REGOLAMENTO PER L'UTILIZZO DEI SISTEMI INFORMATIVI E DI COMUNICAZIONE TELEFONICA

Approvato con determinazione dell'amministratore unico n. 31 del 15/12/2011

Indice

PREMESSA

La tecnologia informatica oggetto di questa policy sono computer, posta elettronica, accesso ad internet, telefoni, telefoni cellulari, assistenti digitali personali, voice mail, stampanti, fotocopiatrici, fax e altri supporti elettronici, attrezzature o strumenti che sono fornite da Afol MB e che va sotto il nome di "sistema informativo" .

A tal fine, si è ritenuto opportuno individuare l'insieme di regole atte a definire il corretto comportamento da tenere nell'utilizzo dei dispositivi e dei servizi a carattere informatico messi a disposizione degli utenti, garantendo la conformità dei sistemi informativi ai requisiti di sicurezza ed alle vigenti normative sulla tutela della privacy.

Art. 1 - Oggetto

Il presente regolamento ha per oggetto i criteri operativi di accesso e utilizzo dei servizi informatici e telematici da parte degli utenti che fruiscono di tali servizi e dei dispositivi hardware ad essi assegnati per l'espletamento delle loro funzioni.

Il rispetto del presente regolamento consente il raggiungimento degli obiettivi della sicurezza dei dati trattati dall'Agenzia in termini di Riservatezza (prevenzione di accessi abusivi o non autorizzati) e integrità (che le informazioni non siano state alterate da incidenti o abusi).

Art. 2 - Uso degli strumenti e dei servizi informativi: modalità di accesso e norme di comportamento

L'uso degli strumenti e dei servizi informativi è indispensabile per assicurare l'efficienza e l'efficacia dell'Agenzia. Tutti gli utenti sono tenuti a mantenere in buono stato di manutenzione e aggiornamento gli strumenti hardware e software loro assegnati ed a osservare le seguenti norme di utilizzo dei servizi.

Il CSI (Centro Sistemi Informativi), al fine di garantire la sicurezza del sistema si riserva la facoltà di sospendere temporaneamente i servizi informatici per effettuare accertamenti e controlli.

Per accedere ai servizi informatici da una postazione di lavoro l'utente è tenuto ad autenticarsi utilizzando un codice identificativo (username) rilasciato dal CSI e una parola chiave segreta (password). Poiché la conoscenza della password può consentire a terzi l'accesso indebito e/o fraudolento alla rete di Afol ogni utente è tenuto ad attenersi alle seguenti regole:

- conservare la propria password con riservatezza e diligenza non cedendola a terzi;
- cambiare obbligatoriamente con periodicità la propria password (massimo ogni sei mesi) utilizzando password alfanumeriche complesse di almeno otto caratteri composte da lettere, numeri e caratteri speciali, evitando di utilizzare parole o informazioni facilmente riconducibili all'utente (per es. numero di targa della propria auto, anno di nascita, ecc);
- non utilizzare credenziali d'accesso (username e password) di altri utenti, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza;

- non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione;
- bloccare la propria postazione prima di allontanarsi dalla stessa, mediante i tasti "ctrl" + "alt" + "canc" ed il successivo click su "blocca computer" o, in alternativa, mediante i tasti "  " + "L".
- installare software o componenti hardware diversi da quelli forniti solo previa verifica di compatibilità ed autorizzazione da parte del CSI;
- prendere tutte le precauzioni necessarie a prevenire l'accesso ai dati salvati in locale sulla postazione di lavoro da parte di persone non autorizzate. L'utente è infatti responsabile di tali dati;
- salvare periodicamente i dati importanti residenti sul proprio PC per evitare spiacevoli inconvenienti, come la perdita dei file causata da guasti hardware o da cancellazione involontaria;

Divieti

- non è consentito l'utilizzo degli strumenti e dei servizi informatici per attività non connesse allo svolgimento delle mansioni lavorative assegnate;
- non è consentito a nessuna postazione di lavoro, fissa o mobile che sia, disinstallare o disattivare sistemi di protezione (antivirus, antispyware, antispam, personal firewall) o aggirare politiche di sicurezza distribuite dal CSI a livello centralizzato.
- E' fatto divieto all'assegnatario cedere anche temporaneamente a terzi l'uso dei beni di cui è in possesso.

Art. 3 - Prevenzione delle infezioni da virus

Su tutti gli elaboratori è mantenuto quindi attivo il software antivirus installato dall'amministratore di sistema, che deve essere continuamente aggiornato. E' fatto assoluto divieto di disattivare e o modificare detto software. Questa regola rappresenta una misura minima di sicurezza imposta per legge. Qualora un incaricato/utente si accorgesse del mancato funzionamento od aggiornamento del software antivirus installato sul proprio elaboratore è pregato di darne immediata comunicazione al Centro Sistemi Informativi.

Art. 4 - Uso dei servizi di comunicazione

Internet, intranet, extranet, posta elettronica e tutto ciò che la tecnologia permette e permetterà di realizzare, sono strumenti fondamentali per assicurare l'efficienza e l'efficacia dell'Agenzia. L'impegno di Afol MB è di svilupparne l'uso capillare e massivo per migliorare la qualità dei servizi e la tempestività della comunicazione sia all'interno dell'Azienda che con gli interlocutori esterni.

A questo scopo Afol provvede a dotare tutti i dipendenti di un'utenza per l'accesso ai servizi di posta elettronica e alla intranet.

Art. 4.1-Posta elettronica

Si premette che tutte le informazioni archiviate negli elaboratori e nei sistemi di comunicazione istituzionale (inclusi documenti, altri files, etc.) sono di proprietà Afol MB. Ciò vale anche per la posta elettronica che, proprio

in quanto equiparata alla corrispondenza epistolare, rappresenta ormai una forma di comunicazione analoga a quella scritta su carta intestata.

L'accettazione e la stretta osservanza del presente Regolamento è condizione essenziale per ottenere l'attribuzione in uso di una casella e-mail da parte di Afol.

Si ricorda che ai sensi e per gli effetti di diverse disposizioni normative (D.lgs. 231/2001, D.lgs. 196/2003, etc.), l'Agenzia è anche obbligata ad effettuare periodicamente controlli ed ispezioni a campione, anche a garanzia della sicurezza e riservatezza dei dati personali oggetto di trattamento.

L'uso dell'indirizzo di posta elettronica assegnato da Afol comporta l'utilizzo del nome dell'agenzia. Il materiale e i contenuti inviati sono diretta responsabilità dell'utente, che deve evitare che propri comportamenti in rete possano ledere l'immagine interna ed esterna dell'ente e/o dei colleghi, o ne possano comportare l'insorgere di qualsiasi tipo di responsabilità (civile/penale/amministrativa ecc).

Occorre inoltre osservare alcune precauzioni per evitare che le mail scambiate arrechino rischi ai servizi informativi aziendali o contribuiscano a diffondere informazioni riservate. A tale scopo ogni utente è tenuto ad attenersi alle seguenti regole:

- Utilizzare i sistemi di posta elettronica istituzionale esclusivamente per ragioni professionali.
- Proteggere la propria cassetta di posta attraverso l'utilizzo di una password alfanumerica complessa possibilmente diversa da quella di accesso al pc, nel rispetto dei requisiti di lunghezza minima e complessità disciplinati nei capitoli precedenti.
- Eliminare senza aprire nemmeno in anteprima ogni e-mail con allegati sospetti specialmente se di dubbia o sconosciuta provenienza.
- Effettuare la manutenzione della casella di posta eliminando i messaggi non più attuali e contenenti allegati di grandi dimensioni e archiviando i messaggi di posta dalla cassetta su server (se posseduta) alla propria casella sita sulla propria postazione di lavoro; ciò renderà maggiormente efficienti le prestazioni del sistema di posta elettronica.
- In caso di assenze prolungate attivare un messaggio automatico che indichi il periodo di assenza ed eventualmente un altro riferimento al quale inviare i messaggi di lavoro urgenti.
- In caso di assenza non programmata, su richiesta di un responsabile, l'utente interessato autorizza l'amministratore di sistema a ripristinare la propria password di accesso e a comunicarla al predetto responsabile al fine di rendere possibile la lettura esclusivamente dei messaggi necessari a garantire la continuità del servizio.
- E' opportuno apporre la propria firma in calce ad ogni e-mail secondo gli standard definiti dall'Ente in modo da essere sempre chiaramente identificabili ed agevolare le comunicazioni anche telefoniche.
- Utilizzare il servizio nel pieno rispetto del Codice in materia di protezione dei dati personali.

Divieti

- Sono vietate pratiche di spamming, cioè di invio e diffusione di grandi quantità di messaggi indesiderati (messaggi a catena, inserimento di utente e password nei messaggi, ecc.). L'inoltro di messaggi non sollecitati (ad esempio informazioni, avvisi, notizie etc.) deve essere attentamente valutato.
- E' vietato aprire mail di pishing (adescamento) poiché all'interno di esse è celato del software malevolo in grado di compromettere il corretto funzionamento del pc. Tali mail sono identificabili facilmente dal fatto che spesso sono inviate da un simil operatore bancario / finanziario o postale a utenti che non hanno mai avuto rapporti di alcuna natura con il reale operatore.

- E' vietato l'invio di mail con allegati di dimensioni rilevanti o a un numero elevato di destinatari perché ciò può compromettere l'efficienza del servizio attraverso un sovraccarico dei server. Qualora fosse necessario spedire un messaggio di grosse dimensioni a più di dieci persone è opportuno richiedere la creazione – anche temporanea – di una lista di distribuzione.
- E' tassativamente vietato l'utilizzo di un linguaggio non conforme alle comuni regole della buona educazione nelle comunicazioni via mail, siano esse interne o esterne. Sono vietati insulti, improperi, espressioni oscene, frasi a chiaro riferimento sessuale, anche nelle comunicazioni a carattere ufficiale, e qualunque altra espressione volta a ledere la dignità personale, il buon nome dei collaboratori interni ed esterni, dell'Ente e di qualunque altra persona fisica o giuridica con la quale si entri in contatto.
- Altresì è fatto divieto, in quanto illecito penalmente perseguibile, di inviare mail con link a siti a carattere pedopornografico e di allegare file multimediali della stessa natura, e comunque qualunque contenuto violi norme civili, amministrative o penali di diritto nazionale, comunitario ed internazionale
- È fatto divieto di utilizzare i sistemi di posta elettronica istituzionale per sollecitare o fare proseliti per finalità commerciali, di propaganda in favore di organizzazioni esterne, catene di lettere, ovvero per altre finalità estranee all'attività istituzionale.
- È fatto divieto di tentare di rappresentare la posizione di Afol MB, mediante l'uso di sistemi di posta elettronica istituzionale, su qualsiasi questione di carattere pubblico attraverso forum di discussione e devono porre in essere ogni sforzo per salvaguardare l'immagine pubblica dell'Azienda.
- È fatto divieto di utilizzare i sistemi di posta elettronica istituzionale per scopi personali, di carriera, o di profitto individuale, ovvero per sollecitare un affare estraneo all'attività dell'organizzazione.
- È fatto divieto di utilizzare i sistemi di posta elettronica istituzionale per inviare o ricevere materiali protetti dal diritto d'autore, segreti commerciali, informazioni finanziarie proprietarie, o altro materiale appartenente ad organizzazioni diverse dall'ente, salvo che tali attività costituiscano parte integrante di doveri verso i cittadini. La mancata osservanza del diritto d'autore ovvero di accordi di licenza può condurre ad azioni disciplinari dell'organizzazione ovvero ad azioni legali dei legittimi titolari del diritto d'autore.

Art. 4.2-Programmi di messaggistica istantanea e social networking

Tra gli strumenti messi a disposizione da Afol MB ai propri collaboratori interni ed esterni vi sono strumenti di messaggistica istantanea quali Windows Messenger, Google Talk, Yahoo Chat, Facebook e similari che permettono lo scambio di comunicazioni e files in maniera immediata.

L'utilizzo di tali strumenti – ai quali è in genere associato un account di posta elettronica – è disciplinato in maniera identica in tutto e per tutto all'utilizzo della posta elettronica.

E' fatto tassativo divieto associare un qualunque account del dominio @AFOLMONZABRIANZA.IT a qualsiasi strumento di messaggistica istantanea e/o chat e/o socialnetworking.

Pertanto la registrazione a tali servizi a carattere semi professionale – su tali strumenti è possibile rimanere in contatto con tecnici specialisti di settore ma anche con amici e parenti – è consentita solo con l'utilizzo di un account personale non riconducibile in alcun modo ad Afol e accettando le norme comportamentali previste per la posta elettronica, poiché, in qualità di pubblici dipendenti, si è tenuti a una condotta che non leda in alcun modo il buon nome e l'immagine propria, dei colleghi e dell'ente.

Per i forum, le newsletter e i newsgroup a carattere professionale è concessa la registrazione con account del dominio @AFOLMONZABRIANZA.IT a condizione che il gestore sia pubblicamente noto come operatore professionale.

Il personale ha la responsabilità di salvaguardare e migliorare l'immagine pubblica dell'Ente e di utilizzare la posta elettronica per finalità legittime ed etiche in stretta connessione allo svolgimento delle proprie mansioni. Tutti gli utenti sono responsabili dell'applicazione rigorosa del presente Regolamento. Si ricorda che tutte le informazioni archiviate negli elaboratori e nei sistemi di comunicazione istituzionale sono di proprietà dell'ente, ciò vale anche per gli strumenti di messaging anche non riportante nessun suffisso o segno distintivo.

Art. 4.3-Internet

Afol fornisce accesso alla rete Internet per lo svolgimento dell'attività lavorativa. La navigazione in Internet comporta numerosi rischi che possono minacciare la sicurezza della rete, dei dati e della postazione di lavoro. Per evitare tali rischi l'accesso ad Internet è filtrato e controllato da adeguati apparati di sicurezza.

Al fine di prevenire disservizi e utilizzi impropri della rete, il Centro Sistemi Informativi si riserva di attivare in qualsiasi momento ulteriori filtri che regolino o limitino l'accesso. A tale scopo si provvede inoltre a sottoporre a filtro categorie di siti considerati pericolosi o non correlati con l'attività professionale svolta.

Tenendo conto che l'uso di internet è consentito per lo svolgimento della propria attività lavorativa, l'utente è tenuto al rispetto delle seguenti norme di comportamento:

- per ragioni di efficienza e sicurezza della rete, verificare le dimensioni e la provenienza degli eventuali files (immagini, video, documenti etc.) che si intendano scaricare;
- valutare con attenzione l'opportunità di compilare, fornendo dati personali propri e di Afol, form o moduli disponibili in rete;
- valutare con attenzione l'opportunità di partecipare a forum, blog, social network e community a vario titolo presenti in rete: tali categorie, seppur non espressamente vietate, rientrano in quella tipologia di siti di cui è consentito un uso moderato;
- valutare con attenzione l'opportunità di effettuare l'upload o comunque la condivisione in rete di materiale di cui si disponga per l'esercizio della propria attività lavorativa.
- E' consentito l'uso a fini personali per l'accesso alla propria casella privata di posta tramite il web (cosiddette webmail), con periodicità tale da non inficiare l'attività lavorativa. Le prescrizioni – riportare in questo Regolamento – sui contenuti ed i materiali veicolati tramite rete Internet devono essere rispettate anche con riferimento alla web mail privata, poiché vengono utilizzate risorse messe a disposizione dall'ente.

Divieti

- non è consentito scaricare ed installare programmi non autorizzati che potrebbero danneggiare il sistema ricevente o carpire a qualunque titolo informazioni riservate;
- non è consentito l'accesso e la navigazione se non a mezzo della rete Afol: è pertanto vietato l'utilizzo di chiavette personali e di Internet provider diversi, salvo i casi autorizzati dal direttore di riferimento;
- non è consentita l'effettuazione di transazioni finanziarie a carattere continuativo (remote Banking, acquisti on-line, ecc.), salvo i casi autorizzati dal direttore di riferimento;

- non è consentito scaricare/scambiare materiale informatico privo di licenza o in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
- inoltre è vietato compiere qualsiasi azione tesa ad aggirare o compromettere i meccanismi di protezione dei sistemi informatici;
- è fatto tassativo divieto visualizzare pagine web a carattere pedopornografico e/o scaricare file multimediali della medesima natura. La violazione di tale norma, oltre a far incorrere l'utente nella responsabilità penale disciplinata dalla leggi vigenti;
- è fatto divieto di tentare di rappresentare la posizione dell'ente su qualsiasi questione di carattere pubblico attraverso forum di discussione e devono porre in essere ogni sforzo per salvaguardare l'immagine pubblica dell'organizzazione, fatte salve le eccezioni espressamente autorizzate dal legale rappresentante dell'ente in virtù del carattere pubblico attinente al ruolo rivestito.
- è fatto divieto di utilizzare la rete Internet per scopi personali, di carriera, o di profitto individuale, ovvero per sollecitare un affare estraneo all'attività dell'ente.
- È fatto divieto di utilizzare Internet per immettere in Rete (upload) ovvero ricevere (download) materiali protetti dal diritto d'autore, segreti commerciali, informazioni finanziarie proprietarie o altro materiale appartenente ad organizzazioni diverse dall'organizzazione. La mancata osservanza del diritto d'autore ovvero di accordi di licenza può condurre ad azioni disciplinari del datore di lavoro ovvero ad azioni legali dei legittimi titolari del diritto d'autore.

Art 4.4-PEC (Posta Elettronica Certificata)

La Posta Elettronica Certificata (PEC) è un'estensione della posta elettronica tradizionale, la quale consente di avere un riscontro certo, con valenza legale, dell'avvenuta consegna del messaggio. Allo scopo Afol MB ha istituito una casella PEC (afolmonzabrianza@pec.it), conforme alla normativa vigente, per la ricezione e l'invio di messaggi e allegati che necessitino di riscontro di ricevuta.
Il direttore generale e/o i direttori/responsabili di area autorizzano, tramite incarico scritto, uno o più utilizzatori della PEC, per i quali valgono le regole definite al punto 4.1. All'utilizzatore viene notificata la password per l'accesso al servizio PEC, che dovrà custodire con diligenza e riservatezza.

Art. 5 – Telefonia fissa e mobile, chiavette dati, notebook

Afol provvede a dotare i propri dipendenti degli strumenti di lavoro di ultima generazione che consentono di essere produttivi anche mobilità o senza essere fisicamente presenti presso il proprio ufficio.

L'uso degli strumenti oggetto del presente articolo, rientra nella piena responsabilità dell'utente che, a propria tutela, tiene rigorosamente riservate le proprie credenziali di accesso ai dispositivi fornite.

Tenendo conto che l'uso di tali dispositivi è consentito per lo svolgimento della propria attività lavorativa, l'utente è tenuto al rispetto delle norme di comportamento di seguito descritte.

Art 5.1-Telefoni fissi

Ogni postazione di lavoro è dotata di un telefono fisso di ultima generazione attraverso il quale effettuare chiamate verso gli altri telefoni interni dell'ente. Su richiesta del Direttore responsabile, il Centro Sistemi

Informativi può abilitare gli apparecchi in dotazione ai dipendenti ad effettuare chiamate esterne locali, interurbane, internazionali e verso cellulari. Al fine di controllare la spesa per la telefonia il Centro Sistemi Informativi adotta strumenti di monitoraggio dei costi che comunque garantiscono la privacy dell'utilizzatore.

Art 5.2-Telefoni cellulari

Su richiesta del Direttore responsabile, il Centro Sistemi Informativi dota i collaboratori del richiedente di telefono cellulare in maniera tale che essi siano sempre raggiungibili telefonicamente per far fronte a necessità di servizio la cui urgenza non è prorogabile.
L'utente è tenuto al rispetto delle seguenti norme di comportamento:

- I telefoni cellulari di servizio vengono forniti con sim dell'operatore di telefonia mobile scelto dall'Ente.
- E' pertanto possibile chiamare i numeri telefonici dei dispositivi mobili appartenenti alla RAM (Rete Aziendale Mobile) e quei numeri esterni espressamente e motivatamente autorizzati.
- L'assegnazione di telefono cellulare è subordinata all'accettazione scritta di suddette regole.
- In casi eccezionali, per motivate esigenze di servizio, su richiesta del Direttore responsabile, è possibile provvedere a fornire apparecchi telefonici dotati di sim "open" abilitate a chiamare tutti i numeri fissi e mobili su territorio nazionale.
- In caso di furto o smarrimento del telefono cellulare di servizio l'utente dovrà darne tempestiva comunicazione al competente Servizio unendo alla stessa copia della denuncia all'Autorità giudiziaria e/o ai Comandi delle Forze dell'Ordine competenti ad acquisire le predette denunce. Afol MB provvederà a far bloccare telefono e numero telefonico dal gestore competente. La mancata denuncia prevede la piena e totale assunzione di ogni tipo di responsabilità diretta e indiretta da parte dell'assegnatario del bene. In caso di smarrimento è facoltà di Afol MB addebitare il costo di reintegro del dispositivo smarrito. Medesima facoltà è esercitabile in caso di furto qualora fosse evidente la negligenza o l'omessa diligenza nella condotta dell'assegnatario. (es: furto di un telefono lasciato incustodito in luogo pubblico o privato senza alcuna misura anti effrazione)

Divieti

- E' tassativamente vietata la cessione a terzi, a qualunque titolo, del dispositivo assegnato.
- E' altresì vietato, in presenza di sim "open", effettuare telefonate personali non prefissate dal 46. Il Centro Sistemi Informativi, nel pieno rispetto della normativa vigente in materia di privacy, effettuerà in collaborazione col gestore telefonico, la verifica periodica della spesa di telefonia mobile sia a livello di singolo dipendente sia a livello di macro aggregati.

Art 5.3-Chiavette USB per la connessione a Internet

Su richiesta del Direttore responsabile, il Centro Sistemi Informativi dota i collaboratori del richiedente di chiavette USB che permettono la connessione a Internet dei pc/portatili a cui sono collegate. Tali chiavette hanno un limite mensile prefissato di Gigabyte scaricabili superato il quale non è più possibile navigare fino al mese solare successivo, se ne raccomanda pertanto un uso congruo.

Per tali dispositivi valgono le stesse regole definite per l'uso della posta elettronica e della connessione internet.

In caso di sottrazione, furto, smarrimento del dispositivo, l'assegnatario è tenuto a sporgere immediata denuncia presso le Forze dell'Ordine (Polizia/Carabinieri) e a darne tempestiva comunicazione telefonica al Direttore responsabile e al Settore Sistemi Informativi in modo che si possa provvedere al blocco immediato del dispositivo. Alla comunicazione telefonica dovrà seguire copia cartacea inviata via fax o via mail della denuncia. L'omessa denuncia è fonte di responsabilità oggettiva a carico dell'assegnatario.

E' tassativamente vietata la cessione a terzi, a qualunque titolo, del dispositivo assegnato.

Art 5.4-Palmari, notebook e netbook

Su richiesta del Direttore responsabile, il Centro Sistemi Informativi dota i collaboratori del richiedente dei dispositivi in oggetto. Essi consentono la produttività in movimento oltre a permettere la connessione a Internet e la fruizione dei relativi servizi da qualunque punto geografico ove vi sia una rete wireless disponibile, sia essa pubblica o privata.

I dispositivi portatili sono un facilmente oggetto di furto. Se un incaricato ha necessità di gestire dati riservati su un dispositivo portatile, è necessario salvare i documenti contenenti tali dati con password di protezione, ovvero, in caso di dati particolarmente riservati, è obbligatorio l'utilizzo di un programma di crittografia. In tali circostanze sarà inoltre necessario procedere al salvataggio di backup dei dati in rete, al fine di garantire il loro recupero in caso di dimenticanza della password o di perdita del sistema di decriptografazione.
L'utente è tenuto al rispetto delle seguenti norme di comportamento:

- L'utilizzo di tali dispositivi è consentito solo per l'attività lavorativa. Poiché su di essi sono memorizzati dati inerenti il proprio lavoro è opportuno proteggere tali dispositivi tramite una password di accesso richiesta all'accensione.
- In caso di sottrazione, furto, smarrimento del dispositivo, l'assegnatario è tenuto a sporgere immediata denuncia presso le Forze dell'Ordine (Polizia/Carabinieri) e a darne tempestiva comunicazione telefonica al Direttore responsabile e al Settore Sistemi Informativi in modo che si possa provvedere al blocco immediato del dispositivo. Alla comunicazione telefonica dovrà seguire copia cartacea inviata via fax o via mail della denuncia. L'omessa denuncia è fonte di responsabilità oggettiva a carico dell'assegnatario.
- E' facoltà del Direttore responsabile richiedere in qualunque momento la restituzione dei dispositivi assegnati dandone tempestiva e motivata comunicazione all'assegnatario e al Centro Sistemi Informativi in modo da poter provvedere all'eventuale blocco dei dispositivi da remoto.

Divieti

- E' tassativamente vietata la cessione a terzi a qualunque titolo dei dispositivi assegnati.
- È vietato installare qualsivoglia programma e/o software diverso da quelli installati all'origine dall'amministratore di sistema. E' vietato altresì modificare, alterare e/o eliminare le misure di sicurezza di cui lo strumento è stato dotato.

Art 5.5-Business Key

In linea con i poteri di firma conferiti dal direttore generale ai direttori/responsabili di area, questi sono stati dotati dal Centro Sistemi Informativi di business key per la firma digitale di documenti informatici e per interagire con i servizi on line della Pubblica Amministrazione. Per l'utilizzo della B. K. valgono le regole definite al punto 5.3,

in quanto compatibili, ma è fatta salva la possibilità di utilizzo da parte di personale diverso da quello titolare della B. K. purché sia autorizzato – mediante apposito atto scritto – dal proprio dirigente e purché il documento sia prima firmato in forma cartacea dal responsabile stesso.

Art. 6 - Monitoraggi e controlli

Al fine di garantire la sicurezza degli strumenti e dei servizi informatici e di comunicazione telematica, per effettuare statistiche e prevenire usi impropri, il Centro Sistemi Informativi si avvale di sistemi di monitoraggio e controllo, nel rispetto dei principi di pertinenza e non eccedenza.

I controlli e le verifiche, sia preventive che difensive sui sistemi di posta elettronica e di accesso a Internet sono leciti e, ove normati, dovuti per legge.

In caso di controlli preventivi (controlli di effettivo rispetto di regole) e per accessi dovuti ad esigenze di continuità, il dipendente dovrà essere preavvisato (anche a mezzo informatico o telefonico) al fine di garantire la correttezza e la trasparenza verso il lavoratore. Per i controlli difensivi o richiesti da Pubbliche Autorità (PS, ecc.), ovvero in casi di incidenti che necessitino interventi improrogabili e urgenti, la preventiva informazione può essere omessa, in quanto può compromettere la difesa o l'accertamento di diritti o di responsabilità in giudizio. Nel caso di incidenti di tal natura, l'informazione sarà data a posteriori.

Postazione di lavoro

Il Centro Sistemi Informativi verifica che le postazioni di lavoro mantengano lo standard di sicurezza definito. Il riscontro di eventuali anomalie consente al Settore stesso di adottare tutte le misure correttive necessarie, compreso l'isolamento della postazione di lavoro dalla rete Afol. Nel perdurare di tali anomalie il comportamento verrà segnalato al responsabile della struttura di appartenenza del dipendente e al Direttore d'area.

Nel caso l'utilizzo anomalo sia riconducibile ad un utente non dipendente, il comportamento andrà segnalato alla Direzione Generale per l'adozione degli atti di competenza.

Posta elettronica

I contenuti dei messaggi di posta elettronica, compresi i file allegati, sono riservati. L'accesso ai messaggi e ai file allegati è ammesso solo per casi eccezionali e documentati problemi di sicurezza del sistema su richiesta dell'utente o previa comunicazione all'utente stesso.

Il Centro Sistemi Informativi utilizza strumenti di monitoraggio del traffico che mettono in evidenza situazioni anomale di intensità di carico dei sistemi che ne possano compromettere il funzionamento.

Internet

Il Centro Sistemi Informativi verifica il corretto utilizzo della rete ai fini della sicurezza e l'attività sull'uso della rete Internet. Su richiesta esplicita dell'utente, per lo svolgimento di attività diagnostica, può essere temporaneamente memorizzato e controllato il contenuto di una pagina consultata. Una volta effettuata la verifica, la pagina viene cancellata.

Nel caso l'utilizzo anomalo sia riconducibile ad un utente non dipendente, il comportamento andrà segnalato alla Direzione Generale per l'adozione degli atti di competenza.