

so co tis

SOCOTIS S.P.A.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL DECRETO LEGISLATIVO N. 231/2001

CODICE ETICO INFORMATICO

PREMESSA

- La progressiva diffusione di nuove tecnologie informatiche e di telecomunicazione, anche in termini di semplicità di accesso, espone SOCOTIS S.p.a. (la Società) a rischi di un coinvolgimento sia patrimoniale sia penale, creando al contempo problemi di immagine e sicurezza.

- Premesso che l'utilizzo delle risorse informatiche e telematiche aziendali deve sempre ispirarsi ai principi di diligenza e correttezza atteggiamenti questi destinati a sorreggere ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro, si ritiene utile adottare regole interne di comportamento comune, dirette ad evitare comportamenti inconsapevoli e/o scorretti.

1. STRUMENTI INFORMATICI AZIENDALI

1.1 Per Strumenti informatici si intendono l'insieme di elementi *hardware* (*computer*, stampanti, palmari, *smartphone*, *tablet* ecc.), *software* e di comunicazione (reti di *computer* locali e geografiche) utilizzati per la gestione delle informazioni in formato elettronico, nonché le informazioni stesse;

1.2 Gli Strumenti informatici aziendali ed i relativi programmi e/o applicazioni affidati al portatore di interesse della Società sono, come è noto, strumenti di lavoro, pertanto:

a) tali strumenti vanno custoditi in modo appropriato;

b) tali strumenti possono essere utilizzati per fini professionali (in relazione, ovviamente, alle mansioni assegnate) e non anche preminentemente per scopi personali, tantomeno per scopi illeciti;

c) debbono essere prontamente segnalati all'azienda il furto, danneggiamento o smarrimento di tali strumenti.

1.3 Ai fini sopra esposti sono, quindi, da evitare atti o comportamenti contrastanti con le predette indicazioni come, ad esempio, quelli qui di seguito richiamati a titolo indicativo.

2. TUTELA DI *PERSONAL COMPUTER, TABLET, SMARTPHONE,* PALMARI, TELEFONO FISSO (di seguito tutti cumulativamente "Strumenti informatici aziendali")

2.1 Onde evitare il grave pericolo di introdurre *virus* informatici nonché di alterare la stabilità delle applicazioni dell'elaboratore, è consentito installare sugli Strumenti informatici aziendali programmi provenienti dall'esterno solo se espressamente autorizzati per iscritto dal Legale rappresentante o dal Responsabile Sistemi Informativi o suo referente o equivalente aziendale (di seguito "i Responsabili");

2.2 Sugli Strumenti informatici aziendali non è consentito l'uso di programmi non distribuiti e/o autorizzati dai Responsabili che valuterà il rispetto degli obblighi imposti dal d.lgs. 29

dicembre 1992, n. 518 e ss.mm. e ii., sulla tutela giuridica del *software* e dalla legge 18 agosto 2000 n. 248, contenente nuove norme di tutela del diritto d'autore e tutte le successive modificazioni o integrazioni;

2.3 Non è consentito utilizzare strumenti *software* e/o *hardware* atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;

2.4 Non è consentito, se non previa autorizzazione dei Responsabili, modificare le configurazioni impostate sui propri Strumenti informatici aziendali;

2.5 Non è consentita l'installazione sugli Strumenti informatici aziendali di mezzi di comunicazione propri (come ad esempio i *modem*, telecamere, sistemi Voip, ecc.);

2.6 Sugli Strumenti informatici aziendali dotati di scheda audio e/o di porte USB o HDMI o assimilate o di lettore CD non è consentito il trasferimento di dati attraverso tali entrate con strumenti personali nonché l'ascolto di programmi, *files* audio o musicali, se non a fini prettamente lavorativi.

2.7 Non è consentito l'utilizzo di postazioni informatiche e di Strumenti informatici aziendali di altro portatore di interesse della Società, salvo l'espressa autorizzazione di quest'ultimo;

2.8 Non è in alcun modo consentito l'utilizzo di *password* di altro portatore di interesse della Società, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione dei Responsabili.

2.9 Utilizzando gli Strumenti informatici aziendali è fatto obbligo seguire le seguenti norme:

a) bloccare o spegnere lo Strumento informatico aziendale, anche attraverso appositi "salvaschermo", ogni qualvolta si renda necessario allontanarsi dalla postazione di lavoro, anche se per pochi minuti;
b) non dare la possibilità ad altri utenti di leggere il proprio lavoro, qualora si stiano trattando dati riservati/sensibili;
c) effettuare regolarmente un *back-up* di tutti i dati/informazioni più importanti;
d) assicurarsi che tutto il materiale (*usb, CD Rom,* ecc.) proveniente dall'esterno sia, sempre controllato dai Responsabili, prima dell'utilizzo, per accertarsi che non contenga *virus*.
e) informare immediatamente i Responsabili per qualunque segnalazione di *virus*.

3. UTILIZZO DI SUPPORTI ESTERNI

3.1 Non è consentito scaricare sugli Strumenti informatici aziendali *files* contenuti in supporti esterni non aventi alcuna attinenza con la propria prestazione lavorativa;

3.2 Tutti i *files* di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo e relativa autorizzazione all'utilizzo da parte dei Responsabili;

4. UTILIZZO DELLA RETE SOCIETARIA

4.1 Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque *file* che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità;

4.2 La Società si riserva la facoltà di procedere alla rimozione di ogni *file* o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione del presente Codice Etico Informatico;

5. UTILIZZO DELLA RETE *INTERNET* E DEI RELATIVI SERVIZI E DEGLI STRUMENTI INFORMATICI AZIENDALI

5.1 Navigazione in *Internet* durante l'orario di lavoro. L'utilizzo della rete internet aziendale per scopi personali durante periodi di pausa è consentito con moderazione e comunque secondo le seguenti regole:

a) non è consentito navigare in siti che possono rivelare le opinioni politiche, religiose o sindacali del dipendente / collaboratore;
b) non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di *remote banking*, acquisti *on-line* e simili, salvo casi direttamente autorizzati dalla Società e con il rispetto delle normali procedure di acquisto;
c) non è consentito lo scarico di programmi, *files*, *software* gratuiti (*freeware*) o a pagamento e *shareware* prelevati da siti *Internet*, se non espressamente autorizzati per iscritto dalla Società;
d) è vietata ogni forma di registrazione a siti in cui contenuti non siano legati all'attività lavorativa;
e) non è permessa la partecipazione, per motivi non professionali a *forum*, l'utilizzo di *chat line*, di bacheche elettroniche e le registrazioni in *guest book* anche utilizzando pseudonimi (o *nicknames*);
f) non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

5.2 Posta elettronica aziendale e telefono:

Nel precisare che anche la posta elettronica ed il telefono sono strumenti di lavoro, si ritiene utile segnalare che:

a) non è consentito utilizzare la posta elettronica aziendale per motivi non attinenti allo svolgimento delle mansioni assegnate. E' possibile utilizzare il telefono aziendale (mobile e non) per scopi privati con moderazione.
b) non è consentito comunicare, inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;

c) la posta elettronica e le telefonate dirette all'esterno della rete informatica e telefonica aziendale possono essere intercettate da estranei, e dunque, non devono essere usata per inviare documentazione di lavoro o comunicazioni "strettamente riservate";

d) ogni comunicazione (interna ed esterna), inviata o ricevuta, che abbia contenuti rilevanti e non ordinari o contenga impegni per la Società deve essere visionata od autorizzata dai Responsabili o dal proprio superiore;

e) anche fuori dall'orario di lavoro, non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale o *nicknames* comunque riconducibili alla Società per la partecipazione a dibattiti, *forum* o *mailing-list* o comunque per qualsiasi comunicazione non attinente l'attività lavorativa, salvo diversa ed esplicita autorizzazione scritta;

f) anche fuori dall'orario di lavoro non è consentito postare su siti *internet* di qualsiasi genere, ivi inclusi *social networks*, fotografie, commenti, dati di ogni genere attinenti l'attività lavorativa e comunque la Società;

g) non è consentito l'utilizzo di posta elettronica o del telefono di altro portatore di interesse della Società per l'inoltro di comunicazioni a proprio nome o a nome di questi, salvo espressa autorizzazione del medesimo;

5.3 L'utilizzo privato della rete aziendale e dei Sistemi informatici aziendali è soggetto alle seguenti regole:

a) Nel caso di utilizzo privato, devono essere rispettate tutte le Leggi, le regole del presente Codice ed ogni ulteriore regola di comportamento aziendale;

b) L'utilizzo privato è ammesso, oltre con l'osservanza delle regole del presente Codice, solo nel caso in cui:

- Non crei danni, spese o concorrenza all'attività della Società;
- Non comporti danni o diminuzioni della capacità lavorativa dell'utilizzatore o di altri dipendenti / collaboratori, con ciò comprendendo anche il divieto di utilizzo per siti e social networks riportanti contenuti non consoni all'attività lavorativa;
- Non comporti pubblicità di alcun tipo;
- Non consenta a soggetti terzi di ricevere informazioni circa dati societari, elenchi di dipendenti o comunque liste di distribuzione collegate alla Società;
- La Società si riserva il pieno ed incondizionato diritto, nell'eventualità di qualsiasi violazione del presente Codice, di proibire, con effetto immediate, l'utilizzo privato della rete aziendale o dei Sistemi informatici aziendali, sia a livello individuale che collettivo. Inoltre l'utilizzatore sarà immediatamente responsabile, anche in termini risarcitori, di ogni violazione al presente Codice;

- L'utilizzatore è consapevole che in caso di utilizzo privato della rete aziendale o dei Sistemi informatici aziendali, sarà possibile che la Società venga a conoscenza di dati privati dell'utilizzatore che, in tal caso, non potrà opporre alcunché.

6. CONSERVAZIONE DELLE COMUNICAZIONI E NAVIGAZIONI. SANZIONI

6.1. L'utilizzo degli Strumenti informatici e della Rete aziendali comporta che tutte le informazioni e comunicazioni veicolate attraverso di essi siano memorizzate nei *server* aziendali o del Gruppo. Il trattamento di tali dati viene svolto dalla Società in conformità alla Informativa sul trattamento dei dati personali che è stata notificata ad ogni dipendente e collaboratore.

6.2. I Dati trasmessi e/o ricevuti mediante la posta elettronica utilizzata sul luogo di lavoro non vengono comunque utilizzati dalla Società al fine di controllare e/o monitorare il comportamento sul luogo di lavoro del dipendente né allo scopo di acquisire elementi tali da connotarne il profilo. Tuttavia, l'infrazione al presente Codice Etico Informatico da parte dei destinatari dello stesso può essere rilevata e dare origine a sanzioni disciplinari fino, nei casi più rilevanti, anche al licenziamento.

6.3. I riferimenti alle sanzioni disciplinari contenuti nel Codice Etico aziendale sono automaticamente estesi anche al presente Codice Etico Informatico.

7. UTILIZZO DELLE *PASSWORD*

7.1 La *password* utilizzata per gli Strumenti informatici aziendali:

a) deve essere composta da almeno otto caratteri e, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
b) non deve contenere riferimenti agevolmente riconducibili al possessore;
c) deve essere modificata dal possessore: al primo utilizzo; successivamente almeno ogni sei mesi; almeno ogni tre mesi nel caso di trattamento di dati sensibili o giudiziari.

7.2 SOCOTIS S.p.a. ricorda che le *Password* sono lo strumento che permette l'accesso diretto ai dati protetti, è necessario, quindi, adoperare una serie di cautele al fine di scongiurare che le parole chiave vengano scoperte od anche solo individuate. In particolare, per quanto concerne la scelta, le parole chiave utilizzate:

a) non dovranno essere scelte tra parole presenti nel dizionario;
b) non dovranno essere parole ovvie quali : nome proprio; nome del coniuge o dei figli; soprannomi noti; nomi di animali propri; nomi di città di residenza, di nascita o di legame; nomi di strade, vie o piazze con le medesime caratteristiche; identificativo utilizzato per la connessione al sistema (cosiddetto ID); data di nascita propria o di parenti stretti; targa o modello dell'automobile o della moto; numero di telefono di casa o del cellulare; anniversari; numero di matricola se assegnato; giorni della settimana o mesi; parole legate alla carica svolta; ecc;

c) non dovranno essere sequenze alfabetiche o numeriche (es. abcdef, 12345);
d) non devono essere una sequenza di caratteri vicini tra loro sulla tastiera (come : qwerty, fred, pippo, asdfg, mnbvcx, ecc);
e) devono possibilmente contenere una combinazione di caratteri alfabetici, numerici o speciali, includendo in questi ultimi i segni di interpunzione e gli altri simboli disponibili;

7.3 Le parole chiave, inoltre, per quanto attiene alla conservazione :

a) devono essere custodite sempre con il massimo livello di riservatezza;
b) non devono mai essere rivelate a nessuno;
c) non devono mai essere annotate su carta né altrove, soprattutto in prossimità della propria postazione;
d) non devono essere mai riutilizzate né devono essere ripescate tra quelle vecchie, né essere identiche alle vecchie con l'aggiunta di una lettera od un numero in più;
e) non devono assolutamente essere indicate a titolo di esempio sul presente Codice o su altre comunicazioni esemplificative in circolazione in azienda;
f) nel caso si utilizzi una sessione di lavoro connessa sia ad un elaboratore centrale sia ad una rete locale, esse non devono essere le stesse per entrambe le connessioni.