Energy Auditing S.r.l.

Regolamento per l'utilizzo delle risorse informatiche e telefoniche

(redatto dal U.O. Sistemi Informativi di AMG Energia S.p.a.)

Indice:

- **Premessa**
- **Riferimenti normativi**
- **Definizioni**
- **Dotazione hardware e software**
- **Software aziendale**
- **Telefono aziendale**
- **Rete telematica**
- **Credenziali**
- **Supporti magnetici**
- **PC portatili**
- **Posta elettronica**
- **Internet e relativi servizi**
- **Protezione antivirus**
- **Servizi di supporto**
- **Informativa sul regolamento e sanzioni**
- **Aggiornamento e revisione**

Premessa:

Energy Auditing, di seguito denominata azienda, ha adottato il presente documento per regolamentare l'uso delle risorse informatiche e telefoniche.
Questo regolamento inoltre intende contribuire alla massima diffusione della cultura della sicurezza ed evitare che comportamenti inconsapevoli o erronei possano innescare minacce alla sicurezza nel trattamento dei dati.
Le prescrizioni contenute nel presente regolamento si aggiungono e integrano le specifiche istruzioni contenute nel Documento Programmatico della Sicurezza ed impartite agli utilizzatori tramite le lettere di incarico, in attuazione del D.lgs 196/03.
Nell'applicazione di quanto segue si dovrà tenere conto che le funzioni del U.O. Sistemi Informativi sono svolte dalla AMG Energia S.p.a, per effetto di un contratto di servizio, tra la stessa AMG Energia e la Energy Auditing S.r.l.

Riferimenti normativi:

Costituzione della repubblica italiana - articoli 2, 15, 41.

Codice civile articoli 2086, 2087, 2104.

Codice penale articolo 616.

Legge 20 maggio 1970, n. 300 – Statuto dei lavoratori.

Decreto legislativo 29 Dicembre 1992, n. 518 -Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per l'elaboratore.

Legge 18 agosto 2000, n. 248 -Nuove norme di tutela del diritto d'autore.

Decreto legislativo 30 giugno 2003, n. 196 -Codice in materia di protezione dei dati personali.

Legge 21 maggio 2004, n. 128 -Conversione in legge, con modificazioni, del decreto-legge 22 marzo 2004, n. 72, recante interventi per contrastare la diffusione telematica abusiva di materiale audiovisivo, nonché a sostegno delle attività cinematografiche e dello spettacolo.

Decreto legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale.

Linee guida del Garante per la protezione dei dati personali – provvedimenti a carattere generale Registro delle deliberazioni n. 53 del 23 novembre 2006.

Linee guida del Garante per la protezione dei dati personali – provvedimenti a carattere generale Registro delle deliberazioni n. 13 del 1° marzo 2007.

Definizioni:

Azienda: Energy Auditing S.r.l., azienda del gruppo AMG Energia spa, utilizza i servizi informatici da essa prestati in virtù di apposito contratto di servizio.

Utilizzatore: Il soggetto interno o esterno all'azienda abilitato all'uso degli strumenti elettronici (informatici e telefonici)

Amministratore di sistema: Il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema informativo aziendale con la gestione dei sistemi operativi, degli applicativi, dei data base e del sistema telefonico, unitamente alla gestione e manutenzione degli strumenti elettronici e alla custodia delle credenziali di autenticazione. L'amministratore di sistema è una figura designata da AMG Energia S.p.a. In ambito privacy è la figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti dei dati personali, compresi i sistemi di gestione di basi di dati, i sistemi software complessi quali i sistemi ERP utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentono di intervenire sui dati personali.

Strumenti elettronici: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si svolge l'attività di lavoro.

Responsabile del trattamento dati personali: Il soggetto incaricato dal titolare del trattamento cui competete la designazione degli incaricati del trattamento e la vigilanza sul trattamento stesso.

Dotazione hardware e software:

1. Ogni dispositivo hardware (Personal Computer, Telefono, Stampante ecc.) e software (applicativi aziendali, prodotti di office automation) è assegnato alla azienda che lo utilizza mediante il personale interno per l'esclusivo espletamento del proprio lavoro, pertanto è espressamente vietato utilizzare la dotazione ricevuta per finalità diverse dalla propria attività lavorativa. E altresì vietato replicare sui dischi locali dei PC il software in dotazione o parti di esso senza esplicita autorizzazione del Responsabile del trattamento dati personali e dell'Amministratore di sistema.

2. L'utilizzatore anche temporaneo, è responsabile dell'uso e della custodia delle apparecchiature a lui assegnante e deve adempiere a tale responsabilità ispirandosi al principio della diligenza e correttezza.

3. Il personal computer (PC) affidato all'utilizzatore è uno strumento di lavoro.

4. Non è consentito installare nel PC alcun prodotto software o hardware, tutte le installazioni sono di esclusiva competenza dell'Amministratore di sistema o di suoi

incaricati. A richiesta scritta del Responsabile Tecnico o dell'Organo Amministrativo, su autorizzazione dell' U.O. Sistemi Informativi, l'Amministratore di sistema provvede a consegnare a ciascun utilizzatore le apparecchiature per lui richieste, corredate del software necessario allo svolgimento delle proprie mansioni.

5. Non è consentito modificare le caratteristiche impostate sui PC assegnanti, i punti di rete di accesso e le configurazioni impostate per le reti LAN/WAN dell'azienda.

6. Il PC deve essere spento, salvo avviso contrario da parte dell'ufficio Sistemi Informativi, prima di lasciare gli uffici o in caso di assenze prolungate. In ogni altro caso deve essere effettuata l'operazione di "logoff" dalla rete e dalle applicazioni in uso o attivato il blocco del PC mediante " Blocca Computer" o "screen saver" protetto da password, prima di allontanarsi dalla postazione.

7. Ciascun utilizzatore deve provvedere alla manutenzione dello spazio di memoria del proprio PC mediante la cancellazione dei file obsoleti o non più utilizzati previo salvataggio dei dati, tranne che gli stessi siano duplicati o estratti di altri dati personali già oggetto dei salvataggi aziendali programmati. Tale cancellazione deve essere eseguita almeno con cadenza semestrale.

8. Le informazioni archiviate sul PC devono essere esclusivamente quelle necessarie all'espletamento dell'attività lavorativa. Non è consentita la memorizzazione di documenti informatici di natura privata, oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

9. L'uso delle apparecchiature e della rete informatica aziendale è concesso esclusivamente agli utilizzatori consegnatari limitatamente alla dotazione loro assegnata. E' fatto divieto a persone estranee all'azienda di usare in tutto o in parte le risorse informatiche e telefoniche dell'azienda. È obbligo degli utilizzatori consegnatari, segnalare all' U.O. Sistemi Informativi l'uso improprio da parte di terzi della propria postazione, sia che ne abbiano diretta conoscenza sia che ne abbiano ragionevole sospetto.

10. L'utilizzatore è responsabile dell'uso improprio delle apparecchiature da lui lasciate accese ed incustodite, pertanto quando queste non serviranno dovranno essere disattivate.

11. Le unità periferiche, locali o di rete, devono essere collegate, installate e configurate dal personale dell' U.O. Sistemi Informativi. Ciascuna unità periferica deve essere usata secondo le modalità d'uso indicate dalle apposite istruzioni ovvero secondo le istruzioni fornite dal personale dell' U.O. Sistemi Informativi. Per segnalare eventuali guasti occorre utilizzare il servizio di Helpdesk della intranet aziendale (qualora l'utente sia abilitato) secondo le regole indicate ai successivi articoli 68 e 69 del presente regolamento, o rivolgersi al Responsabile Tecnico.

12. È vietato spostare, disconnettere, riconfigurare le apparecchiature periferiche per qualsiasi ragione. Gli eventuali trasferimenti per causa di servizio devono essere di concerto con il Responsabile Tecnico e coordinati dal personale dell' U.O. Sistemi Informativi, a richiesta dell' Organo Amministrativo.

13. L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, cartucce di inchiostri, toner, floppy disk, CD, DVD) è riservato allo svolgimento del proprio lavoro.

14. In caso di guasto di qualsiasi apparecchiatura in dotazione all'utilizzatore le operazioni di manutenzione, riparazione o sostituzione sono di esclusiva competenza dell' U.O. Sistemi Informativi. Qualsiasi operazione compiuta da altri è ritenuta manomissione e come tale sanzionata.

Software aziendale:

15. Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dall' U.O. Sistemi Informativi (dlg 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore), ne la riproduzione o duplicazione di programmi informatici (Legge n. 128 del 21/05/2004 e successive norme di legge o loro modificazioni)

16. L'utilizzo del software assegnato a ciascun utilizzatore deve avvenire secondo le istruzioni ricevute durante la formazione e secondo le istruzioni fornite dall'help in linea di ciascuno di essi qualora presente. Nel caso di dubbi sul corretto utilizzo o funzionamento dei prodotti software assegnanti l'utilizzatore deve rivolgersi al Responsabile Tecnico o al servizio di Helpdesk dell' U.O. Sistemi Informativi secondo le regole di cui agli articoli 68 e 69 del presente regolamento.

17. Non è consentito scaricare file contenuti in dispositivi di archiviazione esterni (magnetici, ottici) non aventi alcuna attinenza con la propria attività lavorativa.

18. In caso di malfunzionamento del software in dotazione all'utilizzatore le operazioni di manutenzione, correzione o aggiornamento sono di esclusiva competenza dell' U.O. Sistemi Informativi. Qualsiasi operazione compiuta da altri è ritenuta manomissione e come tale sanzionata.

Telefono aziendale:

19. Il telefono aziendale ed il "profilo di utilizzo" (abilitazione per lo svolgimento del traffico telefonico) viene assegnato, a richiesta del Responsabile Tecnico e dell'Organo Amministrativo, dal dirigente dell'area Sicurezza Patrimonio Logistica, a ciascun utilizzatore.

20. L'assegnazione del "profilo di utilizzo" avviene attraverso la consegna di una lettera in busta chiusa contenente un numero identificativo dell'utente ed un codice "PIN".

21. Identificativo utente e PIN devono essere utilizzati e conosciuti esclusivamente dal consegnatario. In caso di smarrimento,dimenticanza o sospetta divulgazione del codice "PIN" l'utilizzatore informa l' U.O. Sistemi Informativi al fine di ottenere un nuovo codice.

22. Del traffico telefonico viene effettuata regolare registrazione e riepilogazione quantitativa mensile. I riepiloghi vengono consegnati mensilmente al dirigente dell' Area Sicurezza Patrimonio Logistica.

23. Ciascun utilizzatore consegnatario del telefono e del "profilo di utilizzo" risponde delle chiamate effettuate con il proprio codice "PIN", nel caso in cui l'utilizzatore si allontani dal posto di lavoro è tenuto a disconnettersi dal telefono mediante l'operazione di "logoff".

24. Non è consentita alcuna manovra tecnica o di spostamento degli apparecchi telefonici e dei loro cavi di collegamento alla rete aziendale. Gli eventuali trasferimenti per ragioni di servizio devono essere richiesti agli uffici aziendali competenti per le manutenzioni (Sistemi Informativi e Sicurezza Patrimonio Logistica).

25. Su richiesta, motivata ai sensi del Dlgs. N. 196/2003, del Responsabile del trattamento dei dati personali di ciascuna area (privacy), da inoltrarsi all' U.O. Sistemi Informativi, possono essere conosciuti i dati del traffico telefonico fino al dettaglio dei singoli numeri chiamati, limitatamente agli ultimi 90 giorni. Il dettaglio del traffico rilevato per il singolo utilizzatore viene consegnato al competente Responsabile del trattamento dei dati personali, il quale ne potrà disporre per quanto consentito e nei limiti del predetto Dlgs. N. 196/2003 .

26. In caso di guasto o malfunzionamento del telefono in dotazione all'utilizzatore le operazioni di manutenzione, riparazione o sostituzione sono di esclusiva competenza degli uffici aziendali per le manutenzioni. Qualsiasi operazione compiuta da altri è ritenuta manomissione e come tale sanzionata.

Rete telematica:

27. La rete aziendale è l'infrastruttura tecnologica che consente la trasmissione dei dati e la loro distribuzione in azienda. Dell'esercizio e della manutenzione della rete è competente e responsabile l'Amministratore di sistema tramite gli uffici aziendali per le manutenzioni.

28. È vietato utilizzare la rete aziendale per fini non espressamente autorizzati. È vietata altresì ogni manipolazione, operazione di natura hardware e software,

intervento tecnico, sostituzione di apparati e apparecchiature appartenenti alla rete aziendale. Nessun intervento di qualsiasi natura e tipo è consentito su qualsiasi apparato e/o strumento tecnico contenuto all'interno degli armadi di distribuzione.

29. Ogni accesso alla rete è protetto da password.

30. La connessione di stazioni di lavoro e/o qualsiasi dispositivo dotato di interfaccia di rete è di esclusiva competenza del personale dell' U.O. Sistemi Informativi.

31. Le unità di rete sono aree logiche di memoria adibite a contenere dati aziendali che si ha interesse a condividere e non possono contenere dati di natura diversa da quelli aziendali. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su tali unità potranno essere svolte regolari attività di manutenzione da parte del personale dell' U.O. Sistemi Informativi senza alcun preavviso agli utilizzatori.

32. È vietato replicare sui dischi locali dei PC dati aziendali, banche dati e documenti sensibili senza esplicita autorizzazione del Responsabile del trattamento dati personali e dell'Amministratore di sistema; quest'ultimo ha il compito di provvedere, per ciascun caso presentatogli, ad indicare le politiche di sicurezza da adottare.

33. Il personale dell'U.O. Sistemi Informativi potrà in qualunque momento, previa autorizzazione dell'Amministratore di sistema, procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del patrimonio hardware e software dell'azienda, dandone comunicazione al responsabile del trattamento dell'area privacy interessata.

34. In caso di guasto o malfunzionamento della rete nella sua parte attiva o passiva le operazioni di manutenzione, riparazione o sostituzione sono di esclusiva competenza degli uffici aziendali per le manutenzioni. Qualsiasi operazione compiuta da altri è ritenuta manomissione e come tale sanzionata.

Credenziali:

35. Le credenziali di accesso, costituite dal "Nome utente" e dalla "password", sono rilasciate dall'Amministratore di sistema, su autorizzazione dell'U.O. Sistemi Informativi, a richiesta dell'Organo Amministrativo.

36. Ad ogni utilizzatore viene assegnato un nome utente ed una password che sono di esclusivo uso personale.

37. La password è segreta, deve essere conosciuta soltanto dal consegnatario e va gestita secondo le istruzioni impartite. Nessun utilizzatore, sia esso amministratore, dirigente o dipendente di grado superiore, coordinato o

subordinato, ha diritto di conoscere le password assegnante ad altri utilizzatori. Nessuna persona estranea all'azienda ha diritto di conoscere le password degli utilizzatori con cui viene a contatto per qualsiasi motivo.

38. Ciascun utilizzatore può accedere ai sistemi usando esclusivamente il nome utente a lui assegnato. Non è consentito ad alcuno utilizzare nomi utenti diversi da quelli assegnanti.

39. La password di logon alla rete aziendale,deve essere cambiata dall'utilizzatore alla scadenza stabilita che viene segnalata dal sistema operativo. Le altre password vengono variate periodicamente dall'Amministratore di sistema.

40. Le password devono rispondere ai criteri di complessità indicati nella lettera di consegna dall'incaricato della custodia delle copie delle credenziali.

41. Nella composizione della propria password e' vietato all'utilizzatore adoperare dati personali (nomi, date di nascita, età,ecc), o dati in qualsiasi modo a lui riconducibili.

42. Nel caso si sospetti che la password abbia perso per qualsiasi ragione la segretezza, l'utilizzatore a ciò abilitato deve cambiarla immediatamente. Se non abilitato al cambio l'utilizzatore dovrà avvisare il Responsabile del trattamento dei dati dell'area privacy interessata, il quale, per impedire tempestivamente intrusioni indebite, provvederà tramite l'U.O. Sistemi Informativi, a richiedere all'Amministratore di Sistema, incaricato al rilascio delle credenziali, l'assegnazione di una nuova password.

43. L'Organo Amministrativo o il Responsabile Tecnico deve comunicare tempestivamente per iscritto all'U.O. Sistemi Informativi ogni variazione riguardante ciascun dipendente con riferimento a cambio di mansione, trasferimento, sospensione, durata e cessazione del rapporto di lavoro.

44. Per il personale assunto a tempo determinato oppure nella qualità di consulenti o collaboratori a qualsiasi titolo, l' Organo Amministrativo o il Responsabile Tecnico all'atto della richiesta delle credenziali, dovrà comunicare all'U.O. Sistemi Informativi la data di inizio e di fine del rapporto intrattenuto con l'azienda.

Supporti magnetici:

45. In caso di riutilizzo o definitivo smaltimento di qualsiasi supporto magnetico (dischetti, cassette, cartucce) contenente dati sensibili l'utilizzatore deve adottare ogni misura utile ad impedire che il loro contenuto venga indebitamente conosciuto provvedendo alla formattazione del supporto magnetico in caso di riutilizzo o alla sua distruzione fisica in caso di smaltimento. L' U.O. Sistemi Informativi fornirà tutte le opportune istruzioni e/o strumenti atti ad attuare quanto previsto dal Garante per la protezione dei dati personali in materia di

smaltimento di supporti magnetici. In ogni caso l'utilizzatore è responsabile della custodia degli stessi, prima, durante e dopo l'uso, nonché della eventuale indebita divulgazione del loro contenuto nei limiti delle responsabilità a lui attribuite ai sensi del Dlg. 196/03.

PC portatili:

46. Il PC portatile deve essere custodito con diligenza dall'utilizzatore assegnatario.

47. Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, inoltre ciascun assegnatario dovrà provvedere alla consegna semestrale del notebook al personale di Sistemi informativi per le attività di verifica e aggiornamento necessarie.

48. Nel caso di furto o smarrimento del PC portatile il consegnatario deve sporgere denuncia all'autorità di polizia e successivamente informare il proprio responsabile per il trattamento dei dati, l'Amministratore di sistema e l' U.O. Sistemi Informativi, allegando alla nota informativa copia della denuncia.

Posta elettronica:

49. L'abilitazione all'uso della posta elettronica aziendale, a richiesta dell' Organo Amministrativo o del Responsabile Tecnico, deve essere autorizzata dall'U.O. Sistemi Informativi e configurata dall'amministratore di sistema.

50. La casella di posta, assegnata all'utilizzatore, è uno strumento di lavoro. L'utilizzatore è responsabile del suo corretto uso che si attua esclusivamente nello svolgimento dell'attività lavorativa.

51. E' vietato utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum, mail-list, social network o altra finalità estranea all'attività di lavoro.

52. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. Il sistema di posta avvisa l'utilizzatore del raggiunto limite di spazio disponibile, che non può essere superato, e delle modalità alternative di cancellazione o eventuale archiviazione dei messaggi.

53. Nel caso di mittenti sconosciuti o messaggi insoliti o qualora l'allegato sia sospetto(file con estensione .exe, .scr, .pif, .bat, .cmd), si devono cancellare i messaggi senza aprirli.

54. E' vietato inviare catene telematiche (ad esempio catene di Sant'Antonio, ecc). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente all'Amministratore di Sistema ed interromperne la diffusione per non

compromettere l'efficienza del sistema di posta aziendale. Non si devono in alcun caso aprire gli allegati di tali messaggi.

55. In calce a ciascun messaggio di posta elettronica per conoscenza degli utilizzatori e dei destinatari verrà automaticamente applicata una nota esplicativa (disclaimer) per informare che le caselle di posta elettronica sono di natura aziendale e destinate ad esclusivo utilizzo aziendale e pertanto esiste la possibilità di accesso ad esse per motivi di emergenza. In tal caso, per garantire la continuità del servizio in assenza dell'utilizzatore ed a richiesta del dirigente dell'area, il responsabile del trattamento dei dati personali può chiedere all'amministratore di sistema una nuova password per l'accesso alla casella da utilizzare temporaneamente al fine di conoscere i dati per i quali si è rilevata la necessità dell'accesso. Esaurita tale operazione l'accesso alla casella verrà bloccato sino al rientro dell'utilizzatore. All'atto del rientro in servizio l'utilizzatore viene informato dall'amministratore di sistema dell' avvenuto accesso alla propria casella nei termini sopra esposti e abilitato ad assegnarsi una nuova password.

Internet e relativi servizi:

56. L'accesso ad internet e ai relativi servizi viene concesso come supporto allo svolgimento della propria attività lavorativa. Non è consentito l'accesso ai siti internet non attinenti alle mansioni affidate.

57. L'abilitazione all'accesso ad internet deve essere richiesta per ciascun utilizzatore dal dirigente dell'area, autorizzata dall'U.O. Sistemi Informativi e configurata dall'Amministratore di sistema.

58. E' vietato all'utilizzatore scaricare software gratuito (freeware) e shareware prelevato da siti internet, se non espressamente autorizzato dall'Amministratore di sistema.

59. E' altresì vietato accedere a flussi streaming audio/video da internet per scopi non istituzionali (ad esempio ascoltare la radio o guardare video o filmati utilizzando le risorse internet).

60. E' vietato all'utilizzatore la registrazione, con la mail aziendale, a siti internet non attinenti alle mansioni affidate.

61. E' vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books, accesso ai social network e altra forma di intrattenimento o gioco telematico.

62. L'azienda, mediante opportuni filtri informatici, attua politiche di navigazione dedicate a singoli o a gruppi di utilizzatori rendendo disponibile l'accesso a siti i cui contenuti sono finalizzati all'attività di lavoro, all'informazione socio culturale,

all'informazione di carattere commerciale alla cronaca con l'esclusione di altri siti i cui contenuti non sono rispondenti a tali finalità.

Protezione antivirus:

63. Ogni utilizzatore in caso di rilevazione di virus segnalata dal software antivirus deve immediatamente sospendere l'attività senza spegnere il computer, e avvisare l' U.O. Sistemi Informativi della segnalazione ricevuta.

64. Non è consentito l'utilizzo di floppy disk, cd, cd riscrivibili, dvd, nastri magnetici di cui sia sconosciuto il contenuto, la provenienza e/o non sia espressamente dichiarato l'autore o l'editore.

65. Ogni dispositivo magnetico di provenienza esterna all'azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus non dovrà essere usato ed il supporto dovrà essere consegnato al personale dell' U.O. Sistemi Informativi.

66. L'eventuale violazione delle norme contenute agli articoli 64,65 e 66 che provochino qualsiasi tipo di danno alla dotazione informatica dell'utilizzatore è ritenuta grave manomissione e come tale sanzionata.

Servizi di supporto (Helpdesk):

67. L'erogazione dei servizi di supporto per le problematiche di tipo hardware e software è realizzata mediante il servizio di Helpdesk dell'U.O. Sistemi Informativi, attraverso procedure informatiche centralizzate sulla intranet dell'azienda.

68. Per ricevere supporto e/o assistenza è necessario che il responsabile tecnico apra apposita chiamata al servizio di Helpdesk indicando la tipologia di problema (hardware, software, DB aziendali ecc) secondo i menù presenti nel form di richiesta assistenza,fornendo una descrizione sintetica del problema e segnalando la persona cui far riferimento.

Informativa sul regolamento e sanzioni:

69. Il presente regolamento deve essere portato a conoscenza di tutti gli utilizzatori delle risorse informatiche e telefoniche aziendali.

70. La violazione delle norme del presente regolamento e ogni atto che in esso è contemplato come manomissione ed è perseguibile e punibile tramite i

provvedimenti disciplinari previsti dal vigente CCNL, ove applicabile, e irrogati con le modalità dallo stesso indicate e, se del caso, secondo quanto sanzionato dalle leggi in ogni tempo vigenti in sede civile e penale.

71. L'irrogazione di qualsiasi tipo di sanzione per condotta illecita dell'utilizzatore non pregiudica gli ulteriori atti diretti al recupero del maggior danno subito dall'azienda per causa delle citate condotte illecite.

Aggiornamento e revisione:

72. Il presente Regolamento è soggetto a revisione con frequenza annuale.