PROTOCOLLO MOG EX D. LGS. 231/2001

USO DEI SISTEMI INFORMATICI

Rev. 00 del 05/12/2016

Rev.	**Motivo revisione**	**Approvato**
00	Prima emissione	Consiglio di amministrazione
		Data: 05/12/2016

1. SCOPO

Scopo del presente protocollo è disciplinare l'uso dei sistemi informatici della Società da parte degli utenti al fine di:

a) Perseguire il rispetto delle normative vigenti in materia e la ragionevole prevenzione delle ipotesi di reato previste dal D.lgs. n. 231/2001 e dei fenomeni corruttivi;

b) Garantire la sicurezza dei sistemi informatici della Società.

Il presente protocollo costituisce altresì regolamento per l'uso della posta elettronica e di internet, a mente del provvedimento del Garante per la tutela dei dati personali (di seguito anche "Garante") del 10/3/2007 e s.m.i.

2. AMBITO

Il presente protocollo ha ad oggetto l'utilizzo dei sistemi informatici della Società e si rivolge a tutti gli Utenti e Amministratori di Sistema.

3. DEFINIZIONI

Si definisce "sistema informatico" un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di "codificazione" e "decodificazione" - dalla registrazione o memorizzazione, per mezzo di impulsi elettronici, su supporti adeguati, di dati, cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare informazioni, costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente. (Cass. pen., sez. VI 14-12-1999 (C.C. 04-10-1999), n. 3067). "Sistema telematico" si ha quando l'elaboratore è collegato a distanza con altri elaboratori.

Per "utente" si intende chiunque al quale sia assegnato in uso un sistema informatico dalla Società, ovvero che abbia accesso alle reti informatica aziendale o a dati, informazioni o programmi pertinenti ad un sistema informatico o alla rete aziendale.

Per "profilo" si intende l'insieme delle autorizzazioni e facoltà concesse dalla Società inerenti all'accesso e/o all'utilizzo di sistemi informatici o telematici, ovvero di reti informatiche interne (es. intranet) o esterne (es. internet) o di programmi, registri, archivi, banche dati della Società o di terzi.

Per "amministratore di sistema" si intende il soggetto così qualificato dal D.lgs. 196/2003 e dal provvedimento del Garante 27/11/2008, e cioè il soggetto al quale è conferito il compito di sovrintendere alle risorse dei sistemi informatici della Società.

4. RESPONSABILITA'

E' responsabilità di tutte le funzioni aziendali coinvolte nelle attività oggetto del presente protocollo osservarne e farne osservare il contenuto e segnalare tempestivamente all'O.d.V. e al R.P.C.T., in ragione delle rispettive competenze, ogni evento suscettibile di incidere sull'operatività ed efficacia del protocollo medesimo (per es.

modifiche normative, mutamenti dell'attività disciplinata, modifiche della struttura aziendale e delle funzioni coinvolte nello svolgimento dell'attività, ecc.), in relazione alla capacità preventiva di reati previsti dal D.lgs. 231/2001 o di fenomeni corruttivi.

È responsabilità del Presidente e del Direttore, o di chi ne fa le veci, curare la conservazione del protocollo e la formazione dei soggetti tenuti ad applicarla.

Ciascuna funzione aziendale è responsabile della veridicità, autenticità ed originalità della documentazione e delle informazioni rese nello svolgimento dell'attività di propria competenza.

5. PRINCIPI GENERALI

Lo svolgimento dell'attività in oggetto deve improntarsi al rispetto delle vigenti disposizioni di legge, nonché dei principi e delle misure di prevenzione dei reati e dei fenomeni corruttivi previsti nel Modello di organizzazione, gestione e controllo, nel Piano Triennale di Prevenzione della Corruzione e Trasparenza.

Al fine di assicurare correttezza e trasparenza, è operata la separazione delle funzioni lungo tutte le fasi del processo, onde consentire una serie di controlli a catena e l'imputazione delle responsabilità per le scelte compiute. Tutte le operazioni relative all'oggetto della presente sono compiute da soggetti identificabili e sotto la supervisione del superiore gerarchico.

La Società è dotata di un regolamento (c.d. "policy") aziendale vincolante per i destinatari. In caso di conflitti tra quanto previsto dal regolamento e quanto previsto dal MOG, troverà applicazione quest'ultimo.

La Società si dota delle misure di tutela dei dati personali a norma delle vigenti disposizioni a tutela dei dati personali, alle quali gli utenti e l'amministratore di sistema sono tenuti ad attenersi.

La Società è in possesso di sistemi informatici (computer, server, reti LAN e wireless, connessioni di linea, routers, ecc…), comprensivi di hardware e software regolarmente licenziati, concessi in uso agli utenti con lo scopo esclusivo di adempiere alle proprie obbligazioni nei confronti della Società in relazione al perseguimento dell'oggetto di quest'ultima. Il loro utilizzo è, quindi, consentito nei limiti di tali finalità.

Tutti i software installati nei sistemi della Società sono e devono essere regolarmente licenziati ed il loro uso si attiene ai limiti delle licenze. Della conservazione della documentazione comprovante la legittimità dell'uso dei software installati è responsabile l'amministratore di sistema; copia delle licenze è conservata presso la Società. L'installazione dei software è riservata all'amministratore di sistema ed è fatto divieto agli utenti di eseguire tali operazioni.

Ogni utente è personalmente responsabile dell'integrità (fisica e funzionale) dei sistemi medesimi, dei dati, delle informazioni e dei programmi ad essi relativi, ed è quindi tenuto ad aggiornare, ove richiesto, i sistemi di protezione (antivirus, firewall, ecc.…) dei sistemi in utenza.

L'accesso ad ogni singolo sistema informatico e telematico è limitato ad uno o più utenti identificati, attraverso la sorveglianza dei locali ed il ricorso a chiavi fisiche (le porte di accesso ai locali sono chiuse a chiave) e logiche (user ID e password). Queste ultime appartengono in ogni caso (anche quando modificate dall'utente) alla Società.

Ad ogni User-ID corrisponde un profilo di accesso ai sistemi informatici, alle reti aziendali e ad internet.

Ad ogni profilo corrispondono l'utilizzo concesso degli applicativi, il limite di accesso al sistema informativo aziendale e le attività consentite (visualizzazione, inserimento dati, modificazione dei dati inseriti). Le User-ID sono assegnate unicamente dall'amministratore di sistema, in accordo con le disposizioni del Direttore, sentito il responsabile di funzione.

Qualora un utente sia in possesso di chiavi di accesso a sistemi informatici non della Società, che egli debba utilizzare nell'ambito delle attività svolte per conto della Società, l'utente è tenuto a:

1) dare informazione al Direttore del possesso di tali chiavi, del titolare esterno di tali chiavi, delle ragioni per le quali esse siano state concesse.
2) conservare le chiavi di accesso con modalità tali da non consentire a soggetti non autorizzati di venirne a conoscenza;
3) fare uso delle chiavi di accesso nei limiti delle autorizzazioni concesse;
4) non appena vengano meno le ragioni per le quali le autorizzazioni di accesso a sistemi informatici esterni siano state concesse, dare comunicazione al terzo concedente della circostanza, e restituire ovvero annullare le chiavi di accesso.

Sarà cura della Società dare comunicazione al terzo concedente della circostanza sub 4), affinché questi assuma i provvedimenti conseguenti.

Può essere data in uso agli utenti una casella di posta elettronica con account personale. L'uso di posta elettronica attraverso questa casella è ad esclusivo scopo istituzionale e mai personale. La posta elettronica in entrata ed in uscita da detta casella deve intendersi come diretta ed inviata da una funzione aziendale e come tale, essa è accessibile ai superiori dell'utente.

Le comunicazioni mediante posta elettronica sono accompagnate dalla seguente iscrizione in calce, anche in lingua inglese:

Avvertenze ai sensi Regolamento Europeo 2016/679

Le informazioni contenute in questo messaggio sono riservate, confidenziali ed a uso esclusivo del destinatario ed è vietata la loro diffusione. Qualora riceveste il presente messaggio per errore e non ne siate destinatari, Vi preghiamo di darcene notizia via e-mail, di astenervi dal consultare il messaggio stesso e gli eventuali file allegati e di cancellare il messaggio dal Vostro sistema informatico. Costituisce comportamento contrario ai principi del Regolamento Europeo 2016/679 trattenere il messaggio, diffonderne il contenuto, inviarlo ad altri soggetti, copiarlo in tutto od in parte, utilizzarlo da parte di soggetti diversi dal destinatario. ALAC S.p.A. garantisce la massima riservatezza dei dati da Voi comunicati; gli stessi saranno trattati in ottemperanza alle normative vigenti. L'interessato può esercitare i propri diritti di soggetto interessato dandone comunicazione all'indirizzo e-mail acquedotto.langhe@acquambiente.it.

ALAC S.p.A. non si assume alcuna responsabilità per eventuali intercettazioni, modifiche o danneggiamenti del presente messaggio e-mail.

È consentito agli utenti accedere ad una casella di posta elettronica ad uso personale su web.

Gli utenti, durante i periodi di assenza, sono tenuti a predisporre messaggi di risposta automatici con i quali si avvisano i mittenti di messaggi di posta elettronica alla casella con dominio aziendale, che questi sono stati ricevuti, ma che non potranno essere letti sino al rientro dell'utente assente e che, pertanto, in caso di urgenza essi dovranno essere inviati nuovamente all'indirizzo del rispettivo responsabile di funzione e/o di progetto.

L'accesso alla rete internet potrà essere limitato mediante ricorso a black list di siti vietati.

È vietato qualsiasi uso dei sistemi informatici per scopi incompatibili con quello per il quale essi sono concessi in uso agli utenti. In particolare è vietato:

- l'uso ludico dei sistemi informatici;
- operare il download, il caricamento o l'installazione di software (musicali, film, foto, programmi, ecc....) non autorizzati e, comunque, in violazione del diritto d'autore;
- rendere in qualsiasi modo noto a terzi non autorizzati, o comunque consentire a questi la conoscenza di dati, informazioni, formule, descrizioni di processi, documenti, materiale di qualsiasi natura, coperto da riservatezza o la cui conoscenza da parte di soggetti terzi potrebbe recare danno alla Società o a terzi;
- produrre, detenere, diffondere, in qualsiasi forma e modo, materiale pornografico, pedopornografico, di propaganda od istigazione a fini terroristici, ovvero offensivo dell'onore o dignità di terzi, o comunque in violazione di legge;
- compiere azioni dirette o strumentali a violare abusivamente sistemi informatici, registri o archivi informatici della Società di terzi, e/o falsificare dati, informazioni o documenti informativi di qualsiasi specie;
- porre in essere una delle condotte previste dal D.lgs. 231/2001, ed in particolar modo dall'art. 24bis, ovvero anche altra condotta strumentale alle medesime.

È altresì vietato, a meno che non sia specificatamente ed espressamente autorizzato, l'utilizzo per scopi personali non ricompresi in quelli sopra elencati.

L'uso dei videoterminali deve essere compiuto in conformità alle prescrizioni del D.lgs. 81/2008, riportate nelle istruzioni operative del sistema di gestione della sicurezza sul lavoro adottato.

I dati e le informazioni relativi alle utenze, al personale, ai clienti e/o ai fornitori, i registri amministrativi, i libri sociali, i dati e le informazioni sulle condizioni economiche, patrimoniali e/o finanziarie della Società hanno carattere riservato e non possono essere divulgati a terzi non aventi diritto, né essere usati per scopi diversi dall'esecuzione delle mansioni assegnate.

La società esegue copie di sicurezza degli archivi informatici, tali da offrire la ragionevole sicurezza, alla luce delle conoscenze del momento, della conservazione della documentazione informatica per il tempo previsto dalle norme vigenti.

Nei limiti della normativa vigente, il responsabile della funzione, il Direttore, l'amministratore di sistema, sono autorizzati dalla Società e dagli utenti, con la sottoscrizione del presente protocollo, ad accedere ai sistemi informatici e a prendere cognizione dei dati, programmi, informazioni, messaggi di posta elettronica ad essi

pertinenti, ai fini di garanzia della continuità dell'attività d'impresa, di manutenzione e di tutela della sicurezza dei sistemi medesimi (operazioni di tutela).

Con specifico riguardo alla posta elettronica, nel caso di assenza programmata, l'utente può indicare con comunicazione scritta al Direttore un dipendente suo fiduciario, per l'apertura della posta elettronica destinata all'account personale. In tal caso l'accesso alla posta elettronica è consentito esclusivamente a quest'ultimo.

Sempre nei limiti delle normative vigenti, il responsabile della funzione, il Direttore e/o l'amministratore di sistema compiono verifiche periodiche direttamente sui sistemi informatici in ordine al loro corretto impiego, al rispetto delle prescrizioni contenute nel presente protocollo ed ai fini di prevenzione dei reati per i quali trova applicazione il D.lgs. 231/2001 (operazioni di controllo). Le operazioni di controllo sono effettuate preferibilmente alla presenza dell'utente.

Tutta la corrispondenza con l'O.d.V. e con il R.P.C.T. è sempre riservata e non potrà essere aperta, né visionata, se non da costoro.

Chi svolge operazioni di tutela o di controllo è tenuto a conservare il riserbo e a non divulgare a terzi le informazioni o dati, riservati, ovvero personali o sensibili ai sensi del D.lgs. 196/2003, relativi all'utente o terze persone delle quali vengano a conoscenza nel corso delle operazioni effettuate, purché non siano esse stesse pertinenti ad un reato, ovvero ad un illecito ai sensi del codice disciplinare della Società. Le informazioni raccolte nel corso delle operazioni di controllo, o comunque lecitamente apprese anche casualmente dalla Società, possono essere utilizzate nell'ambito di procedimenti disciplinari a norma del codice disciplinare della Società, ovvero per la tutela giurisdizionale della Società o di terzi, davanti a corti nazionali o estere o arbitrati di qualsiasi specie.

La Società può revocare, in tutto o in parte, l'uso dei sistemi informatici, ovvero impedire, in tutto o in parte, l'accesso ad internet ad uno o più utenti (p.es. facendo uso di filtri). I poteri di revoca e le politiche di limitazione all'uso dei sistemi informatici e telematici (accesso alle reti Internet ed intranet, all'uso della posta elettronica, ecc….) spettano al Direttore.

Con la sottoscrizione del presente protocollo, tutti gli utenti accettano espressamente ed aderiscono alle prescrizioni contenute nel presente protocollo, comprese quelle concernenti l'utilizzo dei sistemi informatici e quelle relative agli accessi ai medesimi ed ai dati e alle informazioni ad essi pertinenti, nonché all'uso di tali dati ed informazioni, nei limiti qui specificati.

6. PRINCIPI DI CONDOTTA

Le assegnazioni in uso di un sistema informatico o telematico o di un profilo sono richieste dal responsabile di funzione. La richiesta è motivata con riferimento alle attività che l'utente è chiamato a compiere. I profili e l'uso dei sistemi informatici sono assegnati unicamente dall'amministratore di sistema con l'avallo del Direttore, che verifica la compatibilità con le mansioni assegnate e la presenza di eventuali precedenti disciplinari, dietro richiesta del responsabile di funzione o di commessa. I profili assegnati sono registrati e conservati dall'amministratore di sistema e dalla Società.

I sistemi informatici sono concessi in uso mediante consegna da parte dell'amministratore di sistema di "User-Id" e password di accesso al sistema e alle utilities protette (sap, intranet, ecc..). Le password sono conservate dall'amministratore di sistema e dalla Società. Costoro provvedono alla conservazione delle stesse con modalità tali

da non consentire a terzi non autorizzati di venire a conoscenza delle password. Le password e le ID appartengono in ogni caso alla Società.

Con la concessione in uso di un sistema informatico e/o l'assegnazione di un profilo, ovvero la modifica del medesimo, l'utente riceve il presente protocollo e ne sottoscrive copia per accettazione delle prescrizioni in esso contenute ed autorizzazione senza riserve ai soggetti preposti alle operazioni di tutela e di controllo all'accesso ai sistemi informatici assegnati all'utente nonché ai dati, alle informazioni, ai programmi, alla posta elettronica in esso contenuti o ad esso pertinenti, nonché alla loro conservazione ed utilizzo, nei limiti qui specificati.

L'utente conferisce altresì autorizzazione a prendere cognizione, nelle ipotesi di accesso ai sistemi informatici, di dati personali o sensibili presenti nel sistema informatico in uso o ad esso pertinenti, con i soli vincoli di conservarli e di non renderli noti a terzi, se nei casi consentiti dalla legge, ovvero di uso dei medesimi nell'ambito di procedimenti disciplinari a carico dell'utente medesimo o di procedimenti giurisdizionali o arbitrali a tutela della Società o terzi.

Ad ogni cambio di mansione il responsabile di funzione dell'utente e/o il responsabile di commessa, comunica la necessità del cambio di profilo all'amministratore di sistema, il quale provvede alla revoca immediata del precedente profilo. Per l'autorizzazione ed assegnazione di un nuovo profilo si applicano le prescrizioni precedenti.

Si procede all'immediata revoca di User-Id e profilo, con le modalità sopra descritte, nel caso di interruzione del rapporto con la Società. Si applica il Protocollo "Personale".

I profili sono soggetti a revisione periodica.

Il responsabile di funzione o il Direttore autorizzano l'accesso ai sistemi informatici in uso agli utenti al medesimo sottoposti, ai fini di garantire la continuità dell'attività a questi spettante, nei casi di assenza non programmati e non giustificati dall'esercizio del diritto di sciopero o altri diritti sindacali. Il responsabile di funzione e/o il Direttore chiedono all'amministratore di sistema l'assegnazione di un profilo provvisorio limitato allo scopo. L'operatore in sostituzione è nominativamente identificato ed agisce sotto la supervisione del Direttore o di un suo delegato. È fatto divieto all'operatore in sostituzione di divulgare a terzi ogni informazione relativa all'utente appresa nel corso dell'attività svolta in sostituzione di questo e, in particolare, di far uso o visionare l'account di posta elettronica dell'utente. Gli utenti con la sottoscrizione del presente protocollo, autorizzano gli accessi in loro sostituzione qui descritti ai sistemi informatici loro concessi in uso.

La manutenzione di sistemi informatici (sw ed hw) è responsabilità dell'amministratore di sistema, il quale supervisiona altresì l'opera di eventuali fornitori esterni. L'utente con la sottoscrizione del presente protocollo, autorizza altresì il manutentore ad avere accesso al sistema informatico e ai dati personali in esso contenuti. Il manutentore è vincolato – se esterno alla Società, con apposito contratto – alla riservatezza sui dati, informazioni, programmi inerenti ai sistemi informatici in manutenzione, nonché al rispetto dei principi del modello di organizzazione, gestione e controllo della Società. La violazione di tali obblighi comporta la sanzione previste dal codice disciplinare.

Nel caso in cui si affidino a fornitori esterni attività di manutenzione o di supporto nell'uso dei sistemi informatici o di elaborazione o trattamento, per conto della Società, di dati o informazioni, pertinenti ai sistemi informatici della Società, ovvero si affidino attività che implichino o possano implicare accesso ad archivi, a registri, a libri della Società, o dati o informazioni personali, sensibili o riservati per loro natura o a seguito di impegni assunti dalla

Società, questi fornitori sono vincolati al rispetto di obblighi di riservatezza e dei principi previsti dal modello di organizzazione, gestione e controllo della Società.

Chi svolge l'attività di manutenzione che venga a conoscenza di attività illecite operate sul sistema informatico in manutenzione è tenuto a informarne il D.G, ovvero il Presidente della Società, l'O.d.V. e il R.P.C.T.

La violazione di tali obblighi comporta la sanzione previste dal codice disciplinare.

7. NORME RELATIVE ALL'AMMINISTRATORE DI SISTEMA

L'amministratore di sistema è nominato dal Direttore, preferibilmente tra i dipendenti.

La nomina deve ricadere su persona dotata dei requisiti previsti dalle disposizioni del Garante (capacità ed affidabilità nel rispetto delle norme vigenti).

La nomina è fatta con atto scritto indicante puntualmente le attività a questo assegnate, alla luce del presente protocollo e delle ulteriori esigenze operative della Società. La nomina scritta è conservata dall'amministrazione e messa a disposizione del Garante, a richieste di questo. Il suo nominativo è comunicato all'O.d.V., al R.P.C.T. e a tutti gli utenti.

L'amministratore di sistema opera, con password nominative nelle funzioni di a) utente; b) amministratore di rete; c) amministratore del sistema informatico.

L'attività dell'amministratore di sistema è tracciata mediante la registrazione dei file di log, a norma del provvedimento del Garante 27/11/2008 s.m.i. I file di log sono registrati e conservati per un massimo di 12 mesi, con modalità tali da assicurarne completezza, inalterabilità e verifica della loro integrità. Le registrazioni devono comprendere i riferimenti temporanei, la descrizione dell'evento e l'identificazione dell'amministratore di sistema.

L'amministratore di sistema riferisce periodicamente al Direttore, all'O.d.V. e al R.P.C.T., delle operazioni di tutela e di controllo svolte e dei loro esiti.

8. ITER OPERATIVO

A. CREAZIONE di NUOVO PROFILO.

Il responsabile della funzione inoltra all'amministratore di sistema la richiesta di creazione di un'utenza informatica, specificando se per l'utente è già disponibile un sistema informatico. Con la richiesta indica, con il maggior grado di dettaglio possibile, le mansioni assegnate all'utente, nonché della necessità o meno di avere accesso alle reti informatiche interne e/o esterne, di una casella di posta elettronica.

L'amministratore di sistema trasmette quindi richiesta di autorizzazione all'attivazione al Direttore, il quale verificata la coerenza con il mansionario per il quale l'utente è stato assunto ed i precedenti disciplinari, autorizza l'assegnazione. Con l'autorizzazione può disporre il ricorso a filtri e/o blocchi specifici.

Ottenuta l'autorizzazione, l'amministratore di sistema attiva il profilo, assegnando un User-id (immodificabile) e le password necessarie. Attiva altresì contestualmente i blocchi ed i filtri per l'utente. Inserisce l'utente nell'archivio utenze, con il nominativo dell'utente, la User-id, il tipo, la collocazione ed il numero seriale dei sistemi informatici lasciati in uso, il loro indirizzo IP, le mansioni, il profilo assegnato.

L'amministratore di sistema predispone inoltre la modulistica per l'attivazione, contenente il presente protocollo, una dichiarazione attestante l'accettazione delle prescrizioni contenute, nonché le autorizzazioni agli accessi e al trattamento dei dati. L'utenza rimane bloccata fino a che non è ricevuta la sottoscrizione dell'utente.

L'utente, sottoscritte il presente protocollo e le autorizzazioni richieste, prende possesso del sistema informatico, dell'User Id e delle password. Le password sono consegnate in busta chiusa all'amministratore di sistema.

Le password sono soggette a blocco, nel caso di errata digitazione ripetuta, come da regolamento (Policy)

Ogni nuovo utente è tenuto a consegnare e/o annullare le chiavi accesso a sistemi informatici dei quali non sia più autorizzato all'uso.

B. MODIFICHE AL PROFILO

Quando richiesto dal cambio delle mansioni assegnate, ovvero delle esigenze di servizio, si procede alla modifica di profilo.

Si applicano le disposizioni previste per l'assegnazione di un nuovo profilo, con cambio dell'User-ID. Le richieste di assegnazione del nuovo profilo spettano al responsabile della funzione. Il cambio del profilo può avvenire anche per motivi disciplinari. Si applica il codice disciplinare.

C. REVOCA DEL PROFILO

Se la revoca avviene per motivi disciplinari, si applica il codice disciplinare.

Quando si interrompono i rapporti con la Società, il Direttore provvede ad informare con immediatezza l'amministratore di sistema del giorno il cui l'utente non necessita più del profilo. Il profilo è revocato dall'amministratore di sistema il giorno stesso, e la User ID cancellata dal sistema, con la revoca di ogni autorizzazione e facoltà ad essa correlata.

D. *CAMBIO DI POSTAZIONE*, che non comporti mutamenti nel profilo

È richiesto o autorizzato dal responsabile di funzione, sentito se del caso il RSPP. L'amministratore di sistema effettua le verifiche tecniche del caso, sotto la supervisione del RSPP anche in funzione delle prescrizioni del D.lgs. 81/2008.

L'amministratore di sistema aggiorna l'archivio utenze.

E. *RESTITUZIONE* del sistema informatico assegnato

Il sistema informatico assegnato deve essere restituito, quando si interrompe il rapporto con la Società.

In questo caso, si procede all'immediata cancellazione di tutti i dati contenuti nelle memorie del sistema informatico, con la sola eccezione dei casi per i quali il rapporto è stato interrotto in relazione all'uso del sistema informatico. In tal caso si conservano i dati pertinenti ad un reato, ovvero ad un illecito ai sensi del codice disciplinare della Società, nei limiti di tempo e con le modalità consentite dalla legge.

Può procedersi al cambio di sistemi informatici assegnato con il cambio di mansione o di postazione, nonché per motivi di manutenzione. In ogni caso, si procede a disabilitare le password di accesso al sistema

informatico. I manutentori accederanno con loro password, assegnata allo scopo. Conclusa la manutenzione e restituito il sistema informatico, si assegnerà nuova password di accesso provvisoria.

Se il sistema informatico è destinato a nuovo utente, operata la rimozione e restituzione dei dati e delle informazioni di esclusiva pertinenza del precedente utente l'amministratore di sistema procede alla formattazione del sistema informatico ed a rendere questo-disponibile per nuova utenza.

È cura dell'amministratore di sistema l'aggiornamento costante dell'archivio User-ID.

9. SANZIONI

La violazione delle disposizioni qui contenute è sanzionata in base al sistema disciplinare adottato dalla Società ai sensi del D.lgs. 231/2001 e L. 300/1970.

10. NORME DI RIFERIMENTO

D.lgs. 231/2001, disposizioni normative in materia di dati personali e linee guida del Garante marzo 2007, provvedimento del Garante 27/11/2008, L. 300/1970, D.lgs. 81/2008, Codice etico della Società e loro successive modificazioni ed integrazioni.