REGOLE SULL'UTILIZZO DEGLI STRUMENTI INFORMATICI, DI INTERNET E DELLA POSTA ELETTRONICA

NR Rev	Descrizione modifiche	Data
0	Prima stesura	Settembre 2018

Indice

Premessa

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone la Società e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'Azienda stessa.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, **Ercos Spa** ha adottato un Regolamento interno diretto ad evitare anche comportamenti inconsapevoli che possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Ogni utilizzo delle apparecchiature, degli elaboratori, delle reti e dei dati diversi dalle finalità professionali deve essere strettamente limitato e di natura occasionale, salve le eccezioni espressamente previste nel presente Regolamento. Poiché anche nella normale attività lavorativa, alcuni comportamenti possono mettere a rischio la Sicurezza e l'immagine aziendale, di seguito vengono richiamate semplici regole procedurali finalizzate non tanto a censurare comportamenti consapevolmente scorretti e già di per sé proibiti, ma soprattutto per evitare condotte che inconsapevolmente possano causare rischi alla Sicurezza del trattamento dei dati aziendali.

A seguito dell'emanazione, da parte del Garante per la Protezione dei Dati Personali, del provvedimento generale del 1 marzo 2007 avente ad oggetto "Linee guida del Garante per posta elettronica e internet" ed al fine di conciliare l'esigenza di tutela della privacy dei dipendenti e collaboratori ed il corrispondente potere/dovere del Titolare di assicurare la funzionalità e il corretto impiego degli strumenti informatici da parte degli stessi, **Ercos Spa** ha adottato il presente **Disciplinare interno** che regolamenta, pur nel rispetto dei principi di pertinenza e non eccedenza, le modalità di utilizzo da parte dei suddetti dipendenti e collaboratori della rete ed in genere di tutti gli strumenti tecnologici aziendali.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del D.Lgs. 30 giugno 2003 n. 196, e seguenti modifiche (D.Lgs 101, 10 Agosto 2018, contenente le misure minime di sicurezza, nonché integrano le informazioni già

fornite agli interessati in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.
Considerato inoltre che Ercos Spa, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha da tempo deciso di mettere a disposizione dei propri collaboratori che ne necessitassero per il tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti (computer portatili, telefoni cellulari, etc.), sono state inserite nel regolamento alcune clausole relative alle modalità ed i doveri che ciascun dipendente e collaboratore deve osservare nell'utilizzo di tale strumentazione.

1. Entrata in vigore del regolamento e pubblicità

1.1 Il nuovo regolamento entrerà in vigore il 01/11/2018, salvo successive modifiche ed integrazioni. Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

1.2 Copia del regolamento, oltre ad essere affisso nelle bacheche aziendali, potrà essere prelevato da ciascun dipendente al seguente indirizzo: www.ercos.it

2. Campo di applicazione del regolamento

2.1 Il nuovo regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto.

2.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "incaricato del trattamento".

2.3. Allo scopo di consentire a questi strumenti di perseguire le finalità per le quali sono stati acquisiti, e al fine di garantire che gli strumenti di lavoro possano mantenere le loro funzionalità senza essere danneggiati, anche a seguito di eventuali comportamenti non corretti degli operatori, si

danno qui di seguito alcune informazioni e regole di utilizzo cui tutti, dipendenti e collaboratori, dovranno attenersi.

3. Utilizzo delle stazioni di lavoro

3.1 **La stazione di lavoro (pc, terminale o notebook) affidata all'utente è uno strumento di lavoro**. La Funzione ICT fornisce il necessario supporto agli utenti per il corretto utilizzo delle postazioni di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. La stazione di lavoro deve essere custodita con cura evitando ogni possibile forma di danneggiamento. Gli utenti sono tenuti a conservare le stazioni di lavoro nella configurazione loro assegnata; è quindi vietato:

- togliere/aggiungere/cambiare componenti hardware e software;
- cambiare l'ubicazione delle apparecchiature,

senza la preventiva autorizzazione della funzione ICT.

La configurazione della stazione di lavoro prevede che i dati siano residenti sulle unità di rete a disposizione.

L'utilizzo in rete di PC e di qualsiasi altra attrezzatura informatica personale di dipendenti e di terzi è consentita previa autorizzazione della Funzione ICT, che ne stabilisce le modalità di accesso.

I dati riservati di norma non possono essere registrati su PC portatili; diversamente sono gestiti sotto il controllo della funzione ICT.

3.2 La postazione di lavoro data in affidamento all'utente permette l'accesso alla rete di Ercos S.p.a solo attraverso specifiche **credenziali di autenticazione** come meglio descritto al successivo punto 4 del presente Regolamento.

3.3 Ercos S.p.a rende noto che il personale incaricato che opera presso il servizio Information and Communication Tecnology (nel seguito per brevità "Servizio ICT") della Società è stato autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.).

3.4 Detti interventi, in considerazione dei divieti di cui ai successivi punti nn. 8.2 e 9.1,

potranno anche comportare l'accesso in occasione dei controlli necessari ai fini della **corretta manutenzione ed uso degli strumenti** elettronici: ciò consentirà l'eventuale accesso ai dati trattati da ciascuna stazione di lavoro, ivi compresi gli archivi di posta elettronica, nonché i dati relativi alla navigazione nei siti internet acceduti dagli utenti abilitati. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Azienda, si applica anche in caso di assenza prolungata od impedimento dell'utente.

3.5 Il personale incaricato del servizio ICT ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole stazioni di lavoro al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata e/o autorizzazione dell'utente o, in caso di oggettiva necessità ed urgenza**,** a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

3.6 Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del Servizio ICT per conto di Ercos S.p.a né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone la Società a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.

3.7 Salvo preventiva espressa autorizzazione del personale del Servizio ICT, non è consentito all'utente modificare le caratteristiche impostate sulla propria stazione di lavoro né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.).

3.8 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del Servizio ICT nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 10 del presente Regolamento relativo alle procedure di protezione antivirus.

3.9 La stazione di lavoro deve essere spenta ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo perdurante inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso**.**

4. Gestione ed assegnazione delle credenziali di autenticazione

4.1 Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del Servizio ICT, previa formale richiesta del Responsabile dell'ufficio/area nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente. Nel caso di collaboratori a progetto e coordinati e continuativi la preventiva richiesta, se necessaria, verrà inoltrata direttamente dal Responsabile dell'ufficio/area con il quale il collaboratore si coordina nell'espletamento del proprio incarico.

4.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal Servizio ICT, associato ad **una parola chiave (password) riservata** che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Servizio ICT.

4.3 È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, **almeno ogni tre mesi** come previsto dal sistema informativo installato in Azienda. Il sistema avvertirà l'utente della scadenza della password e della necessità di modifica della stessa.

4.4 La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno <u>otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.</u>

4.5 Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, dovrà procedere in tal senso d'intesa con il personale del Servizio ICT.

5. Utilizzo della rete

5.1 Per l'accesso alla rete ciascun utente deve essere in possesso della specifica credenziale di

autenticazione.

5.2 È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parola chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

Le cartelle utenti presenti nei server 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 in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back-up da parte del personale del Servizio ICT. Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio da parte del personale incaricato del Servizio ICT. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.

5.3 Il personale del Servizio ICT, in caso di identificazione di file o applicazioni in genere pericolose per la sicurezza della rete e/o dei singoli PC, potrà procedere alla rimozione degli stessi, previa comunicazione all'utente incaricato.

5.4 Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

6. Utilizzo e conservazione dei supporti rimovibili

6.1 Tutti i supporti magnetici rimovibili (CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

6.2 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale del Servizio ICT e seguire le istruzioni da questo impartite.

6.3 In ogni caso, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

6.4 Non è consentita l’uscita dalle sedi aziendali di hardware e supporti magnetici, ottici o cartacei, se non preventivamente autorizzati.

6.5 E’ vietato l’utilizzo di supporti rimovibili personali.

6.6 L’utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

6.7 E' interdetta l'installazione o l'uso di supporti rimovibili sulle stazioni di lavoro. Per eventuali necessità in proposito occorrerà farsi autorizzare dal responsabile ICT.

7. Utilizzo dei dispositivi mobili

La Funzione ICT fornisce dispositivi mobili quali notebook, cellulari, internet key, tablet; fornisce inoltre il necessario supporto agli utenti per il corretto utilizzo di essi.

L'utente è responsabile del dispositivo mobile assegnatogli dal Servizio ICT e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

7.1 A tali dispositivi si applicano le regole di utilizzo previste dal presente regolamento con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.

7.2 Anche per tali dispositivi l’installazione di programmi dovrà essere effettuata a cura del servizio ICT, al fine di garantire il rispetto dei criteri di sicurezza informatica nell’uso della rete.

7.3 I dispositivi mobili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

7.4 Gli utenti devono inoltre comunicare alla funzione ICT eventuali guasti o anomalie, riscontrate nell’uso dei dispositivi, e informare tempestivamente di eventuali smarrimenti o furti.

7.5 L’utilizzo di tali dispositivi è limitato all’utente o agli utenti assegnatari; è quindi vietato cederne l’uso, anche temporaneo, a terzi se non preventivamente autorizzato.

7.6 I dati aziendali riservati di norma non possono essere registrati su tali dispositivi mobili; diversamente devono essere gestiti sotto il controllo della funzione ICT.

7.7 Tali disposizioni si applicano anche nei confronti di eventuali incaricati esterni.

Smart working: le precauzioni Privacy

7.8 Il lavoro agile (o smart working) è una modalità di esecuzione del rapporto di lavoro subordinato caratterizzato dall'assenza di vincoli spaziali, stabilita mediante accordo tra dipendente e datore di lavoro; una modalità che aiuta il lavoratore a conciliare i tempi di vita e lavoro e, al contempo, favorire la crescita della sua produttività.

La definizione di smart working, contenuta nella Legge n. 81/2017, pone l'accento sulla flessibilità organizzativa, sulla volontarietà delle parti e sull'utilizzo di strumentazioni che consentano di lavorare da remoto (come ad esempio: pc portatili, tablet e smartphone).

7.9 Il dipendente che sia stato autorizzato allo svolgimento di attività lavorativa in regime di smart working verrà dotato - in via temporanea, se non già precedentemente assegnata - della strumentazione necessaria. Tale strumentazione consiste in: pc portatile, connessione wifi e telefono cellulare. Lo smart working può essere concesso per una sola giornata alla settimana, pertanto in previsione dello stesso il dipendente dovrà farsi carico di ritirare la strumentazione presso l'Ufficio ICT il giorno precedente e riconsegnarla tassativamente la mattina successiva; eventuali impossibilità o variazioni dovranno essere tempestivamente comunicate e concordate con l'Ufficio ICT. Il pc portatile e la connessione wifi permetteranno al dipendente di lavorare sul desktop citrix con le stesse modalità del lavoro eseguito in ufficio - salvo l'impossibilità di stampare i documenti - mentre il cellulare consentirà la reperibilità telefonica. Qualora il dipendente voglia attivare il trasferimento di chiamata dall'ufficio verso il cellulare assegnatogli, egli dovrà, previa formazione, attivare tale funzionalità sul proprio telefono fisso il giorno precedente a quello previsto per lo smart working e disattivarla il giorno successivo. Le chiamate in entrata pervenute al centralino e destinate all'operatore in Smart working saranno trasferite al cellulare in dotazione.
Alla strumentazione fornita si applicano tutte le norme già previste ai punti precedenti.
In particolare, in conformità al Regolamento UE 679/2016 in materia di protezione del dato personale, il dipendente che lavora in Smart Working dovrà prestare particolare cautela nella conservazione dei dispositivi a lui assegnati. L'eventuale perdita o sottrazione di uno di detti dispositivi costituisce una forma di "data breach", ovvero di violazione dei dati personali o, potrebbe costituire, comunque, un serio rischio per la conoscibilità a terzi non autorizzati dei dati personali in esso contenuti.

Nel caso di smarrimento o sottrazione di uno dei dispositivi concessi in uso al dipendente in Smart Working, lo stesso sarà tenuto a darne immediata comunicazione telefonica e scritta a privacy@ercos.it comunque entro 24 ore dalla conoscenza del fatto (sottrazione o perdita).

Il dipendente non potrà mai lasciare incustodito il bene a lui assegnato proprio per evitare un'eventuale sottrazione dello stesso.

Si ricorda, inoltre, che nessun soggetto terzo oltre al dipendente autorizzato allo Smart Working potrà conoscere il contenuto dei documenti di lavoro siano essi in forma cartacea che elettronica: pertanto il dipendente nell'esercizio della sua attività di smart working dovrà prestare ogni cautela in modo che terzi o familiari o conviventi non possano venire a conoscenza di detti dati personali utilizzati o di informazioni aziendali nei luoghi ove si esercita lo Smart Working.

8. Uso della posta elettronica

8.1 **La casella di posta elettronica assegnata all'utente è uno strumento di lavoro.** Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

8.2 È fatto divieto di utilizzare le caselle di posta elettronica ***nome.cognome@nomeazienda.it*** per motivi diversi da quelli strettamente legati all'attività lavorativa, salvo i casi di assegnazione di notebook e/o telefoni cellulari ad uso promiscuo. Anche in tali ultimi casi sarà comunque necessario attenersi alle misure di salvaguardia della sicurezza nel trattamento dei dati aziendali. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp4) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la partecipazione a catene telematiche (o cd. "di Sant'Antonio"). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale del Servizio ICT. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

8.3 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

8.4 Il servizio di posta elettronica aziendale non è un servizio in tempo reale, ovvero il tempo fra

invio e ricezione di un messaggio non è istantaneo e dipende da molti fattori esterni.

8.5 È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

8.6 È obbligatorio porre la massima attenzione nell'aprire i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

8.7 Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) dovrà essere impostato dall'utente per inviare automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura.

8.8 In caso di necessità ed impossibilità dell'utente la procedura potrà, su richiesta, essere attivata dal Servizio ICT.

8.9 Sarà comunque consentito al superiore gerarchico dell'utente o, comunque, sentito l'utente, a persona individuata dall'azienda, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario (ad es: mancata attivazione della funzionalità di cui al punto 8.7; assenza non programmata ed impossibilità di attesa di cui al punto 8.8).

8.10 Il personale del servizio ICT, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potrà accedere alla casella di posta elettronica per le sole finalità indicate al punto 3.3, preavvertendo l'utente, laddove possibile.

8.11 Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale di Ercos S.p.a debitamente incaricato potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nella propria policy aziendale.

8.12 In caso di ricezione accidentale di messaggi di valenza ufficiale sulle caselle assegnate, gli assegnatari riceventi dovranno inoltrarli tempestivamente alla Segreteria utilizzando l'indirizzo: info@ercos.it

E’ inoltre espressamente vietato, salvo autorizzazione espressa del proprio Responsabile, salvare/stampare/inoltrare e portare fuori dai luoghi di lavoro documentazione aziendale. A titolo esemplificativo e non esaustivo è vietato:

- stampare e.mail aziendali per scopi personali;
- Inviare informazioni sensibili ad indirizzi di posta personali;
- fotocopiare/scansionare documentazione aziendale per scopi personali;
- inoltrare a terzi estranei all’azienda documentazione interna/informazioni ricevute per mezzo di strumenti informatici o via cartacea, salvo che non sia funzionale allo svolgimento di prestazioni professionali a favore della stessa Ercos S.p.a.

9. Navigazione in Internet

9.1. La stazione di lavoro assegnata al singolo utente ed abilitata alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa, salvo quanto in appresso specificato.

In questo senso, a titolo puramente esemplificativo, l’utente non potrà utilizzare internet per:

- l’upload o il download di software gratuiti (freeware e shareware), nonché l’utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all’attività lavorativa (es.: filmati e musica) e previa verifica dell’attendibilità dei siti in questione (nel caso di dubbio, dovrà essere a tal fine contattato il personale del Servizio ICT);
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum non professionali, l'utilizzo di chat-line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile d’ufficio;

Al fine di evitare la navigazione in siti non pertinenti all’attività lavorativa Ercos S.p.a rende peraltro nota l’adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l’upload o l’accesso a determinati siti inseriti in una black list.

E' tuttavia consentito ai dipendenti di poter accedere per finalità personali a siti di informazione (Giornali e quotidiani) e/o di altro genere (es. siti prenotazione treni/aerei/home banking) purché per un periodo di tempo assai limitato e solo per eventuali necessità ed urgenze. Tale navigazione per finalità personali deve essere comunque improntata a criteri di buona fede e correttezza e non può in alcun caso pregiudicare il disbrigo assiduo e diligente delle mansioni assegnate.

9.2 Gli eventuali controlli, compiuti dal personale incaricato del Servizio ICT ai sensi del precedente punto 3.3, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre 30 giorni, ossia il tempo indispensabile per il corretto perseguimento delle finalità di sicurezza dell'azienda.

10. Protezione antivirus

10.1 Il sistema informatico di Ercos S.p.a è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo (evitando, quindi, di compiere quei comportamenti vietati dal presente regolamento e già menzionati: es. navigazione su siti non sicuri, download di file non autorizzati, etc.). E' fatto assoluto divieto a ciascun utente di modificare le impostazioni del software antivirus.

10.2 Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso nonché segnalare prontamente l'accaduto al personale del Servizio ICT.

10.3 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, dovrà essere prontamente consegnato al personale del Servizio ICT.

11. Utilizzo dei telefoni

11.1 Il telefono aziendale (fisso e/o portatile) affidato all'utente è uno strumento di lavoro. L'uso del telefono è consentito esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti

l’attività lavorativa stessa . La ricezione o l’effettuazione di telefonate personali mediante utilizzo del telefono fisso aziendale è consentito solo nel caso di comprovata necessità ed urgenza.

11.2 Qualora venisse assegnato un cellulare aziendale all’utente, quest’ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare aziendale si applicano le medesime regole sopra previste per l’utilizzo del telefono fisso aziendale: in particolare è vietato l’utilizzo del telefono cellulare messo a disposizione per inviare o ricevere messaggi di natura personale o comunque non pertinenti rispetto allo svolgimento dell’attività lavorativa, salvo diverse disposizioni aziendali.

11.3 Non sono soggetti a tale disciplina i telefoni cellulari concessi dall’Azienda in uso promiscuo a titolo di benefit.

11.4 L’utilizzo del proprio cellulare personale durante l’orario di lavoro è consentito laddove ricorrano ragioni di necessità e/o urgenza. L’utilizzo deve essere comunque improntato a criteri di buona fede e correttezza e non può in alcun caso pregiudicare il disbrigo assiduo e diligente delle mansioni assegnate.

12. Osservanza delle disposizioni in materia di Privacy

12.1 È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicato nella lettera di designazione ad incaricato del trattamento dei dati ai sensi del D.Lgs. n. 196/2003.

12.2 In adempimento del provvedimento generale del Garante per la Protezione dei Dati Personali del 1 marzo 2007 avente ad oggetto “Linee guida del Garante per posta elettronica e internet” e ai sensi dell’articolo 13 del D.Lgs. 196/2003 (“Codice Privacy”) Ercos S.p.a desidera fornire ai propri dipendenti e/o collaboratori alcune informazioni relative al trattamento dei dati personali raccolti in esecuzione del presente Regolamento contenente le regole sull’utilizzo degli strumenti informatici, di internet e della posta elettronica. I dati raccolti saranno trattati esclusivamente per le finalità elencate nel seguente regolamento (fra le quali si ricordano a titolo esemplificativo i dati raccolti a seguito di manutenzione degli strumenti informatici nonché quelli raccolti a seguito di controlli per verificare il rispetto da parte degli utenti delle regole qui riprodotte) e saranno trattati con modalità telematiche e/o su supporto cartaceo. Si ricorda agli utenti che il conferimento dei dati per le finalità sopra citate è necessario ai fini dell’utilizzo degli

strumenti elettronici forniti in uso all'utente e che di conseguenza l'eventuale rifiuto di fornire tali dati impedirà alla Società di garantire agli utenti l'uso stesso degli strumenti. I dati personali raccolti dalla Società non saranno oggetto di diffusione e potranno essere comunicati esclusivamente a personale di fiducia di Ercos S.p.a(come ad esempio società di servizi che

forniscono supporto nella manutenzione degli strumenti informatici) legati alla Società da stretti vincoli contrattuali che garantiscono la riservatezza e l'integrità delle informazioni trattate. Tutti i dipendenti e/o collaboratori sono titolari dei diritti previsti all'articolo 7 del Codice Privacy che possono essere esercitati con richiesta rivolta al Titolare (Ercos) al seguente indirizzo: privacy@ercos.it

13. Accesso ai dati trattati dall'utente

13.1 Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Direzione Aziendale, tramite il personale del Servizio ICT o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

14. Sistemi di controlli graduali e conservazione dei dati

14.1 Ercos S.p.aha predisposto il proprio sistema informativo e la rete intranet ed internet al fine di utilizzare tali beni aziendali per esclusive esigenze organizzative e/o produttive.

A tal fine, si avvale legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4 comma 2), di sistemi che consentono indirettamente un controllo a distanza (controlli preterintenzionali) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori; e ciò, anche in presenza di attività di controllo discontinue.

In particolare tale attività di controllo potrà essere esercitata nel caso in cui si rivelino anomalie di

funzionamento o si rendano necessarie attività di manutenzione o, comunque, in tutte le ipotesi in cui sia a rischio la sicurezza dei citati beni aziendali e/o la sicurezza sul lavoro in generale.

In caso di anomalie, il personale incaricato del servizio ICT effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.
Questa attività di controllo a distanza sarà pertanto lecita e dettata dal principio di necessità.
Ercos S.p.a non utilizza sistemi hardware e/o software idonei ad effettuare un controllo a distanza dei lavoratori, in particolare mediante:

□□ la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
□□ la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
□□ la lettura o la registrazione dei caratteri inseriti tramite la tastiera e analogo dispositivo;
□□ l'analisi occulta del computer portatili affidati in uso.
In alcun caso verranno compiuti controlli prolungati, costanti o indiscriminati.
14.2 In merito alla conservazione dei dati, Ercos S.p.a adotta le seguenti procedure:
In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici è giustificata da una finalità specifica e comprovata e limitata nel tempo necessario a raggiungerla. Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e avverrà solo in relazione:
□□ ad esigenze tecniche o di sicurezza del tutto particolari;
□□all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
□□ all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria e della polizia giudiziaria.
In questi casi, il trattamento dei dati personali sarà limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di

organizzazione strettamente correlate agli obblighi, compiti e finalità esplicitati.

15. Sanzioni

15.1 È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL e dal Codice Disciplinare Aziendale, nonché con tutte le azioni civili e penali consentite.

16. Norme finali.

16.1. Le disposizioni del presente regolamento si applicano, per quanto compatibili, anche alle ipotesi di collegamento alla rete aziendale da postazioni esterne all'ufficio (ad esempio: collegamento da casa);

16.2 Sono fatte salve diverse disposizioni scritte eventualmente emanate dall'azienda in attuazione della possibilità di smart working prevista dal modello di welfare aziendale per tempo vigente.

17. Aggiornamento e revisione

17.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate da Ercos S.p.a..

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