatori che hanno accesso ad un medesimo dato non siano presenti per un lungo periodo, per cui di seguito per semplicità *si* farà riferimento al solo caso b) come di seguito indicato:
  - nel caso in cui l'operatore che ha normalmente accesso al dato non possa per lungo periodo garantire ciò, sarà cura del responsabile del trattamento vicariare tale mancanza;
  - nel caso il responsabile del trattamento sia in grado di utilizzare le attrezzature e gli applicativi informatici normalmente utilizzati dall'operatore, basterà che il responsabile del trattamento richieda al Servizio Tecnologie dell'Informazione le abilitazioni necessarie ad accedere al dato; una volta ricevute le abilitazioni opportune potrà accedere ai dati al posto dell'operatore assente; il responsabile del trattamento dovrà informare di ciò l'incaricato assente alla prima occasione utile;
  - nel caso il responsabile del trattamento non sia in grado di utilizzare direttamente le attrezzature e gli applicativi informatici normalmente utilizzati dall'operatore, farà richiesta al tecnico del Servizio Tecnologie dell'Informazione che normalmente si occupa degli aspetti tecnici dell'applicativo di accedere ai dati necessari in qualità di incaricato temporaneo;
  - la misura precedente dovrà essere utilizzata solo nel caso in cui l'urgenza lo richieda e nella misura strettamente necessaria a risolvere la situazione contingente; se l'esigenza va oltre la singola necessità e qualora i tempi lo consentano, il Responsabile del trattamento disporrà di abilitare un diverso incaricato, in aggiunta a quello assente, all'accesso dei dati; il responsabile del trattamento dovrà informare di ciò l'incaricato assente alla prima occasione utile;
  - sarebbe opportuno che la individuazione di un diverso incaricato da abilitare all'accesso ai dati avvenisse da parte del responsabile all'interno di una rosa di fiduciari allo scopo previsti dall'incaricato; una tale gestione, se attuata, è in carico ai responsabili del trattamento;
  - le diverse richieste attinenti alla casistica descritta dovranno essere documentate da richieste scritte, eventualmente anche formulate via mail.

Utilizzo dei supporti di memorizzazione

È vietato l'uso di supporti di memorizzazione removibili per la memorizzazione di dati personali o sensibili. Deroghe a tale regola sono possibili solo nei casi in cui sia possibile dimostrare il corretto uso dei supporti di memorizzazione ai sensi del D.L. 196/2003 Allegato B, punti 21 e 22:

1. è possibile il reimpiego del supporto solo nel caso non siano più recuperabili le informazioni precedentemente memorizzate;
2. nel caso non sia garantibile il requisito di cui al punto (1), il supporto removibile dopo l'uso andrà distrutto.

In generale i supporti di memorizzazione – anche non removibili - che contengono dati personali o sensibili, nel caso non possano essere cancellati in maniera da renderne irrecuperabile il contenuto, una volta dimessi – per es. per obsolescenza o per guasto -, dovranno essere distrutti o smaltiti in maniera tale che il contenuto non sia più recuperabile.

Buon uso della rete di comunicazione e delle attrezzature aziendali di comunicazione

La rete di trasmissione dati e fonia è un prezioso bene aziendale condiviso e pertanto va gestita nel rispetto delle esigenze complessive di azienda. In funzione di ciò viene fatto esplicito e tassativo divieto di connettere in rete stazioni di lavoro se non dietro esplicita e formale autorizzazione del Sistema Informativo Aziendale. È altresì vietato alterare in qualsiasi modo la configurazione software della stazione di lavoro - o di altri dispositivi direttamente connessi alla rete, dati o fonia - per quanto attiene all'accesso alla rete. È anche fatto divieto di utilizzare in qualsiasi modo la rete aziendale per fini non espressamente autorizzati. In particolare tali divieti si possono tradurre, anche se non esaurire, nelle seguenti esplicite proibizioni:

- divieto di condividere cartelle in rete (né dotate di password, né sprovviste di password) se non espressamente autorizzate dal Servizio tecnologie dell'informazione ;
- divieto di alterare la configurazione di rete di stazioni di lavoro e altri dispositivi in rete (stampanti condivise, ecc…), comprendendo in ciò anche il divieto di aggiungere protocolli di rete o servizi in rete (per es. condivisione di stampanti in rete, browsing di risorse di rete, ecc…);
- è vietato intercettare/monitorare/ascoltare/leggere dati sulla rete di trasmissione dati o sulla rete di comunicazione in fonia.

È vietata l'installazione non autorizzata di Modem per linee analogiche o digitali che sfruttino il sistema di comunicazione in fonia per l'accesso a banche dati esterne o interne all'Azienda. È vietata l'installazione non autorizzata di apparati di rete di qualsiasi tipo – hub, switch, router, access point WI-FI, access server, ecc… - È vietata l'installazione di qualsiasi attrezzatura informatica o di comunicazione non espressamente autorizzata dal Servizio tecnologie dell'Informazione.

È vietata l'installazione di hardware o software di qualsiasi tipo che consenta o faciliti il by pass delle misure di presidio del confine aziendale - per es. software di comunicazione che garantiscano accessi che non passino dai Firewall Aziendali o dagli altri accessi autorizzati e presidiati -.

L'utente è inoltre tenuto a conservare con la massima cura eventuali dispositivi per l'accesso ai sistemi aziendali e ad usarli conformemente alle specifiche indicazioni d'uso. La perdita o danneggiamento degli stessi sarà sanzionata.

I responsabili delle varie macro articolazioni organizzative, di concerto con i responsabili del trattamento e con il Sistema Informativo Aziendale sono responsabili della adozione degli atti e delle misure organizzative necessarie a garantire un adeguato controllo relativamente alle norme di buon uso dei sistemi informatici e di telecomunicazione dell'azienda.

Virus

Si invitano gli utenti:

- alla massima cautela nella gestione dei supporti magnetici e della posta elettronica: in particolare ogni qualvolta un supporto di memorizzazione - dischetto removibile, nastro magnetico, disco magneto-ottico e ogni altro supporto di memorizzazione removibile - sia stato utilizzato su un computer diverso dal proprio - supponendo che il proprio PC sia immune da infezioni - occorrerà verificare l'assenza di virus mediante un programma antivirale aggiornato. Se non vi è l'assoluta certezza che il proprio computer possieda un antivirus aggiornato non sarà possibile utilizzare il supporto di memorizzazione - in quanto potenzialmente infetto -;

- in generale sarebbe bene conoscere sempre con precisione quale sia la fonte dei dati, ed essere certi che tale fonte sia affidabile e sicura; è preferibile non utilizzare un supporto di memorizzazione removibile di cui non si conosca la fonte;
- è bene sempre evitare di leggere o utilizzare allegati di messaggi di posta elettronica che non provengano da fonti certe, riconosciute e sicure; nel caso pervenga un messaggio di tale natura procedere immediatamente alla eliminazione. Nel caso si abbia il sospetto che il proprio sistema di elaborazione sia stato infettato avvertire il personale tecnico competente e non operare per alcun motivo scambio di supporti di memorizzazione o posta elettronica con altri. Nel caso si abbia notizia di un nuovo tipo di virus, comunicare tale informazione all'ufficio reti del Servizio Tecnologie dell'Informazione, evitando indiscriminati messaggi a tutti i propri conoscenti - questo evita l'ingenerarsi di falsi allarmi e di inutili catene di Sant'Antonio.

Internet

- è vietato l'utilizzo personale e non istituzionale della connessione a internet aziendale
- tutti gli accessi ad Internet vengono registrati sul sistema di sicurezza aziendale in appositi file di log; tali log tengono traccia dei seguenti dati per ogni accesso:
  - identificativo dell'utente che ha navigato in internet;
  - identificazione della stazione di lavoro;
  - Data e ora
  - Riferimento al sito visitato (URL)

  Tali log sono indispensabili all'Azienda per poter costantemente monitorare il corretto funzionamento del sistema nella sua globalità e per poter effettuare statistiche periodiche sull'uso del sistema entrambi su base anonima; i log saranno trattati in maniera tale da fornire informazioni in maniera aggregata in modo da precludere l'immediata identificazione degli utenti, a meno che non vi siano specifiche ragioni per accedere al dettaglio massimo, cioè alle informazioni di tipo nominativo.

- l'Azienda si riserva di filtrare l'accesso a siti che risultino non in relazione con le attività istituzionali; il filtraggio verrà attuato mediante l'inserimento del sito in una cosiddetta "Black list" ovvero nell'inserimento del sito in una categorizzazione, eventualmente predisposta anche da fornitori esterni specializzati; la lista dei siti inaccessibili o delle categorie potrà essere chiesta al Servizio Tecnologie dell'Informazione da chiunque e in caso di motivate ragioni potrà essere autorizzata la navigazione sul sito mediante rimozione dalla lista di esclusione; l'esclusione dei siti verrà operata periodicamente in base all'analisi di dati aggregati;

- a titolo di esempio, senza che questo costituisca un elenco esaustivo, non è consentito:
  - servirsi o dar modo ad altri di servirsi della stazione di accesso a Internet per attività non istituzionali, attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
  - scaricare software dalla rete; eventuali necessità dovranno essere appositamente richieste al Servizio Tecnologie dell'Informazione che provvederà a eseguire fisicamente lo scarico da stazione protetta, applicare le misure antivirus relative e consegnare il software al richiedente;
  - utilizzare Internet Provider diversi da quello aziendale e la connessione di stazioni di lavoro aziendali alle reti di detti provider con sistemi di connessione diversi (es. modem) da quello centralizzato;
  - usare la rete in modo difforme da quanto previsto dal presente documento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete;

- produrre e pubblicare propri siti Web sulla infrastruttura tecnologica dell'Azienda; ogni eventuale necessità di realizzare siti Web personali o di struttura dovrà essere espressamente autorizzata dal Responsabile del trattamento dei dati;

Posta elettronica

- è vietato l'utilizzo personale e non istituzionale della posta elettronica aziendale;

Il sistema di posta elettronica in uso, e concesso in utilizzo, non è un sistema di posta certificata salve talune postazioni a ciò abilitate, non vi è pertanto la garanzia della consegna o della ricezione dei messaggi di posta, né fornisce garanzia di privatezza relativamente ai messaggi inviati in quanto non usa alcuna tecnica di crittografia dei contenuti o di protezione delle autenticazioni. È pertanto fatto divieto di inviare materiali che non siano compatibili con tali caratteristiche del servizio;

- il sistema di posta elettronica tiene traccia di tutte le e-mail inviate e ricevute:
  - data e ora;
  - identificativo della stazione di lavoro che ha inviato il messaggio;
  - indirizzo di posta del mittente;
  - indirizzo del destinatario;
  - Anche in questo caso i log vengono mantenuti per lo stesso periodo e le stesse finalità indicate per gli accessi Internet;

- tutta la posta in transito sul sistema aziendale viene controllata da un sistema antivirus che, oltre a bloccare le e-mail con dei virus, effettua i seguenti controlli:
  - blocco delle e-mail con allegati potenzialmente pericolosi (ad esempio con estensioni EXE, COM, .VBS, .PIF, .SCR, .SYS, .BIN, .OVL, .DRV, .OVY, .LNK, ZIP, RAR etc. etc.).
  - blocco delle e-mail con dimensioni complessive (messaggio di posta + allegati) superiori a 7 Mb.
  - blocco delle e-mail con più di 30 allegati e/o più di 50 destinatari.
  - in particolari situazioni, ad esempio massicce ricezioni di e-mail infette, il Servizio tecnologie dell'Informazione si riserva di bloccare e cancellare le e-mail che contengano particolari allegati o che abbiano nell'oggetto o nel corpo del messaggio particolari parole e/o frasi riconducili alla violazione di sicurezza o a codice pericoloso.

Al fine di garantire il corretto funzionamento della posta elettronica aziendale e di evitare la proliferazione del traffico indebito – che in termine tecnico viene chiamato SPAM – l'Azienda ha in uso un sistema AntiSPAM che filtra tutta la posta gestita. Il sistema AntiSPAM utilizza regole euristiche per decidere l'inoltro o meno di un messaggio. Le regole di filtraggio possono causare:
- il passaggio di SPAM qualora non sufficientemente selettive;
- il mancato inoltro di posta elettronica erroneamente giudicata dal sistema come SPAM.

Per le ragioni sopra indicate si vieta l'utilizzo della posta elettronica di materiali in copie uniche o comunque per l'invio di comunicazioni di cui debba essere garantito l'inoltro al destinatario.

- l'Azienda favorisce la condivisione di indirizzi di posta elettronica fra più utilizzatori mediante l'adozione di cosiddette "maling list", cioè di gruppi di indirizzi;
- l'Azienda non fornirà indirizzi di posta elettronica aziendali per usi di tipo personale, ma non vieta la consultazione del contenuto di indirizzi di tipo personale, anche dall'interno dell'azienda, qualora la modalità di consultazione di tali informazioni sia compatibile con i

vincoli di sicurezza del sistema aziendale e ciò avvenga in maniera non eccessiva e pregiudizievole degli obblighi del lavoratore nei confronti dell'Azienda;

- qualora vengano inviati messaggi di posta elettronica che prevedano che l'eventuale risposta possa essere conosciuta da più persone nell'ambito dell'Azienda, occorrerà rendere edotto di ciò il destinatario;
- fatte salve le limitazioni di cui ai punti precedenti l'Azienda favorisce l'utilizzo della posta elettronica come strumento per la rapida comunicazione fra i dipendenti, fra dipendenti e cittadini, fra pubbliche amministrazioni, purché queste comunicazioni siano parte delle attività istituzionalmente previste e compatibili con le mansioni proprie di ogni operatore; fatte salve le limitazioni precedentemente esposte, alla trasmissione telematica di atti e documenti all'interno dell'Azienda per posta elettronica è riconosciuta la stessa validità della trasmissione per via cartacea; in particolare potranno essere trasmessi atti deliberativi, disposizioni dirigenziali e documenti in genere che non contengano dati sensibili e il cui mancato recapito non ingeneri danni per l'azienda, per i dipendenti o per altri; l'utilizzo della posta elettronica, in questi casi, potrà sostituire completamente l'invio di carta; atti o documenti aventi valenza generale possono essere comunicati a tutti o a grande parte dei dipendenti dell'Azienda; ciò può avvenire tramite l'utilizzo di apposite liste di distribuzione che sono messe a disposizione in posta elettronica; esigenze particolari od occasionali di comunicazione ad un numero di utenti il cui volume o la cui qualità non sia già stata prevista dovranno essere inoltrate dal Servizio tecnologie dell'Informazione;

- a titolo di esempio, senza che questo costituisca un elenco esaustivo, non è consentito:
  - utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni non istituzionali o azioni equivalenti;
  - utilizzare il servizio di posta elettronica per inoltrare catene di S. Antonio, giochi, scherzi, barzellette e altre e-mail avulse dal contesto lavorativo.
  - usare la rete in modo difforme da quanto previsto dal presente documento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete.

Utilizzo dei sistemi di comunicazione in fonia – telefoni fissi, telefoni mobili, ecc… -

- è vietato l'utilizzo personale e non istituzionale del telefono;
- l'Azienda, mediante configurazioni sugli apparati tecnologici, impedisce l'effettuazione di chiamate dalla rete aziendale verso determinate categorie di numeri – ad esempio numeri a pagamento per servizi particolari che si giudicano non interessanti dal punto di vista istituzionale, ecc… -;l'operatore che abbia la necessità di utilizzare, per fini istituzionali, una classe di numeri non abilitata potrà richiedere una specifica abilitazione;
- per fini di controllo della spesa telefonica l'Azienda tiene traccia delle telefonate effettuate – qualora queste inducano un onere economico per l'Azienda; non sono ad esempio tracciate le telefonate in ingresso che sono tipicamente non onerose in termini economici -. Viene registrato:
  - il numero del chiamante;
  - il numero chiamato;
  - la data e ora di inizio della telefonata e la data e ora di fine della stessa

- tutti i log sopra citati vengono conservati dall'Azienda per un anno solare in maniera disaggregata per poter confrontare gli andamenti di costo con i dati aggregati degli anni precedenti; i dati disaggregati dal primo gennaio dell'anno al trentuno dicembre dell'anno potranno essere tenuti fino alla fine di marzo dell'anno successivo per i controlli istituzionali, dopo di che dovranno essere aggregati in maniera tale che possano essere utilizzati per i confronti con i periodi successivi; i controlli verranno effettuati in maniera non nominativa e

aggregata – ad esempio aggregando i dati per edificio o per unità erogante –; qualora i dati evidenzino anomalie tali da giustificare controlli aggiuntivi potranno essere ulteriormente approfonditi; normalmente sarà necessario adottare una gradualità nei controlli che preveda prima il controllo del dato aggregato e la notifica di eventuali anomalie e solo successivamente qualora il problema persista un controllo sui dati disaggregati; qualora l'integrità del sistema tecnologico dell'azienda o la gravità del fatto lo rendano necessario sarà possibile accedere immediatamente al dato disaggregato; qualora possibile, gli approfondimenti sui dati che si rendessero necessari saranno condotti con verifiche a campione; in generale tutte le verifiche dovranno rispettare i criteri della pertinenza e non eccedenza rispetto al fine di controllo amministrativo proprio dell'Azienda; qualora le verifiche portino all'accertamento della violazione delle presenti regole o più in generale all'accertamento di utilizzi impropri, l'Azienda si riserva di adottare le opportune misure disciplinari e amministrative;

- l'utilizzo dei log dovrà in ogni caso essere compatibile con quanto prescritto dal d.lg. 13 maggio 1998, n. 171 "Disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni, in attuazione della direttiva 97/66/CE del Parlamento europeo e del Consiglio, ed in tema di attività giornalistica".
- nel caso in cui sia necessario effettuare comunicazioni telefoniche agli interessati, occorre aver chiesto preliminarmente all'interessato medesimo l'autorizzazione a conferire con chi risponda all'apparecchio. In caso di risposta negativa l'operatore deve chiedere in alternativa un numero riservato;
- occorre fare attenzione a discutere, comunicare o comunque trattare dati personali/sensibili per telefono in presenza di terzi non autorizzati che potrebbero inavvertitamente venire a conoscenza di tali dati.

Ulteriori istruzioni

Utilizzo di fax

- in caso di invio di documentazione a mezzo fax, bisogna prestare attenzione alla corretta digitazione del numero cui inviare il documento e verificarne l'esattezza; qualora vengano trasmessi dati idonei a rivelare lo stato di salute, è opportuno anticipare l'invio del fax avvertendo il destinatario, assicurarsi che il ricevimento avvenga nelle mani del medesimo ed evitare che soggetti estranei o non autorizzati possano conoscere il contenuto della documentazione inviata
- l'apparecchio fax deve essere sempre collocato in luogo non accessibile a terzi non autorizzati

Utilizzo di fotocopiatrice e stampante

- in caso di stampa o duplicazione non riuscite di documentazione contenente dati personali / sensibili, occorre evitare di gettare i fogli nel cestino senza aver provveduto a rendere illeggibile il contenuto dei dati.
- qualora si utilizzi carta riciclata per fotocopie e stampe, occorre sempre accertarsi che non siano accidentalmente riportati dati personali e/o sensibili
- occorre utilizzare con attenzione le macchine fotocopiatrici di ultima generazione che possono scannerizzare e memorizzare il documento, talvolta conservando il file elettronico dello stesso

Tutela del diritto d'autore

Vista la legge 248 del 18/08/2000 relativa alla tutela del diritto d'autore:

- si vieta la riproduzione o la duplicazione con qualsiasi mezzo e a qualsiasi titolo dei programmi informatici e dei manuali a corredo dei programmi, si ricorda infatti che anche i manuali sono

coperti dalla legge sul diritto di autore e possono essere riprodotti solo dietro autorizzazione del titolare dei diritti esclusivi;
- è fatto divieto ad ogni utilizzatore del sistema informativo aziendale, scaricare gestire, in qualsiasi modo trattare dati o informazioni che violino la normativa sulla tutela del diritto d'autore;
- qualora l'operatore nonostante tale divieto infranga tale normativa sarà penalmente e civilmente responsabile del proprio operato sollevando l'azienda da ogni responsabilità.

Servizio deputato ai controlli

Il Servizio deputato ai controlli previsti dal presente disciplinare è il Servizio Tecnologie dell'Informazione.

Facoltà dell'Azienda

Qualora l'Azienda:
- abbia ad accertare manomissioni alle configurazioni del sistema informatico, telematico, telefonico aziendale e/o accessi indebiti allo stesso;
- riscontri diffusioni indebite di informazioni atte a pregiudicare la sicurezza del sistema informatico, telematico, telefonico aziendale o il suo buon funzionamento e/o a permettere ad altri accessi o altri privilegi non dovuti;
- abbia concrete ragioni che portino a pensare che la sicurezza del sistema tecnologico aziendale possa essere minacciata

si riserva il diritto di:
- effettuare controlli specifici tesi ad accertare lo stato dei fatti relativamente all'uso delle attrezzature aziendali;
- disabilitare le autorizzazioni all'accesso e all'uso delle attrezzature aziendali;
- segnalare al responsabile organizzativo situazioni e comportamenti anomali degli operatori.

In caso di problemi inerenti la sicurezza della infrastruttura tecnologica l'Azienda si riserva il diritto di adottare tutte le misure tecniche che garantiscano la gestione della contingenza, ad esempio isolando dalla rete stazioni che siano state infettate da virus che ne pregiudichino il buon funzionamento, aggiornando configurazioni software e/o hardware, ecc… Tutte le azioni messe in atto dovranno essere valutate in una logica di costo/beneficio e dovranno essere improntate ad un criterio di minimizzazione del disservizio.

L'Azienda si riserva la facoltà di sospendere l'accesso ai servizi qualora anche a seguito di segnalazioni rappresentate dal Responsabile Organizzativo sussistano nel tempo reiterate evidenze delle inadempienze da parte dell'operatore.

L'Azienda si riserva la possibilità di interrompere i servizi informatici per le manutenzioni ordinarie e straordinarie e per la gestione dei guasti, impegnandosi tuttavia, nel limite del possibile, ad avvertire preventivamente gli utenti di dette interruzioni.
