36 REGOLAMENTO ICT

36.1 Premessa

L'illecito o anche semplicemente l'inappropriato utilizzo della strumentazione informatica aziendale da parte dei dipendenti può generare in capo all'azienda ed al datore di lavoro una serie di responsabilità sia penali che civili, qualora non si dimostri di aver adottato tutte le precauzioni al fine di evitare il configurarsi delle stesse: basti pensare alla inversione dell'onere della prova che il D.Lgs. 196/2003 prevede in relazione alla adozione di misure di sicurezza idonee o la prova in capo alla Società di cui all'art.6 del D.Lgs.231/2001.

Questo è quanto emerge da un recente impianto normativo e dal relativo orientamento dottrinale, secondo cui il datore di lavoro può rispondere del reato di cui all'art. 40 del codice penale in caso di illecito commesso all'interno dell'azienda da un proprio dipendente, in quanto "non impedire un evento che si ha l'obbligo di impedire, equivale a cagionarlo" ovvero non attivarsi al fine di impedire l'evento illecito posto in essere dal proprio dipendente può equivalere a cagionare l'illecito stesso.

Premesso che l'utilizzo delle risorse informatiche e telematiche della Aziende in generale deve ispirarsi al principio della correttezza e della diligenza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, la Te.Am. Teramo Ambiente S.p.A., recependo quanto prescritto dal Garante della Privacy nel "Provvedimento 1 Marzo 2007 – Lavoro: le linee guida del Garante per posta elettronica ed Internet", ha predisposto un regolamento interno diretto ad evitare che comportamenti, anche inconsapevoli, possano innescare problemi o favorire minacce alla sicurezza dei dati e/o alla liceità dei loro trattamenti.

Tali prescrizioni sono, dunque, formulate principalmente in attuazione del D.Lgs. 196/2003 sulle misure di sicurezza obbligatorie. Giova sottolineare, inoltre, come la recente Legge n. 48 del 18 marzo 2008, "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno", abbia elevato l'informazione, e conseguentemente i dati ed i sistemi elaborativi che la trattano, al livello di bene giuridico di rango costituzionale tanto da far istituire al Legislatore italiano il concetto giuridico di "domicilio informatico" (cfr. art. 615 ter del Codice Penale e art.24 bis del D.Lgs. 231/2001).

Il presente costituisce, altresì, regolamento attuativo delle "linee guida" del Garante della Privacy in tema di utilizzo e controllo degli strumenti elettronici. Scopo del Regolamento è quello di perseguire la duplice finalità della tutela degli interessi produttivi del datore di lavoro e della dignità e riservatezza del lavoratore, individuando un giusto equilibrio tra la libertà e la autonomia operativa del lavoratore stesso e il diritto della

Azienda a tutelare il proprio patrimonio ed i propri beni (materiali ed immateriali) con disposizioni che privilegino la prevenzione alla repressione.

Questo regolamento tiene anche conto del controverso provvedimento del Garante della Privacy "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008" (G.U. n. 300 del 24 dicembre 2008) modificato con provvedimento del 25/06/2009.

Viene, altresì, disciplinato l'impiego dei dispositivi cosiddetti "mobile", come smartphone e tablet in quanto ampiamente diffusi nell'utilizzo personale pienamente introdotti in contesti aziendali. Analogamente viene preso in considerazione il cosiddetto BYOD ("Bring Your Own Device") ovvero la tendenza, sempre più marcata, all'utilizzo di dispositivi personali in ambito aziendale che a fronte di una evidente praticità, induce una quantità di problemi di gestione e di sicurezza dei dati e delle infrastrutture.

Il fattore umano è l'elemento chiave per l'attuazione di un sistema di sicurezza. Affinché le misure di sicurezza individuate siano efficaci, è necessario che tutti pongano la necessaria cura nell'impiego delle protezioni e sviluppino la capacità di partecipare attivamente alla gestione della sicurezza sfuggendo all'errore comune quanto marchiano di centralizzare il processo in capo ad una unica figura o area aziendale.

Inoltre, nell'ottica proattiva del D.Lgs. 231/2001 in cui i cosiddetti reati informatici sono collocati come reati presupposti all'art. 24 bis, l'Azienda deve dotarsi e mettere in atto uno strumento normativo che oltre a definire ruoli e responsabilità nelle modalità di accesso al sistema ICT, assicuri la correttezza e la sicurezza della operatività dei Sistemi Informativi tramite policy e procedure. In particolare, tale strumento normativo, che trova anch'esso espressione nel presente regolamento, deve assicurare:

- il corretto e sicuro funzionamento degli elaboratori elettronici;
- la protezione da software malevolo o comunque pericoloso;
- il backup di informazioni e programmi;
- la protezione dello scambio di informazioni attraverso l'uso di tutti i tipi di strumenti per la comunicazione anche verso terzi;
- il controllo sui cambiamenti che avvengono su elaboratori e sistemi;
- la gestione dei supporti rimovibili;
- obblighi e doveri degli utenti interni;
- il processo di gestione ed il ciclo di vita delle credenziali.

36.2 Definizioni

- *amministratore di sistema:* Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente regolamento vengono considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi;
- *Apps*: Applicazioni per dispositivi mobili che si possono essere rese disponibili / scaricate da diverse fonti, quali app-store on-line correlati a piattaforme dei produttori dei dispositivi, siti pubblici on-line non correlati a specifici produttori, elenchi di applicazioni sviluppate in ambito aziendale;
- *autenticazione informatica:* la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie al fine di garantire la sicurezza dell'accesso;
- *banca di dati:* qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
- *blocco:* la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
- *BYOD* (Bring Your Own Device): approccio per l'utilizzo di dispositivi mobili evoluti in ambito aziendale che prevede che gli utenti dei servizi informativi aziendali possano utilizzare il dispositivo di loro proprietà;
- *comunicazione:* il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- *comunicazione elettronica:* ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;
- *credenziali di autenticazione:* i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
- *diffusione*: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- *dato anonimo:* il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

- *dato personale*: qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- *dato a conoscibilità limitata:* il dato la cui conoscibilità è riservata per legge o regolamento a specifici soggetti o categorie di soggetti;
- *dato delle pubbliche amministrazioni*: il dato formato, o comunque trattato da una pubblica amministrazione;
- *dato pubblico:* il dato conoscibile da chiunque;
- *dati identificativi:* i dati personali che permettono l'identificazione diretta dell'interessato;
- *dati sensibili*: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- *dati giudiziari:* i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
- *disponibilità:* la possibilità di accedere ai dati senza restrizioni non riconducibili a esplicite norme di legge;
- *documento informatico:* la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
- *jailbreaking*: attività effettuata su un dispositivo (generalmente contro le regole/politiche che ne determinano l'utilizzo), al fine di permettere un'estensione dei servizi disponibili;
- *incaricati:* le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- *interessato:* la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
- *firma elettronica:* l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica;
- *firma elettronica qualificata:* la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica;

- *firma digitale:* un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;
- *fruibilità di un dato:* la possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione;
- *Garante:* l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675;
- *gestione informatica dei documenti*: l'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici;
- *misure minime:* il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;
- *parola chiave:* componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
- *posta elettronica:* messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza;
- *profilo di autorizzazione:* l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
- *responsabile del trattamento*: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
- *reti di comunicazione elettronica:* i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;
- *strumenti elettronici*: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

- *sistema di autorizzazione:* l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;
- *smartphone:* uno smartphone è un dispositivo portatile, alimentato a batteria, che coniuga le funzionalità di telefono cellulare con quelle di elaborazione e trasmissione dati tipiche del mondo dei personal computer;
- *tablet*: dispositivi assimilabili per componenti hardware e software agli smartphone, dai quali si distinguono per dimensioni dello schermo, possibile assenza del modulo telefonico, destinazione d'uso;
- *titolare del trattamento:* la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- *trattamento:* qualunque operazione o complesso di operazioni, effettuate anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- *validazione temporale:* il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi;
- *VPN (Virtual Private Network)*: modalità di trasmissione dati in modalità privata (criptata o analogo) su rete pubblica, tipicamente Internet.

36.3 Oggetto e ambito di applicazione

1. Il presente regolamento disciplina le modalità di accesso e di utilizzo dei Sistemi ICT e dei servizi applicativi che, tramite gli stessi, è possibile ricevere o offrire all'interno e all'esterno dell'Azienda.
2. In tal senso la Rete di Te.Am. - Teramo Ambiente S.p.A. è costituita dall'insieme delle risorse infrastrutturali e dal patrimonio informativo digitale posseduto o gestito dalla Società. Per Risorse infrastrutturali si intendono i componenti hardware e software. Il Patrimonio informativo, invece, è l'insieme delle banche dati in formato digitale ed in generale tutti i documenti prodotti tramite l'utilizzo degli strumenti appartenenti alla infrastruttura ICT.
3. Il presente regolamento si applica a tutti gli utenti interni ed esterni che sono autorizzati ad accedere alla Rete aziendale. Per utenti interni si intendono tutti gli Amministratori, i Dirigenti, i dipendenti a tempo indeterminato e a tempo determinato e i collaboratori anche occasionali.

4. Per utenti Esterni si intendono: le ditte fornitrici di software che effettuano attività di manutenzione limitatamente alle applicazioni di loro competenza, enti esterni autorizzati da apposite convenzioni all'accesso a specifiche banche dati con le modalità stabilite dalle stesse, collaboratori esterni e consulenti autorizzati.

36.4 Principi generali, diritti e responsabilità

1. Te.Am. Teramo Ambiente S.p.a. promuove l'utilizzo degli strumenti propri delle tecnologie dell' informazione e della comunicazione (ICT) per il perseguimento delle proprie finalità e della "mission" aziendale.
2. Gli utenti manifestano liberamente il proprio pensiero nel rispetto dei valori e degli obiettivi della Azienda, dei diritti degli altri utenti e di terzi, salvaguardando l'integrità dei sistemi e delle relative risorse, in osservanza di Leggi, norme e obblighi contrattuali.
3. Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina oltre che di legalità. Ogni utente è responsabile civilmente e penalmente del corretto uso delle risorse informatiche, dei servizi applicativi e dei programmi ai quali ha accesso nonché dei propri dati e dai dati trattati per conto dell'azienda.
4. La postazione di lavoro costituita da Personal Computer, periferiche, software di base, software applicativi e connessione alla rete, viene consegnata completa di quanto necessario per svolgere le proprie funzioni; pertanto è vietato modificarne la configurazione senza la previa autorizzazione dell'Amministratore di Sistema.
5. Il software applicativo installato sui Personal Computer è quello necessario all'espletamento dalle specifiche attività lavorative dell'operatore. E', pertanto, fatto divieto di installare qualsiasi programma da parte dell'utente o di altri operatori, senza il previo consenso dell' Amministratore di Sistema. L' utente ha l'obbligo di accertarsi che gli applicativi utilizzati siano muniti di regolare licenza. A riguardo l' Amministratore di Sistema ha facoltà di procedere a verifiche e controlli.
6. Ogni utente è responsabile dei dati memorizzati nel proprio Personal Computer compresi eventuali supporti rimovibili. Per questo motivo egli è tenuto ad effettuare la copia di questi dati secondo le indicazioni emanate dal titolare del trattamento dei dati o suo delegato, sentito l'Amministratore di Sistema.
7. Per ragioni di sicurezza e protezione dei dati e dei sistemi, le attività compiute nella Rete Informatica possono essere soggette a rilevamento e registrazione in appositi file (log) e ed essere ricondotte ad uno specifico account di rete. Tali file, tuttavia, possono essere soggetti a trattamento esclusivamente per fini istituzionali, per attività di monitoraggio e controllo e

possono essere messi a disposizione dell'autorità giudiziaria in caso di accertata violazione della normativa vigente. La riservatezza delle informazioni in essi contenute è soggetta a quanto dettato dal D.Lgs. n. 196/2003.

36.5 Soggetti legittimati all'utilizzo di strumenti ICT

1. L'utilizzo della posta elettronica e l'accesso ad Internet sono accordati al dipendente con la lettera di designazione ad "incaricato" di cui all'art.30 del D.Lgs. 196/2003 e con le relative istruzioni riguardanti anche la sicurezza dei dati;
2. Il Titolare potrà designare uno o più "responsabili", fornendo loro precise istruzioni sui tipi di controllo ammessi e sulle relative modalità;
3. Agli incaricati alla amministrazione e/o alla manutenzione dei sistemi è vietato l'accesso a dati personali presenti in cartelle o spazi di memoria eventualmente assegnati ai dipendenti ed è posto l'obbligo di svolgere esclusivamente le operazioni strettamente necessarie per adempiere al proprio incarico, con divieto di svolgimento di attività di controllo a distanza, anche di propria iniziativa sull'attività dei lavoratori ex art.4 della Legge 20 Maggio 1970, n. 300; ai dipendenti sono resi noti i nominativi ed i compiti dei manutentori.
4. L' Amministratore di Sistema può compiere le operazioni strettamente necessarie per adempiere al proprio incarico come da provvedimento del Garante della Privacy in materia.

36.6 Divieti di utilizzo

Al fine di garantire la funzionalità, la sicurezza ed il corretto impiego degli strumenti elettronici e, al tempo stesso, la protezione della riservatezza dei dipendenti, messa a rischio dalla possibilità di costante monitoraggio offerte dalla tecnologia (es.: profilazioni, comunicazione/diffusione di dati personali, anche sensibili) vengono esplicitate le seguenti limitazioni relative all'utilizzo e alle modalità di impiego delle risorse ICT aziendali

36.6.1 Divieti di utilizzo di Personal Computer

Sono vietati:

1. l'accesso al sistema informatico della Società e il mantenersi all'interno di esso per motivi non lavorativi o non di servizio;
2. l'installazione di programmi personali ulteriori rispetto a quelli forniti dall' Azienda;
3. la modificazione delle configurazioni impostate dall'Amministratore di Sistema;
4. l'utilizzo dei supporti magnetici, ottici o a stato solido, senza preventiva autorizzazione del Titolare, sentito l'Amministratore di Sistema.

36.6.2 Divieti di utilizzo della rete Internet

Premesso che l'azienda adotta un servizio di filtraggio della navigazione Web le cui "black list" vengono continuamente aggiornate, non è consentito:

1. navigare su siti non correlati con la prestazione lavorativa, anche se ancora non inseriti nelle "black list";
2. il download di programmi o di file multimediali (audio, video, etc.), salvo espressa autorizzazione da parte dell'Amministratore di Sistema;
3. la partecipazione a forum, non preventivamente autorizzata, e l'utilizzo di chat line, la partecipazione ad aste on-line (es.: e-bay), fruizione di servizi di e-commerce, etc.;
4. la conservazione di file a contenuto offensivo, discriminatorio, illecito penalmente e civilmente;
5. l'uso per finalità ludiche anche al di fuori dell'orario di lavoro o durante le pause;
6. l'attivazione di strumenti di videochiamata (es.: skype) salvo espressa e motivata autorizzazione del Titolare, sentito l'Amministratore di Sistema;

36.6.3 Divieti di utilizzo della Posta Elettronica

Non è consentito:

1. l'uso della posta elettronica per ragioni non attinenti ai compiti affidati e alla mansione;
2. l'invio o la memorizzazione di messaggi offensivi o discriminatori;
3. l'uso della posta elettronica semplice, ossia senza la integrazione con funzioni di sicurezza come la crittografia o la protezione dei files con password, per documenti riservati o confidenziali;
4. l'uso della posta elettronica per partecipare a dibattiti, forum o mailing list non pertinenti con l'attività lavorativa o, comunque, di contenuto offensivo o discriminatorio.

36.7 Prevenzione dell'utilizzo improprio

1. Gli strumenti informatici, intesi in senso lato, sono di proprietà della Azienda e devono essere utilizzati per fini produttivi e professionali. A ciascun dipendente viene demandata la responsabilità di utilizzare la infrastruttura e le attrezzature (Personal Computer, cellulari, notebook, etc.) nonché gli accessori ad esse connessi, in modo professionale, lecito e sicuro, rispettando le Leggi vigenti, i comuni principi morali ed etici, la privacy e la riservatezza dei dati trattati.
2. Ciascun dipendente è responsabile per l'utilizzo, in violazione del presente regolamento, da parte di terzi, anche se conosciuti o affini, del computer aziendale e, in generale, degli strumenti a lui eventualmente affidati

36.8 Internet

1. Tutti i dipendenti sono tenuti ad utilizzare i servizi di rete esclusivamente nell'ambito delle proprie mansioni di lavoro, secondo direttive circostanziate nella consapevolezza che ogni accesso ad una risorsa può essere facilmente ricondotto alla persona che lo ha effettuato;
2. Tutti i dipendenti devono agire con il massimo livello di professionalità quando operano in Internet evitando di catalizzare o provocare eventi dannosi anche al fine di non ledere l'immagine della Azienda;
3. Vengono, in ogni caso, messe in atto tutte le necessarie precauzioni al fine di evitare che intrusi possano intromettersi, attraverso Internet, nel sistema informatico aziendale (firewall perimetrale) o che attraverso Internet possano essere introdotti virus o altre forme di malware (antivirus centralizzato);
4. E' fatto divieto di abbandonare propria postazione informatica lasciando inserita la propria password (sessione aperta);
5. La connessione Internet deve essere utilizzata per gli scopi ed il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;
6. E' tollerato l'uso privato, purché del tutto occasionale, non prolungato e non interferente nell'attività lavorativa della infrastruttura e dei servizi aziendali di rete ma non delle infrastrutture elaborative e di storage, per le quali è ammesso in forma esclusiva e tassativa un utilizzo in ambito aziendale e professionale;
7. Vengono individuate congiuntamente dal Titolare e dall'Amministratore di Sistema, sentiti i Dirigenti, categorie di siti considerati correlati o meno con la prestazione lavorativa con conseguente configurazione dei sistemi in modo tale da inibire l'accesso ai siti non correlati;
8. Vengono adottati sistemi di filtraggio finalizzati a prevenire la esecuzione di determinate operazioni reputate non attinenti all'attività lavorativa, quali l'upload o l'accesso a determinati siti (inseriti in una black list) e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato);
9. E' vietato fornire a terzi l'accesso alla connessione Internet aziendale senza la esplicita autorizzazione dell'Amministratore di Sistema;
10. E' vietato prestare o cedere a terzi qualsiasi apparecchiatura informatica;
11. Non sono consentiti, salvo specifica ed esplicita autorizzazione dell'Amministratore di Sistema, impieghi di applicazioni cosiddette "portabili" ossia eseguite direttamente da memorie esterne (come Winpenpack, PortableApps, e analoghe).

36.9 Posta Elettronica

1. La Posta elettronica aziendale è uno strumento di lavoro ed in quanto tale resta di esclusiva proprietà della Azienda e deve essere utilizzato esclusivamente per fini professionali in riferimento alle specifiche mansioni attribuite all'utente in ambito aziendale;
2. L'uso della Posta Elettronica Aziendale comporta, da parte dell'utente, l'impegno e la esposizione contestuale del marchio, dell'immagine e dei valori dell'Azienda e, di conseguenza, costituisce una assunzione di responsabilità in tal senso: quando si utilizza la casella di Posta Elettronica Aziendale per comunicare, si rappresenta l'Azienda verso terzi;
3. Non è ammesso l'utilizzo per fini esclusivamente personali della posta elettronica aziendale in uscita, neppure in via del tutto occasionale, non prolungato e non interferente nell'attività lavorativa (cfr. comma precedente);
4. L'utilizzo della casella di posta aziendale in entrata per fini personali è ammesso esclusivamente in via occasionale e non interferente con la attività lavorativa, nel pieno rispetto delle misure di sicurezza contenute nel Documento Programmatico della Sicurezza e del presente regolamento, per contenuti legali, consoni e appropriati. L'utente assume la piena responsabilità dei contenuti che dovesse ricevere nella casella di posta aziendale.
5. Gli accessi alle caselle di posta elettronica devono essere sempre riconducibili ad una persona fisica e, pertanto, ciascun utente deve accedere alla casella email assegnatagli utilizzando in forma esclusiva le proprie credenziali di autenticazione;
6. Sono resi disponibili, in deroga circostanziata al comma precedente, indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, info@teramoambiente.it, ufficioacquisti@teramoambiente.it, segreteriapresidenza@teramoambiente.it etc.), affiancati a quelli individuali con la convenzione <iniziale_nome>.<cognome>@teramoambiente.it;
7. In calce ad ogni email, inserita come "firma", devono essere riportati i dati di recapito del mittente, la funzione aziendale, il logo aziendale con i riferimenti telefonici e la dichiarazione relativa alla riservatezza dei contenuti e avvertimento per i destinatari che i messaggi stessi "non sono di natura personale" e che le risposte possono essere conosciute dalla Società del mittente (Allegato ASDP-150 al DPS);
8. In caso di assenze non programmate (malattia, etc.) che si protraggono per più di 15 giorni lavorativi, il Titolare del Trattamento provvederà, qualora necessario, mediante personale appositamente incaricato (ad es., Amministratore di Sistema; incaricato aziendale per la protezione dei dati, custode delle credenziali), al ripristino della password della casella di posta della persona non disponibile onde accederne ai contenuti. Al rientro dell'interessato verrà riattivata la procedure di rilascio della password esclusiva;

9. In caso di assenza improvvisa o prolungata, se improrogabili necessità di lavoro richiedano la conoscenza dei messaggi di posta elettronica, l'interessato può delegare un altro lavoratore (fiduciario) alla verifica del contenuto di messaggi (con modalità attivata dall' Amministratore di Sistema); il delegato riferirà al proprio Dirigente i "dati rilevanti" per lo svolgimento dell'attività lavorativa.
10. Per quanto ogni server aziendale sia dotato di idonei strumenti di protezione, resta in capo agli utenti la responsabilità della adozione di comportamenti responsabili e di un atteggiamento consapevole verso i rischi derivanti dall'utilizzo di posta elettronica (malware, phishing, spamming) etc.
11. In relazione al disposto del comma precedente, è fatto divieto, agli utilizzatori di posta elettronica di aprire file allegati a messaggi email la cui provenienza risulti incerta o sospetta;
12. Qualora un utente avesse ragione di sospettare la avvenuta introduzione, nel proprio sistema, di codice maligno, è tenuto a scollegare immediatamente il cavo di rete e ad avvisare l'Amministratore di Sistema;
13. Non è consentito l'utilizzo del sistema di posta elettronica in forme che possano tradursi in un danno o semplicemente un disturbo oggettivo arrecato a terzi;
14. E' fatto divieto di consentire a terzi l'accesso e/o l'utilizzo del servizio di posta elettronica aziendale;
15. E' fatto divieto a qualsiasi utente del servizio di posta elettronica di alterare il contenuto delle intestazioni (headers) dei protocolli di comunicazione o di falsificare l'indirizzo email del mittente (spoofing);
16. L'accesso dall'esterno alla propria casella email aziendale è consentito esclusivamente attraverso l'appropriato servizio webmail (www.teramoambiente.it/webmail).

36.10 Utilizzo della LAN e della Intranet

1. Le unità di rete (dischi condivisi, NAS, file server, etc.) sono aree di condivisione di informazioni strettamente professionali e a carattere riservato: in quanto tali non possono in alcun modo essere utilizzate per scopi personali. In queste unità non è consentita la archiviazione di files con contenuti diversi da quelli attinenti alle attività lavorative, neppure per brevi periodi o in via occasionale;
2. Le unità di rete sono oggetto di regolari attività di controllo, amministrazione e salvataggio dati da parte dell'Amministratore del Sistema e/o dagli incaricati da quest'ultimo individuati;
3. Le password di accesso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. E' assolutamente proibito entrare nella rete e nei programmi con le credenziali di altri utenti, fatto che può integrare le fattispecie di accesso abusivo ad un sistema informatico (cfr. art. 615 ter del Codice Penale) e detenzione abusiva di codici di accesso ad un sistema informatico (art.615 quater del Codice Penale);

4. L'Amministratore del Sistema può, in qualunque momento e dandone comunicazione agli eventuali interessati, procedere alla rimozione di ogni file o applicazione che riterrà essere pericoloso per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.
5. I file generati dagli utenti (documenti, immagini, etc.) nell'espletamento della mansione devono essere salvati nelle apposite cartelle di rete indicate dall' Amministratore di sistema e, salvo diversa indicazione, non localmente (Desktop o cartella documenti) al Personal Computer in uso dall'utente stesso;
6. Le copie di sicurezza degli eventuali files di lavoro archiviati, in via eccezionale come da comma precedente, localmente all'elaboratore in uso, sono in capo all'utente;
7. E' in capo a ciascun utente la manutenzione e pulizia, almeno semestrale, dei propri archivi, con la opportuna rimozione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati onde evitare un'archiviazione ridondante;
8. Per ciò che riguarda le stampanti condivise, è cura dell'utente dopo aver effettuato la stampa dei dati, ritirarla prontamente dai vassoi. È buona regola evitare di stampare documenti o file non adatti (dimensioni molto grandi o di formati non supportati) su stampanti condivise.
9. Poiché la banda della rete è una risorsa condivisa e limitata, ogni utente ha in capo la responsabilità di non compiere operazioni (upload o download di file multimediali, invio di mail con allegati molto grandi, ascolto in streaming, etc.) che tendano a monopolizzare la banda passante a discapito degli altri legittimi utenti.

36.11 Utilizzo della postazione di lavoro

1. La postazione di lavoro, intesa come l'insieme di apparecchiature elettroniche quali Personal Computer, monitor, stampanti, scanner etc., affidata al dipendente, è uno strumento di lavoro. Ne consegue che qualsiasi utilizzo diverso da quello previsto non è consentito oltre al fatto che l'uso improprio dello strumento potrebbe compromettere la sicurezza aziendale;
2. L'accesso all'elaboratore è protetto da password la quale deve essere custodita dall'incaricato con la massima diligenza e non divulgata;
3. Non è consentito all'utente di modificare la configurazione impostate sul proprio PC, fatte salve esplicite autorizzazioni dell'Amministratore del Sistema;
4. Non è consentito, al fine di prevenire possibili alterazioni di funzionamento del sistema, installare autonomamente programmi provenienti dall'esterno;
5. Non è consentito l'uso dei programmi diversi da quelli distribuiti ufficialmente dalla Te.Am. Teramo Ambiente S.p.A.

6. Non è consentito, se non previa esplicita autorizzazione dell'amministratore di sistema, installare sul Personal Computer aziendale periferiche hardware proprie o connettere le attrezzature ICT aziendali tra loro o con altri dispositivi (telefoni cellulari, palmari, etc.) di proprietà personale;
7. L'Amministratore di Sistema per l'espletamento delle sue funzioni, in circostanze che ne giustifichino la necessità (minacce alla sicurezza, esigenze aziendali esplicite, eventi disastrosi, controlli difensivi) ha la facoltà accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica (cfr. Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008, pubblicato in G.U. n. 300 del 24 dicembre 2008, modificato con provvedimento del 25/06/2009);
8. Le apparecchiature costituenti la Postazione Di Lavoro devono essere spente prima di lasciare gli uffici o in caso di assenze prolungate dallo stesso. Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo abusivo da parte di terzi;
9. L'installazione sul proprio PC di dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatore, modem, telecamere, etc.), è consentita esclusivamente previa autorizzazione dell'Amministratore del Sistema;
10. È fatto divieto l'accesso simultaneo con lo stesso account da più postazioni di lavoro agli utenti incaricati del trattamento dei dati sensibili, salvo previa autorizzazione da parte dell'Amministratore di Sistema;
11. È fatto obbligo a tutti gli utenti verificare i dati di origine esterna prima di ogni trattamento, avvertendo l'Amministratore del Sistema nel caso siano rilevati virus;
12. Non è consentito il trattamento di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
13. E' fatto obbligo, ogniqualvolta ci si allontana dalla postazione di bloccare la sessione di lavoro (tasto WINDOWS+L) estraendo eventuale hardware di autenticazione.

36.12 Utilizzo di supporti di memorizzazione rimovibili

1. Non è consentito collegare, inserire o utilizzare supporti rimovibili personali se non dietro autorizzazione dell'amministratore di sistema;
2. I supporti eventualmente autorizzati devono essere comunque sottoposti a scansione antivirus;
3. Non è consentito scaricare o comunque salvare i contenuti dei sistemi di elaborazione aziendale su supporti removibili senza autorizzazione sia del Titolare del trattamento sia dell'Amministratore di sistema;
4. I supporti rimovibili contenenti dati personali o sensibili, se non utilizzati, devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al

trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili (cfr. Provvedimento a carattere generale del 13/10/2008). I supporti contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave;

5. Non è consentito scaricare files contenuti in supporti magnetici e/o ottici non aventi alcuna attinenza con la propria prestazione lavorativa;
6. Tutti i files di provenienza incerta od esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo ed alla relativa autorizzazione all'utilizzo da parte dell'Amministratore del Sistema e dei Responsabili di Funzione Aziendale.

36.13 Utilizzo di notebook, netbook e palmtop

1. L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
2. Ai PC portatili si applicano le regole di utilizzo previste per le Postazioni Di Lavoro, con particolare attenzione alla rimozione di eventuali files elaborati sullo stesso prima della riconsegna.
3. I PC portatili Utilizzati all'esterno (convegni, visite in azienda, etc.), in caso di allontanamento, devono essere custoditi in un luogo protetto.

36.14 Utilizzo di dispositivi "mobile"

1. Non è ammesso, per ragioni di sicurezza, il collegamento alla rete LAN aziendale attraverso dispositivi di tipo "mobile" (tablet, smartphone, phablet, etc.);
2. E' vietato l'utilizzo di Internet key "mobile" sui sistemi elaborativi (PC, Notebook, etc.) aziendali;
3. Nel caso in cui il dispositivo venga utilizzato per svolgervi un qualsiasi trattamento di dati personali ex art.4, comma 1, lett a) del D.Lgs.196/2003, è fatto obbligo all'utilizzatore di attivare l'accesso tramite codice ed il blocco automatico del dispositivo;
4. Qualora la funzionalità sia disponibile, è fatto obbligo all'utente di attivare il tracciamento del dispositivo e la possibilità di cancellazione remota dei dati;
5. Sono precluse operazioni di "jailbreaking" (dispositivi Apple) o "root" (dispositivi Android), ovvero analoghe, si dispositivi mobili aziendali;

36.15 BYOD – Bring Your Own Device

- E' ammesso l'utilizzo di dispositivi mobili personali limitatamente all'invio e alla ricezione di email e di documenti non contenenti dati sensibili sotto le seguenti condizioni:
    - L'utente deve comunicare preventivamente al Titolare del trattamento la volontà/necessità di utilizzare il proprio dispositivo;

- L'utente deve attivare meccanismi di blocco dello schermo e di accesso tramite codice nonché, se disponibili, le funzioni di tracciamento del dispositivo e di cancellazione a distanza dei contenuti;
- L'utente deve prestare libero e informato consenso relativamente al fatto che per eventuali indagini difensive (cfr. Legge 7 dicembre 2000, n. 397) ovvero per controlli sulla liceità del trattamento, il Titolare può richiedere integralmente copia dei dati trattati così come la loro cancellazione e la cessazione di utilizzo del dispositivo personale.

- E' precluso, in ogni caso, il ricorso al BYOD con dispositivi sui quali siano stati attuati interventi di jailbreaking o root o analoghi;
- L'impiego di propri dispositivi per lo svolgimento di trattamenti dati aziendali, deve essere esplicitamente autorizzato dal Titolare del Trattamento/Datore di Lavoro, sentito l'Amministratore di Sistema;
- Il collegamento di un dispositivo mobile (tablet /smartphone) aziendale alla LAN è consentito esclusivamente all'Amministratore di Sistema limitatamente ad operazioni urgenti di manutenzione e supporto tecnico e per il tramite di meccansimi e protocolli crittografici;
- Il collegamento di dispositivi mobili (tablet e smartphone) non aziendali alla LAN non è consentito;
- Il collegamento di laptop/notebook/netbook non aziendali (es. notebook personale, consulente, fornitore) alla LAN è deprecato ma consentito in casi residuali e motivati, alle seguenti condizioni:
  - Il Dirigente/Responsabile dell'area avente la necessità ne dà preavviso al Titolare del Trattamento e all'Amministratore di Sistema;
  - L'interessato (i.e. il proprietario/possessore del dispositivo) rilascia il proprio consenso affinchè Te.Am. S.p.A., eventualmente con l'ausilio dell'Amministratore di Sistema, possa verificare l'idoneità dello strumento (assenza di virus e spyware, presenza di antivirus, antispyware e firewall, sistema operativo adeguato ed aggiornato, software registrato regolarmente e dotato di licenza, etc.);
  - Lo strumento risulti idoneo secondo i parametri del punto precedente;
  - Il Dirigente/Responsabile dell'area di riferimento provveda a trasmettere, via email, all'Amministratore di Sistema ed al Titolare la registrazione, almeno, i seguenti elementi essenziali: persona fisica che si collega, dirigenza di riferimento ovvero Alta Direzione, data e ora di inizio collegamento, data e ora di fine collegamento, tipo di dispositivo utilizzato, operazioni rilevanti eseguite, banche dati accedute.

36.16 Accesso alla rete da parte di utenti esterni

1. Affinché un utente esterno venga autorizzato all'uso delle risorse informatiche e dei relativi servizi, è necessario che gli utenti esterni dispongano di un incarico formale;
2. A seguito della richiesta del Dirigente competente, l'Amministratore di Sistema provvederà alla creazione di un account per l'accesso alla rete con i privilegi minimi necessari per l'attività che deve essere svolta.

36.17 Accesso alla rete dall'esterno

1. Non è, in generale, consentito accedere dall'esterno alla rete LAN aziendale ed alle sue risorse: le policy e le regole di sistemi di elaborazione e degli apparati di comunicazione, saranno configurati in tal senso.
2. Qualora insorgesse la necessità di erogare servizi applicativi all'esterno della rete LAN, si dovrà implementare una apposita DMZ (Zona Demilitarizzata) separata dalla rete fidata contenente le banche dati ed i servizi critici ovvero, in alternativa, si ricorrerà ad un servizio di hosting esterno.
3. L'accesso dall'esterno è consentito, esclusivamente tramite tunnel cifrato (VPN) con protocolli allo stato dell'arte, e previo superamento di una procedura di autorizzazione ed autenticazione, all'Amministratore di Sistema ed eventuali manutentori del software applicativo all'uopo autorizzati. In ogni caso tale tipo di accesso può avvenire esclusivamente per finalità manutentive e deve essere registrato nei file di log del server di autenticazione.

36.18 Gestione delle credenziali

1. L'accesso alle risorse informative aziendali deve essere protetto da password o alta misura robusta ed il livello di accesso di ciascun utente disciplinato da un sistema di autorizzazione così come previsto dall'allegato B al D.Lgs.196/2003;
2. Le password di accesso ai sistemi di elaborazione, al software applicativo e alle risorse di rete, sono previste ed attribuite, in forma scritta, dall'Amministratore del Sistema in riscontro a puntuale istanza, in forma scritta, del Dirigente competente. È consentita comunque l'autonoma sostituzione da parte degli incaricati al trattamento con contestuale comunicazione al custode delle password;
3. Le password devono essere modificate al primo accesso e devono essere note solo all'incaricato;
4. Immediatamente dopo aver proceduto alla modifica della password relativamente al primo accesso, l'utente incaricato provvederà a consegnare le password in busta chiusa al Custode delle Credenziali;
5. Agli utenti incaricati vengono impartite dal proprio responsabile istruzioni adeguate affinché adottino le necessarie cautele finalizzate ad assicurare la riservatezza delle proprie password

nonché la diligente custodia di eventuali dispositivi (token) in loro possesso esclusivo e costituenti la componente riservata delle credenziali di autenticazione;

6. La password, è composta da almeno otto caratteri di cui almeno un carattere numerico ed un carattere speciale; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili la parola chiave è modificata almeno ogni tre mesi;
7. La password deve essere immediatamente sostituita, dandone comunicazione al Custode delle Credenziali, nel caso si sospetti che la stessa abbia perso la segretezza;
8. Qualora un utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione o persona dalla stessa incaricata (Responsabile di Funzione, Amministratore del Sistema, Custode delle credenziale);
9. Le credenziali di autenticazione non utilizzate da oltre sei mesi devono essere disabilitate ad eccezione di quelle preventivamente autorizzate per mero scopo di gestione tecnica;
10. Qualora un utente debba assentarsi dal lavoro per un periodo superiore a giorni 15 (quindici) lavorativi, o, in caso di grave necessità contingente che renda indispensabile e indifferibile l'intervento, l'amministratore di sistema, al mero fine di garantire la operatività aziendale e/o la sicurezza del sistema, assicura la disponibilità di dati, strumenti elettronici e risorse assegnati all'utente indisponibili, sostituendo la password e fornendo le credenziali ad un nuovo, temporaneo, incaricato sostitutivo che provvederà alla modifica in corrispondenza del primo accesso a dare comunicazione delle nuove credenziali al custode delle password. Di tale intervento viene informato l'utente surrogato;
11. L'utente è responsabile dell'utilizzo delle proprie credenziali così come delle operazioni che, in virtù della autenticazione tramite esse, vengono compiute.

36.19 Attività di controllo

1. E' fatto salvo il diritto del datore di lavoro di effettuare controlli sull'utilizzo degli strumenti ICT del lavoratore, quando ciò sia dettato:
    a. da esigenze per l'esercizio o la difesa in sede giudiziaria;
    b. da riscontri di gravi inadempienze della prestazione lavorativa;
    c. da oggettivi indizi di commissione del reato;
    d. da esigenze di salvaguardia della vita o dell'incolumità di terzi;
    e. da norme specifiche di legge o dall'autorità giudiziaria;
    f. da esigenze organizzative, produttive, di sicurezza ed il mancato rispetto del presente regolamento che evidenzino comportamenti anomali (evento dannoso, situazione di pericolo, rischi di responsabilità per la Società).

2. La verifica sui comportamenti anomali è effettuata con controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa (o su una certa area);
3. Il controllo anonimo può concludersi con avviso generalizzato sul rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle disposizioni impartite; l'avviso e l'invito sono rivolti solo alla struttura/area/settore in cui è stata rilevata l'anomalia;
4. In assenza di successive anomalie (di norma) non saranno effettuati controlli individuali;
5. Non saranno effettuati controlli prolungati, costanti o indiscriminati.

36.20 Trattamento dei dati con strumenti ICT

1. Al fine di conseguire una corretta gestione dei dati viene definita una gerarchia di conoscibilità sia in termini generali che più specificamente in relazione agli obblighi di Legge derivanti dalla tutela dei dati personali. È quindi necessario procedere ad una classificazione dei dati anche nell'ottica di dover contemporaneamente definire le politiche di accesso agli stessi;
2. La classificazione dei dati è indispensabile nel momento in cui il trattamento avviene tramite l'uso delle tecnologie dell'informazione;
3. Devono, in ogni caso, essere rispettate le Norme sulla tutela dei dati personali, sull'accesso ai documenti amministrativi, sulla tutela del segreto e divieto di divulgazione;
4. La classificazione dei dati costituisce il punto di partenza per determinare come avviene il trattamento dei dati stessi: per quanto tempo sono trattenuti prima di essere distrutti, come sono trattati (dati confidenziali, pubblici, ecc.) e come sono protetti;
5. La classificazione, in generale, avviene in base alle esigenze operative, alla normativa vigente e a tutto ciò che fa parte del "modus operandi" aziendale.

36.20.1 Classificazione dei dati

1. Parallelamente alla individuazione delle tipologie di dato previste dall'art.4 del D.Lgs. 196/2003 (dato personale, dato sensibile, dato giudiziario, etc.) ai fini della pianificazione della sicurezza delle informazioni aziendali si adotta il seguente schema di classificazione in sei classi:
    I. dato pubblico
    II. dato tecnico (dati progettuali o operativi)
    III. dato di tipo amministrativo (contabilità, fatture, ordini);
    IV. dato relativo alle risorse umane (contratti, livelli, permessi, orari, certificati, etc.)
    V. dato riservato
    VI. dato strategico

2. Dal punto di vista dei requisiti di riservatezza si adottano misure diverse a seconda del livello di classificazione:
    I. per il dato pubblico si adottano, quantomeno, le misure minime di sicurezza;
    II. per i dato tecnico si adottano misure di riservatezza superiori al livello 1 mantenendo l'accesso ai soli soggetti cui compete la visualizzazione e abilitando la modifica ad un numero ristretto di soggetti;
    III. il dato amministrativo viene tutelato con misure più stringenti di quelle previste al livello 2 abilitando accesso e modifica esclusivamente alla struttura aziendale competente;
    IV. il dato di livello 4 viene tutelato come il dato di livello 3 con l'aggiunta di ulteriori misure fisiche, tecniche ed informatiche;
    V. Il dato di livello 5 è riservato ai soli vertici aziendali ed è oggetto di speciali misure finalizzate alla riservatezza;
    VI. Il dato di categoria 6 (dato strategico) è riservato ai soli membri del Consiglio di Amministrazione aziendale;

36.20.2 Conservazione dei dati

In ossequio al principio di finalità i sistemi software sono programmati, configurati o utilizzati in modo da cancellare periodicamente ed automaticamente i dati relativi agli accessi ad Internet e al traffico telematico. Eccezionalmente la conservazione può essere protratta, per il tempo indispensabile e per le sole informazioni necessarie, in relazione a:

- esigenze tecniche o di sicurezza particolari,
- indispensabilità dei dati rispetto all'esercizio o difesa di un diritto in sede giudiziaria;
- obbligo di custodire o consegnare i dati per specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

36.21 Amministratore di Sistema

La figura dell'amministratore di sistema è oggetto di uno specifico provvedimento del Garante della Privacy in quanto lo svolgimento delle mansioni di un amministratore di sistema, anche a seguito di una sua formale designazione quale responsabile o incaricato del trattamento, comporta di regola la concreta capacità, per atto intenzionale, ma anche per caso fortuito, di accedere in modo privilegiato a risorse del sistema informativo e a dati personali cui non si è legittimati ad accedere rispetto ai profili di autorizzazione attribuiti.

36.21.1 Designazione

Considerato che i titolari sono tenuti, ai sensi dell'art. 31 del Codice della Privacy, ad adottare misure di sicurezza "idonee e preventive" in relazione ai trattamenti svolti, dalla cui mancata o non idonea predisposizione possono derivare responsabilità anche di ordine penale e civile (artt. 15 e 169 del Codice) e constatato che l'individuazione dei soggetti idonei a svolgere le mansioni di amministratore di sistema riveste una notevole importanza, costituendo una delle scelte fondamentali che, unitamente a quelle relative alle tecnologie, contribuiscono a incrementare la complessiva sicurezza dei trattamenti svolti, e va perciò curata in modo particolare evitando incauti affidamenti, il Titolare è tenuto a individuare solo soggetti che "per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza" (art. 29, comma 2, del Codice). Di conseguenza la attribuzione delle funzioni di amministratore di sistema deve avvenire:

- previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza;
- La designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

36.21.2 Ruolo e compiti

1. Ai fini del presente regolamento, ed in conformità con il Provvedimento del 27 Novembre 2008 successivamente modificato, con la definizione di "amministratore di sistema" si individuano figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti nonché figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi quali i sistemi ERP (Enterprise Resource Planning), le reti locali, gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.
2. Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati. Attività tecniche quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "in chiaro" le informazioni medesime.

3. I principali compiti di un Amministratore di Sistema sono i seguenti:
    - Monitorare l'infrastruttura informatica di competenza attraverso l'analisi dei log, identificando e prevenendo potenziali problemi;
    - Introdurre ed integrare nuove tecnologie negli ambienti esistenti;
    - Installare e configurare nuovo hardware/software sia lato client sia lato server;
    - Applicare le patch e gli aggiornamenti necessari al software di base ed applicativo, modificare le configurazioni in base alle esigenze dell'Azienda;
    - Gestire e tenere aggiornati gli account utente ed i relativi profili di autorizzazione;
    - Fornire risposte alle questioni tecniche sollevate dall'utenza, porre rimedio ai problemi/guasti tramite tecniche di troubleshooting;
    - Pianificare e verificare la corretta esecuzione dei backup e delle repliche;
    - Documentare le operazioni effettuate (Logbook), le configurazioni, le modalità di backup e di ripristino dei dati e dei sistemi, gli eventi e le soluzioni ai problemi;
    - Ottenere le migliori prestazioni possibili con l'hardware a disposizione;
    - Operare secondo le prescrizioni di sicurezza e le procedure interne previste.

36.21.3 Elenco degli AdS

1. Gli estremi identificativi delle persone fisiche Amministratori di Sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.
2. Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, i titolari pubblici e privati nella qualità di datori di lavoro sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Ciò, avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico la cui adozione è prevista dal Provvedimento del Garante n. 13 del 1° marzo 2007 (in G.U. 10 marzo 2007, n. 58); in alternativa si possono anche utilizzare strumenti di comunicazione interna (a es. Intranet aziendale, ordini di servizio a circolazione interna o bollettini). Ciò, salvi i casi in cui tale forma di pubblicità o di conoscibilità non sia esclusa in forza di un'eventuale disposizione di legge che disciplini in modo difforme uno specifico settore.

3. Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare o il responsabile del trattamento devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

36.21.4 Verifica delle attività degli AdS

1. L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari o dei responsabili del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.
2. Devono essere adottati da parte del Titolare del trattamento sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Per Access-Log si intende la registrazione degli eventi generati dal sistema di autenticazione informatica all'atto dell'accesso (o del tentativo di accesso) da parte di un amministratore di sistema o all'atto della sua disconnessione nell'ambito di collegamenti interattivi a sistemi di elaborazione o software.
3. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.
4. Entro il 15 Dicembre di ogni anno, il Titolare del Trattamento in collaborazione con gli Uffici di Staff e di Coordinamento/Direzione Generale - procede, se del caso ricorrendo a personale qualificato esterno debitamente incaricato, redigendo un verbale a dimostrazione dell'avvenuto adempimento

36.22 Formazione

Sono periodicamente previste specifiche attività di formazione ed aggiornamento sulle procedure aziendali di sicurezza informatica per tutti gli utenti interni e, dove rilevante, per utenti terzi;

36.23 Cessazione del rapporto

In caso di cessazione/conclusione del rapporto in essere con l'Azienda l'utente:

- Ha l'obbligo di restituire i beni forniti per lo svolgimento dell'attività lavorativa: PC, Telefoni cellulari, notebook, pendrive USB, etc;
- Ha l'obbligo di riconsegnare integri e completi dati e programmi oggetto della prestazione lavorava;

- Viene destituito da tutte le prerogative di accesso ed utilizzo delle risorse ICT aziendali: in tal senso l'Ufficio del Personale darà pronta comunicazione del personale al fine della tempestiva disabilitazione delle credenziali di accesso.

36.24 Sanzioni

1. La mancata osservanza delle disposizioni del presente regolamento comporta sanzioni, graduate in base alla gravità della violazione in linea a quanto previsto dal contratto collettivo di lavoro applicato;
2. L'irrogazione delle suddette sanzioni non preclude, né pregiudica l'azione giudiziaria del datore di lavoro di denuncia di atti illeciti di rilevanza penale, di risarcimento civile per danni al patrimonio o all'immagine della Società.

36.25 Pubblicazione del regolamento

Il presente Regolamento, viene pubblicizzato:

1. con la consegna di copia ad ogni dipendente autorizzato all'utilizzo degli strumenti elettronici o telematici documentandone l'avvenuta comunicazione con firma per ricevuta;
2. con notifica via email aziendale;
3. affissione sulle bacheche.

36.26 Modifiche ed integrazioni

Il presente regolamento sarà oggetto sistematico di modifiche ed adeguamenti in particolare al fine di mantenere l'allineamento con lo stato dell'arte del progresso tecnico e tecnologico e la massima aderenza alle dinamiche del contesto aziendale. Il procedimento di modifica è il seguente:

1. Qualsiasi Funzione aziendale, nella figura del proprio Responsabile, predispone le proposte di emendamento/integrazione e le trasmette in visione agli altri Responsabili di Funzioni aziendali e all'Amministratore di Sistema;
2. Una volta trasmesso il documento, nello stato di bozza, diviene oggetto di "osservazioni" da ritrasmettere all'Ufficio che ha curato l'istruttoria entro 15 giorni;
3. L'Ufficio Istruente recepisce, sentito l'Amministratore di Sistema, le osservazioni ritenute appropriate e predispone un allegato contenente gli emendamenti rigettati e le relative motivazioni;
4. Il documento, così emendato, con l'allegato degli emendamenti respinti, passa nello stato di "candidato al rilascio" (RC – Release Candidate) e viene inoltrato alle Segreterie per l'inserimento all'Ordine del Giorno del Consiglio di Amministrazione in approvazione;

5. Il testo candidato al rilascio viene analizzato e discusso in Consiglio di Amministrazione ove può essere oggetto di ulteriori modifiche, sentito eventualmente l'Amministratore di Sistema, ed essere approvato o rigettato, tornando in uno degli stadi precedenti con le opportune indicazioni e motivazioni.
6. Iter analogo seguono gli adeguamenti periodici.

36.27 Norme transitorie

Il presente regolamento diviene pienamente efficace a seguito della approvazione dal Consiglio di Amministrazione.