Società soggetta a Controllo e Coordinamento da Parte dell'Ente Provincia di Caserta

Sede Legale ed Uffici Amministrativi: 81100 Caserta, Via Lamberti n. 29Tel. 0823/21.03.90 - Fax.0823/21.29.87 - www.terradilavorospa.com – Email: info@tlspa.it - PEC: tdl@pec.it
Tel. 0823/15.03.996 – Fax: 0823/15.03.991 – Email: controlloimpianti@tlspa.it – PEC: controlloimpiantitlspa@pec.it

MODELLO DI ORGANIZZAZIONE E GESTIONE (M.O.G.) EX D. LGS.231/2001

REGOLAMENTO UTILIZZO STRUMENTI INFORMATICI

INDICE

Sommario

1. SCOPO DEL REGOLAMENTO 3
2. DEFINIZIONI 3
3. REGOLAMENTO OPERATIVO PER L'USO DEGLI STRUMENTI 6
3.1. Principi generali di comportamento 6
3.2. Obblighi del dipendente 7
3.3. Proprietà degli strumenti informatici e telefonici, programmi e dati 8
3.4. Trasparenza nelle condizioni di utilizzo 8
3.5. Finalità dell'utilizzo degli strumenti informatici e telefonici 9
3.6. Condizioni di Utilizzo Del Pc 9
3.7. Installazione di programmi Software 10
3.8. Utilizzo della Posta Elettronica Aziendale 11
3.9. Autorizzazione all'apertura della propria Posta Elettronica 12
3.10. Utilizzo Di Internet 12
3.11. Utilizzo Dei Pc Portatili 13
3.12. Protezione Antivirus 14
3.13. Utilizzo delle dotazioni telefoniche 14
3.14. Procedura di incident response e ripristino 15
3.15. Regolamento per la gestione delle password 16
3.16. Regole per minimizzare i rischi di virus 18
3.17. Tracciabilità dei dati 20
3.18. Applicabilità a soggetti diversi dai dipendenti 21
4. SISTEMA SANZIONATORIO 21

1. SCOPO DEL REGOLAMENTO

Il presente regolamento disciplina le modalità di accesso e di uso della rete informatica e telematica della società TERRA di LAVORO S.p.A in seguito TL e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire.

Inoltre, questo documento definisce le regole principali da seguire durante l'uso della postazione informatica in proprio possesso.

Eventuali situazioni di deviazione accertate rispetto a quanto precisato nel presente documento dovranno essere rimosse nel più breve tempo possibile.

Lo Scopo del presente Regolamento è di:

- dettare e formalizzare le linee di condotta per l'utilizzo dei Personal Computer (hardware e software), della rete LAN, dei telefoni, della posta elettronica, della navigazione in Internet e della rete informatica nonché degli strumenti informatici in genere;
- informare preventivamente i dipendenti-utilizzatori - in ottemperanza a quanto previsto dal Regolamento Europeo 679/2016 relativo alla protezione delle persone fisiche, dal Decreto Legislativo n°196/2003 "Codice in materia di protezione dei dati personali" così come modificato dal D.Lgs. n° 101 del 10 Agosto 2018 nonché dalla legge 20 maggio 1970, n. 300 "Statuto dei lavoratori" – circa le procedure che il Titolare del Trattamento ha adottato in relazione al corretto utilizzo degli Strumenti Informatici e telefonici.

2. DEFINIZIONI

«danneggiamento»: (*vedi art. 635 del Codice Penale***)**: Chiunque distrugge, disperde, deteriora o rende, in tutto o in parte, inservibili cose mobili o immobili;

«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

«trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

«limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

«archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

«titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

«responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

«destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

«terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

«consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

«violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

«dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

«dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

«dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

«impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

«reti di comunicazione elettronica»: i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

«rete pubblica di comunicazioni»: una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

«servizio di comunicazione elettronica»: i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del 7 marzo 2002, del Parlamento europeo e del Consiglio;

«posta elettronica»: messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete

pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

«strumenti elettronici»: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

«autenticazione informatica»: l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

«credenziali di autenticazione»: i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

«parola chiave»: componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

«profilo di autorizzazione»: l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

«sistema di autorizzazione»: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

3. REGOLAMENTO OPERATIVO PER L'USO DEGLI STRUMENTI

3.1. Principi generali di comportamento

La TL promuove l'utilizzo della rete e dei supporti elettronici quale strumento utile per perseguire le proprie finalità.

Gli utilizzatori di strumenti elettronici e informatici manifestano liberamente il proprio pensiero nel rispetto dei diritti degli altri utenti e di terzi, nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche, in osservanza delle leggi, norme e obblighi contrattuali.

Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.

Il posto di lavoro costituito da personal computer viene consegnato completo di quanto necessario per svolgere le proprie funzioni, pertanto è vietato modificarne la configurazione.

Il software installato sui personal computer è quello richiesto dalle specifiche attività lavorative dell'operatore. **È pertanto proibito installare qualsiasi programma da parte dell'utente o di altri operatori**, escluso il Responsabile del Sistema Informativo.

I dati di tutte le Postazioni elettroniche e quelle relative al personale che può accedere viene conservato dal Responsabile del Sistema Informativo.

La TL al fine di prevenire ogni possibile utilizzo non consentito degli strumenti elettronici e della rete aziendale adotta quantomeno le misure minime previste dall'Allegato B del D.l.gs 196/2003 in materia di tutela e trattamento dei dati.

A questi fini **è fatto divieto a tutti i dipendenti della TL** ed a qualsiasi utente che accede ad una postazione informatica di:

- porre in essere condotte, anche con l'ausilio di soggetti terzi, miranti all'accesso a sistemi informativi altrui con l'obiettivo di:
  I. acquisire abusivamente informazioni contenute nei suddetti sistemi informativi;
  II. danneggiare/distruggere dati contenuti nei suddetti sistemi informativi;
  III. utilizzare abusivamente codici d'accesso a sistemi informatici e telematici nonché procedere alla diffusione degli stessi;
- porre in essere condotte miranti alla distruzione o all'alterazione dei documenti informatici aventi finalità probatoria in assenza di una specifica autorizzazione;
- utilizzare o installare programmi diversi da quelli autorizzati dal personale della struttura a cui è affidata la gestione dei sistemi informativi;
- aggirare o tentare di aggirare i meccanismi di sicurezza aziendali (es. Antivirus, Firewall, Proxy server); lasciare il proprio Personal Computer sbloccato e incustodito;
- rivelare ad alcuno le proprie credenziali di autenticazione (nome utente e password) alla rete aziendale o anche ad altri siti/sistemi;
- detenere o diffondere abusivamente codici di accesso a sistemi informatici o telematici di terzi o di enti pubblici;
- entrare nella rete aziendale e nei programmi aziendali con un codice utente diverso da quello assegnato.

3.2. Obblighi del dipendente

Ogni Dipendente è tenuto a prestare la propria attività lavorativa con particolare regolarità, diligenza e correttezza professionale, nel rispetto delle direttive impartite dai superiori e delle disposizioni di servizio, in vista degli obiettivi produttivi e di sviluppo dell'azienda (art. 2104 c.c.).

Non potrà trattare affari, per conto proprio o di terzi, in concorrenza con l'azienda a cui appartiene, né divulgare notizie attinenti all'organizzazione ed i metodi di produzione aziendale, o comunque farne un uso tale da recare pregiudizio all'azienda. In particolare, ogni Dipendente è tenuto, per tutta la durata

del rapporto di impiego, ad osservare la massima riservatezza e non potrà fornire o divulgare notizie, dati, documenti che in relazione alle mansioni affidate venissero comunque in Sua conoscenza o in Suo possesso.

Inoltre, ogni Dipendente è obbligato a custodire e ad impiegare, con particolare diligenza, i beni aziendali che gli verranno concessi in dotazione o in uso in quanto essi stessi contenenti dati personali e sensibili.

3.3. Proprietà degli strumenti informatici e telefonici, programmi e dati

La TL è proprietaria degli strumenti informatici e dei sistemi hardware utilizzati dal proprio personale per lo svolgimento delle attività e si avvale di software e di programmi antivirus di cui la TL è unico ed esclusivo proprietario.

3.4. Trasparenza nelle condizioni di utilizzo

L'utilizzatore è a conoscenza del fatto che le informazioni, le registrazioni e i dati trattati o memorizzati mediante gli Strumenti Informatici aziendali, inclusi i messaggi di posta elettronica inviati e ricevuti e la navigazione in Internet, non possono essere ritenuti completamente privati o confidenziali. In relazione a tale circostanza ed al fine di evitare che si determini in capo al singolo dipendente una legittima aspettativa di riservatezza del messaggio ricevuto attraverso la posta aziendale, si ritiene di specificare la natura aziendale dello strumento informatico e dei contenuti di posta (in entrata ed in uscita) indirizzati all'indirizzo elettronico aziendale.

Conseguenza diretta di tale circostanza è che pur rimanendo le e-mail ed Internet un'area riservata dell'utilizzatore-dipendente tuttavia l'uso della posta e della strumentazione aziendale deve essere finalizzato al solo espletamento dell'attività lavorativa.

La TL, comunque, consente l'accesso e l'uso – dalla postazione aziendale - di altro indirizzo di posta personale per l'invio di e-mail personali, purché lecite e prive di contenuti contrari all'ordine pubblico ed al buon costume secondo quanto in seguito meglio specificato. A tal fine, nel rispetto dei principi di pertinenza e non eccedenza, il Titolare può adottare, attraverso l'Incaricato di Sistema, eventuali misure che consentano la verifica di comportamenti anomali, quali un controllo preliminare dei dati aggregati, riferiti all'intera struttura lavorativa o a sue aree. Ciò al fine di evitare, da parte della TL, successivi controlli specifici che realizzino un'attività di monitoraggio e controllo a distanza del lavoratore-utilizzatore.

3.5. Finalità dell'utilizzo degli strumenti informatici e telefonici

Gli strumenti informatici e telefonici sono uno strumento di lavoro, ed a questo fine ne è consentito l'utilizzo. Qualsiasi eventuale apparente tolleranza da parte della TL non potrà in ogni caso legittimare comportamenti contrari alle istruzioni contenute nel presente regolamento.

3.6. Condizioni di Utilizzo Del Pc

Il Personal Computer (sia postazione fissa sia notebook) affidato all'utilizzatore è uno strumento di lavoro.

L'utilizzo del medesimo per scopi non inerenti all'attività lavorativa - poiché potenzialmente idoneo ad usi impropri o illeciti come violazioni di legge, violazioni di codici aziendali, violazioni di procedure di sicurezza o inosservanza della normativa sulla proprietà intellettuale (è vietata la copia e l'installazione di software non legalmente licenziati) - può essere sottoposto a verifica periodica da parte della TL mediante sistemi automatizzati che comunque non violino il divieto di installazione di “apparecchiature per finalità di controllo a distanza dell’attività dei lavoratori” (articolo, 4, primo comma, legge 300 del 1970).

L'accesso al pc è protetto da password che deve essere custodita dall'utilizzatore con la massima diligenza e non divulgata.

Nei casi di assenza dell’utilizzatore, l’accesso è altresì consentito al superiore gerarchico al fine di porre in essere gli usuali adempimenti, relativi alle normali esigenze di servizio.

Tutti i PC, compresi gli "stand alone"[1] e i portatili, devono avere la versione più aggiornata della protezione antivirus scelta da TL.

Non è consentito all'utente modificare le caratteristiche di configurazione software e hardware impostate sul proprio PC, salvo previa autorizzazione scritta del Titolare del trattamento.

Non è consentita l'installazione sul PC in dotazione di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem), se non con l'autorizzazione scritta del Titolare.

[1] *Stand-alone* tradotto letteralmente: sta in piedi da solo, indipendente. In informatica si dice di un oggetto capace di funzionare da solo, indipendentemente dalla presenza di altri oggetti con cui potrebbe comunque interagire. Detto di un programma, indica il fatto che tale programma può funzionare senza sistema operativo o comunque senza installazione; detto di una periferica significa che tale periferica può svolgere alcune delle proprie funzioni senza essere collegata ad un calcolatore. Detto di un videogioco, significa che tale videogioco è un'espansione di un precedente titolo, ma può funzionare anche senza che quest'ultimo sia installato.

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.
Inoltre, nell'utilizzo dei PC, l'utilizzatore dovrà avere cura di:

a. non lasciare accessibile il suo PC, in sua assenza (ricordiamo che ad esempio gli accessi ad Internet vengono registrati in funzione dell'utente di rete);
b. non lasciare visualizzati sullo schermo, in sua assenza, dati personali;
c. cancellare i dati presenti sul computer o sulla rete quando il loro mantenimento non è più necessario;
d. informare il diretto superiore qualora si accorga di avere accesso a dati e programmi che non sono di sua competenza
e. non utilizzare dischi o supporti esterni con dati o programmi di provenienza ignota, per evitare infezioni da virus nel computer e di danneggiare i dati;
f. chiudere sempre i programmi secondo le appropriate misure di sicurezza. Si ricorda che è assolutamente vietato collegare alla rete aziendale PC "esterni" (es. consulenti, clienti, fornitori etc.), se non attraverso le procedure e l'autorizzazione del proprio Responsabile.
g. nel caso ci sia la necessità di trasferire dati verso l'esterno su supporti dati, di memorizzazione o memorie di massa (USB, HDD, etc.) è fatto obbligo di utilizzare l'apposita procedura di criptazione, che utilizza un metodo di crittografia complessa AES a 256bits, e che quindi impedisce l'accesso ai dati a persone non autorizzate.

3.7. Installazione di programmi Software

L'utilizzatore non è autorizzato a scaricare, copiare o installare software; qualsiasi richiesta o esigenza in tal senso deve essere inoltrata al proprio Responsabile ed autorizzata dal Titolare del Trattamento.
A tal fine si ricorda a tutti gli utilizzatori che sia il software che i diritti di "copyright" sono tutelati mediante sanzioni civili e penali (D. LGS. 29 dicembre 1992, n. 518, sulla tutela giuridica del software e legge 18 agosto 2000 n, 248, contenente disposizioni in tema di tutela del diritto di autore).
La TL vieta tali comportamenti e non assume alcuna responsabilità riguardo a comportamenti degli utenti che possano costituire illecito, ed al contrario si rivarrà sull'utilizzatore per ogni danno o costo nel quale possa incorrere a causa di comportamenti illeciti di quest'ultimo.

L'utente non è autorizzato a cancellare dati o informazioni di proprietà della TL, né a cancellare o modificare l'impostazione dei programmi installati e configurati, salvo quanto esplicitamente indicato nel presente Regolamento.

3.8. Utilizzo della Posta Elettronica Aziendale

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

In particolare, non è consentito:

- l'utilizzo delle caselle di posta elettronica aziendale per partecipare a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione qualora tale uso risponda ad esigenze di lavoro;
- l'invio di messaggi di posta elettronica dal contenuto offensivo, molesto, volgare, blasfemo o comunque inappropriato;
- l'utilizzo di sistemi di posta elettronica o di Strumenti Informatici affidati ad altri utilizzatori, nonché l'uso di account di altri utenti;
- l'utilizzo di password di accesso a singoli documenti o messaggi, o l'uso di tecniche di criptazione, salvo espressa autorizzazione scritta rilasciata caso per caso da parte del Titolare;
- l'utilizzo di "anonymising remailer" o di altri sistemi per mascherare l'identità dell'utilizzatore, salvo che ciò non derivi da specifiche esigenze aziendali e non vi sia stata la preventiva autorizzazione scritta da parte del Titolare;
- l'invio di messaggi di posta elettronica tipo "catene di Sant'Antonio".

Per fini di sicurezza del sistema è obbligatorio controllare i file allegati o gli "attachements" di posta elettronica prima del loro utilizzo, ed è proibito eseguire download di file eseguibili o di documenti da siti Web il cui contenuto non sia inerente le prestazione di lavoro. I documenti aventi natura confidenziale o riservata devono essere protetti da eventuali accessi di soggetti non autorizzati e non devono essere trasmessi a mezzo di posta elettronica, tranne che siano stati approntati adeguati meccanismi di sicurezza. Ogni dubbio in merito alla natura confidenziale o riservata dei documenti deve essere chiarito con il proprio Responsabile.

I messaggi di posta elettronica che costituiscono documenti aziendali devono essere adeguatamente salvati ed archiviati nel mail server aziendale in modo da renderne agevole l'accesso a tutti i soggetti legittimati. Atteso che i costi associati alla conservazione di e-mail non essenziali sono notevoli, al fine

di evitare la perdita delle risorse della TL, l'utilizzatore, sulla base di una propria prudente valutazione, dovrà provvedere a cancellare dalla rete aziendale i messaggi di cui la conservazione non è necessaria.
È consentito da parte della TL l'accesso e l'uso dalla propria postazione aziendale di un indirizzo privato di posta per scopi strettamente personali.
Tale deroga non altera in alcun modo i divieti già previsti per l'uso della posta aziendale, né può essere causa del mancato compimento degli obblighi di servizio. A tal fine si ribadisce il divieto di utilizzazione della posta privata per finalità illecite o contrarie a norme o regolamenti. In ogni caso l'accesso e l'uso, dalla propria postazione aziendale, di un indirizzo di posta privato è consentito:

- purché l'indirizzo di posta elettronica privato non sia utilizzato per spedire o ricevere contenuti, atti, file, notizie o qualsiasi altra informazione o documento attinente all'attività lavorativa;
- purché l'accesso e l'uso dell'indirizzo di posta elettronica privato avvenga esclusivamente durante le pause regolarmente concordate con il datore di lavoro e previste dai contratti collettivi ed aziendali.

3.9. Autorizzazione all'apertura della propria Posta Elettronica

Essendo la casella di posta elettronica uno strumento funzionale al corretto svolgimento dell'attività della TL, l'utilizzatore, in caso di assenza o di prolungato allontanamento dalla propria postazione, autorizza la presa visione della sua casella di posta elettronica da parte del Responsabile, in quanto custode legittimo delle password relative al proprio servizio.
In caso di cessazione per qualsivoglia ragione e/o causa del rapporto di lavoro e/o di collaborazione e/o altro in essere con la TL., l'utilizzatore autorizza espressamente il Responsabile superiore ad accedere alla sua casella di posta elettronica al fine di predisporre la postazione di lavoro per un nuovo utilizzatore ed archiviare (in forma cartacea e/o elettronica) le comunicazioni inerenti all'attività lavorativa. L'utilizzo dell'account sarà mantenuto attivo per un periodo di tempo di sei mesi, sufficiente ad informare clienti/fornitori per assicurare la continuità di lavoro necessaria.

3.10. Utilizzo Di Internet

L'accesso ad Internet e ogni simile accesso deve avvenire solo per esigenze di lavoro. È proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa. In nessun caso l'accesso ad Internet ed ogni simile accesso può essere utilizzato per:

- vedere, scaricare, ricevere o diffondere materiale pornografico, offensivo o osceno;

- compiere attività che possono essere pregiudizievoli per gli interessi della TLo illegali.

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dal Titolare e con il rispetto delle normali procedure di acquisto.

È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

È vietata la partecipazione a Forum-on-line non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi.

La TL per ridurre il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'upload o il download di file, l'uso di servizi di rete con finalità ludiche o estranee comunque all'attività) adotta opportune misure che possono prevenire controlli successivi del lavoratore quali:

- la individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni – reputate inconvenienti con l'attività lavorativa – quali l'accesso a determinati siti o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato);
- trattamento di dati in forma anonima;
- eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

3.11. Utilizzo Dei Pc Portatili

I PC portatili, come tutti gli altri strumenti aziendali, non possono essere usati per scopi diversi da quelli aziendali.

Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, indicati nel paragrafo 3.6 del presente Regolamento, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna

I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi in un luogo adeguatamente protetto.

II dipendente assegnatario che, venendo meno al dovere di diligenza nella custodia, causi il danneggiamento o smarrimento delle dotazioni informatiche affidate, risponderà personalmente del danno patrimoniale arrecato.

Nel caso di furto del PC, atteso che gli stessi contengono informazioni riservate e dati personali, si dovrà provvedere a denuncia immediata anche ai sensi del Decreto Legislativo n°196/2003 "Codice in materia di protezione dei dati personali" così come modificato dal D.Lgs. n° 101 del 10 Agosto 2018.

3.12. Protezione Antivirus

Ogni dipendente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus od altro software aggressive.

E' buona norma per il dipendente controllare il regolare funzionamento I'aggiornamento periodico del software installato secondo le procedure previste.

Nel caso il software antivirus rilevi la presenza di virus, l'utente dovrà immediatamente:

- sospendere ogni elaborazione in corse senza spegnere il computer;
- segnalare l'accaduto al Responsabile.

Gli utilizzatori non devono trasferire dati o programmi sul loro PC provenienti da supporti esterni (es. Memorie USB, Hard Disk Esterni, CD Rom, etc.) non preventivamente monitorati dall'antivirus.

L'utilizzatore che ritenga che il suo PC sia infettato da virus deve spegnere la macchina ed avvisare immediatamente il suo superiore gerarchico. II PC potrà essere riutilizzato solo dopo che il virus sia stato rimosso su autorizzazione del Responsabile secondo le procedure di Restore di seguito indicato.

3.13. Utilizzo delle dotazioni telefoniche

II telefono mobile aziendale - oltrechè la postazione fissa - rappresentano dotazioni elettroniche/telematiche finalizzate o comunque concorrenti a migliorare e/o facilitare Io svelgimento delle mansioni affidate al dipendente.

II personale dipendente assegnatario ne deve avere cura, segnalando ogni anomalia di funzionamento al Responsabile.

AI dipendente assegnatario di telefono fisso fatto espresso divieto di:

- manomettere i componenti dell'apparecchio;
- effettuare operazioni di programmazione non previste dal manuale d'uso pubblicato sul portale aziendale;
- collegare ai telefoni apparecchiature non espressamente autorizzate dall'ufficio Sistemi Informativi (ad es. segreteria telefoniche o altro);
- effettuare chiamate per dettatura di telegrammi (salvo utenti espressamente autorizzati).

AI dipendente assegnatario di telefonia mobile e fatto espresso divieto di:

- rimuovere la SIM dal telefono mobile aziendale per installarla su apparecchio diverse rispetto a quello assegnato; salvo casi di temporanea necessità;
- utilizzare il telefono in dotazione per use personale o comunque per fini diversi da quelli aziendali; salvo I'abilitazione all'addebito personale;
- utilizzare la connessione internet ovvero la gestione di messaggi di posta elettronica per gli apparecchi dotati delle citate funzionalità per scopi differentia quelli lavorativi.

L'uso indebito delle dotazioni telefoniche aziendali comporterà, a carico del trasgressore, I'apertura a sue carico di una procedura disciplinare.

II dipendente assegnatario che, venendo meno al dovere di diligenza, causi la perdita (smarrimento) e/o il danneggiamento delle dotazioni telefoniche affidate, rispondera patrimoniaimente del danno arrecato se, nell'arco di due anni, avrà perso o reso inservibile già due apparecchi. AIl'assegnazione del terzo apparecchio (fisso e/o mobile) il relativo costo sarà addebitato a cedolino paga. L'azienda utilizza sia a propria tutela che per un efficace controlro dei costi un sistema di documentazione addebiti telefonici che archivia tutte le telefonate uscenti ed i costi generati dal singolo telefono aziendale. L'archivio rispetta le normative di tutela della privacy omettendo I'indicazione delle ultime tre cifre del numero chiamato.

3.14. Procedura di incident response e ripristino

Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente il Responsabile, nel caso in cui constatino le seguenti anomalie:

- discrepanze nell'uso degli user-id;
- modifica e sparizione di dati;
- cattive prestazioni del sistema (così come percepite dagli utenti);
- irregolarità nell'andamento del traffico;
- irregolarità nei tempi di utilizzo del sistema;
- quote particolarmente elevate di tentativi di connessione falliti.

In caso di incidente, cioè di un evento che produce effetti negativi sulle operazioni del sistema e che si configura come frode, danno, abuso, compromissione dell'informazione, perdita di beni, sono considerate le seguenti priorità:

- evitare danni diretti alle persone;
- proteggere l'informazione sensibile o proprietaria;

- evitare danni economici;
- limitare i danni all'immagine dell'Ente.

Il Responsabile di riferimento, garantita l'incolumità fisica alle persone, procede a:

- isolare l'area contenente il sistema oggetto dell'incidente;
- isolare il sistema compromesso dalla rete;
- spegnere correttamente il sistema oggetto dell'incidente. Una volta spento il sistema oggetto dell'incidente non deve più essere riacceso;
- documentare tutte le operazioni.

Se l'incidente è dovuto ad imperizia del personale o ad eventi accidentali, ovvero quando non vi è frode, danno, abuso e non è configurabile nessun tipo di reato, il ripristino può essere effettuato, a cura del Responsabile dei Sistemi informativi, direttamente sugli hard disk originali a partire dalle ultime copie di backup ritenute valide.

Altrimenti il Responsabile dei Sistemi Informativi (cioè se rileva tentativi di frode, abuso, o qualsiasi attività dolosa configurabili come reati) deve comunicare l'accaduto al Consiglio di Amministrazione.

La successiva fase di indagine e di ripristino del sistema sarà condotta da personale esperto di incident response, tenendo presente quanto sotto indicato:

- eseguire un tentativo per il recupero dei dati presenti sull'hard disk del sistema compromesso;
- se non si riesce a recuperare tali dati, verrà ripristinato il sistema ed aggiornato con le ultime copie di back-up ritenute valide.

Va ricordato che lo scopo dell'incident response e dell'attività di ripristino è che venga assicurata l'integrità e la sicurezza dello stato del sistema in oggetto e quindi non venga introdotta alcuna alterazione ai dati residenti nel sistema medesimo; un ripristino affrettato del sistema potrebbe alterare le prove dell'incidente.

Il ripristino della disponibilità di tutti i dati personali trattati dalla TLcon strumenti elettronici, che dovessero essere distrutti o danneggiati per qualsivoglia motivo, è assicurato dalla procedura di salvataggio dei dati (back-up) di seguito descritta.

3.15. Regolamento per la gestione delle password

A ciascun incaricato è affidato l'utilizzo e l'accesso ad un PC Client dotato di un sistema di autenticazione informatica, come previsto dall'art. 34, comma 1, lett. a) del Codice.

In particolare, è previsto l'utilizzo da parte degli Incaricati di apposite credenziali di autenticazione che consentono il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

Ciascun Incaricato è reso edotto del fatto che le credenziali di autenticazione sono personali:

- devono essere memorizzate;
- non devono essere comunicate a nessuno;
- non devono essere trascritte.

Le "credenziali di autenticazione" consistono in un codice per l'identificazione dell'incaricato ("user id") non assegnabile, neppure successivamente nel tempo, ad altro incaricato;

La credenziale di autenticazione deve essere associata a una parola chiave riservata conosciuta solamente dal medesimo ("password"), composta da almeno 8 (otto) caratteri, non contenente riferimenti agevolmente riconducibili all'incaricato.

La password, in particolare, deve rispettare i seguenti criteri:

- non deve contenere nomi comuni;
- non deve contenere nomi di persona;
- deve contenere sia lettere che numeri;
- deve comprendere almeno 3 caratteri alfabetici;
- deve comprendere almeno 2 caratteri numerici;
- deve essere diversa dallo user-id;
- deve essere lunga 8 caratteri od al numero massimo consentito dal sistema di autenticazione;
- non deve essere riconducibile all'incaricato del trattamento.

Agli incaricati è prescritta la modifica della password almeno ogni 6 (sei) mesi, ovvero ogni 3 (tre) se i trattamenti svolti hanno ad oggetto dati sensibili. Agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della password.

L'autenticazione dell'incaricato avviene tramite la verifica della "password" relativa alla "user id" associata.

E' previsto un sistema di "password lock-out" che blocca la procedura di accesso al Personal Computer in seguito al verificarsi di un determinato numero di accesso falliti. In particolare, il sistema di password lock-out è impostato sulla base del tipo di servizio cui l'utente può accedere:

- Per quanto riguarda i servizi verso l'esterno è previsto il blocco della procedura di accesso dopo un determinato numero di tentativi falliti;
- Per quanto riguarda i servizi interni all'azienda, quindi l'accesso al dominio, dopo il terzo tentativo di accesso con una password errata, il sistema presenta un delay temporale che impedisce l'uso di attacchi brute force.

Tutti tentativi di accesso non autorizzati sono registrati.

Il Responsabile dei Sistemi Informativi provvede, ogni sei mesi, alla pulizia degli account per la disattivazione delle credenziali inutilizzate nel periodo, o riferite ad incaricati che hanno perso le qualità per accedere ai dati personali.

In caso di smarrimento della password l'utente deve tempestivamente richiedere una nuova assegnazione. Il Responsabile dei Sistemi Informativi provvede ad annullare le vecchie password e ad assegnare le nuove in via provvisoria autorizzando l'Incaricato ad inserire la propria password scelta personalmente.

In caso di necessità improrogabile, su richiesta scritta da parte del Responsabile Amministrazione, quale custode delle credenziali, sostituisce la parola chiave dell'incaricato con una nuova senza bisogno di conoscere la vecchia. Questa procedura garantisce l'impossibilità di collegarsi ai sistemi usando l'identità dell'incaricato senza compiere azioni che non risultino evidenti all'incaricato stesso. Infatti, al suo rientro in azienda, successivo ad un eventuale intervento, l'incaricato non può connettersi con la sua password, risultando quindi automaticamente avvisato dell'avvenuto intervento il quale, in ogni caso deve essere comunicato.

3.16. Regole per minimizzare i rischi di virus

Per minimizzare il rischio da virus informatici, gli utilizzatori dei PC adottano le seguenti regole:

- divieto di lavorare con diritti di amministratore o superutente sui sistemi operativi che supportano la multiutenza;
- limitare lo scambio fra computer di supporti rimovibili (floppy, cd, zip) contenenti file con estensione .EXE, .COM, .OVR, .OVL, .SYS, .DOC , .XLS;
- controllare (scansionare con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;

- evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di “scaricare“ dalla rete internet ogni sorta di file, eseguibile e non. La decisione di “scaricare” può essere presa solo dal Responsabile del trattamento;
- disattivare gli Activex e il download dei file per gli utenti del browser Internet Explorer;
- disattivare la creazione di nuove finestre ed il loro ridimensionamento e impostare il livello di protezione su “chiedi conferma” (il browser avvisa quando uno script cerca di eseguire qualche azione);
- attivare la protezione massima per gli utenti del programma di posta Outlook al fine di proteggersi dal codice HTML di certi messaggi e-mail (buona norma è visualizzare e trasmettere messaggi in formato testo poiché alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer);
- non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti");
- non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta, (in quanto potrebbe essere falso e portare a un sito-truffa);
- non utilizzare le chat;
- consultare con periodicità settimanale la sezione sicurezza del fornitore del sistema operativo e applicare le patch di sicurezza consigliate;
- seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);
- avvisare il Responsabile dei Sistemi Informativi nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC, ovvero in ritardo (in questo caso è possibile che l'infezione abbia raggiunto parti vitali del sistema);
- conservare i dischi di ripristino del proprio PC (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC);
- conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;

- conservare la copia originale del sistema operativo e la copia di backup consentita per legge;
- conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc. fornite dal costruttore).

Nel caso di sistemi danneggiati seriamente da virus il Responsabile dei Sistemi Informativi procede a reinstallare il sistema operativo, i programmi applicativi ed i dati; seguendo la procedura indicata:

- formattare l'Hard Disk, definire le partizioni e reinstallate il Sistema Operativo (molti produttori di personal computer forniscono uno o più cd di ripristino che facilitano l'operazione);
- installare il software antivirus, verificate e installare immediatamente gli eventuali ultimi aggiornamenti;
- reinstallare i programmi applicativi a partire dai supporti originali;
- effettuare il RESTORE dei soli dati a partire da una copia di backup recente. NESSUN PROGRAMMA ESEGUIBILE DEVE ESSERE RIPRISTINATO DALLA COPIA DI BACKUP: potrebbe essere infetto;
- effettuare una scansione per rilevare la presenza di virus nelle copie dei dati;
- ricordare all'utente di prestate particolare attenzione al manifestarsi di nuovi malfunzionamenti nel riprendere il lavoro di routine.

3.17. Tracciabilità dei dati

La TL, anche in esecuzione delle prescrizioni di cui al Provvedimento Garante per la Protezione dei Dati Personali del 27.11.2008 ed s.m.i. è dotata di appositi programmi di tracciabilità e conservazione dei dati e delle operazioni che vengono eseguite dal Responsabile dei Sistemi Informativi su tutti i server/PC, collegati alla rete aziendale. Le operazioni compiute da tutti gli utenti (dipendenti/collaboratori, etc.), memorizzate dal sistema operativo, vengono conservate per le finalità di cui alle disposizioni normative in materia e al fine di essere rese disponibili a fronte di richieste da parte dell'Autorità Giudiziaria. Unicamente al Responsabile del Sistema Informativo è consentito effettuare operazioni sui dati memorizzati.

La tracciabilità "avvisa" nel caso vengano salvati programmi e/o files non autorizzati sui server della TL.

Considerata I'importanza strategica dei server stessi, che costituiscono la banca dati della TL e quindi il patrimonio imprescindibile per il corretto svolgimento delle attività aziendali che deve essere

adeguatamente preservato, il Responsabile del Sistema informativo è autorizzato ad intervenire immediatamente al verificarsi di dette anomalie.

Le operazioni difformi compiute dall'utente in seguito individuato, saranno oggetto di segnalazione al Consiglio di Ammnistrazione.

Le operazioni collegate all'utilizzo della casella di posta elettronica aziendale vengono altresi monitorate tramite apposite log, nel rispetto delle disposizioni di legge in materia. La tracciabilità riguarda solamente i dati identificativi del mittente, destinatario, data e era di spedizione/ricezione del messaggio e oggetto della missiva

Operazioni di tracciabilità dei dati vengone eseguite anche rispetto alle funzioni di stampa attivate dagli utenti connessi alle c.d. stampanti multifunzione della TL nel rispetto delle disposizioni di legge in materia. Anche in questo caso il monitoraggio riguarderà solo il nome dell'utente che ha proceduto alla stampa del file, il nome del file medesimo, il cesto generate, la data e I'ora dell'avvenuta stampa

Ogni nuovo accesso a internet e/o ogni abilitazione all'utilizzo di hardware/software (sia in versione *Solo Lettura* sia in versione *scrittura)* deve essere richiesto ed autorizzato da parte del Responsabile.

AI dipendente che, per motivi di organizzazione del lavoro, venga trasferito ad altro Settore e/o Ufficio ovvero modifichi sostanzialmente le proprie mansioni, I'accesso al servizio internet aziendale verrà automaticamente inibito. Sara cura del nuovo Responsabile se diverso richiedere al Responsabile Sistemi Informativi (un nuovo accesso specificando eventuali limiti di funzionalità).

Ogni nuovo accesso a internet a favore di personale NON dipendente (collaboratori, consulenti, stagisti, etc.) dovrà essere espressamente richiesto dal Responsabile Amministrazione.

3.18. Applicabilità a soggetti diversi dai dipendenti

Tutte le disposizioni del presente Regolamento si applicano, in quanto compatibili, anche a soggetti diversi dai lavoratori dipendenti (collaboratori, consulenti, liberi professionisti etc.) che a vario titolo utilizzano il sistema informativo della TL e/o risultano essere assegnatari di dotazioni informatiche/telematiche e telefoniche aziendali.

4. SISTEMA SANZIONATORIO

La TL espleta la propria attività anche tramite l'ausilio di strumenti informatici e telematici e, per mere esigenze organizzative e produttive, può compiere controlli periodici a campione, riferiti a singole aree produttive o a gruppi di dati aggregati: le relative verifiche verranno comunque eseguite in conformità a quanto previsto della legge 20 maggio 1970, n. 300. Tale attività di verifica non costituisce e non verrà

utilizzata per eseguire controlli a distanza dei lavoratori, l'installazione di eventuali apparecchiature che dovessero rientrare nell'ambito di applicazione dell'art. 4 della legge 20 maggio 1970, n. 300 verrà concordata con le organizzazioni sindacali o autorizzata dall'Ispettorato del lavoro.

La TL informa che l'eventuale verifica sul corretto utilizzo degli Strumenti Informatici è volta a prevenire condotte aventi rilevanza penale, inadempimenti dell'obbligo contrattuale assunto dal lavoratore, uso improprio di attrezzatura aziendale, danni o modifiche nella configurazione del computer, aggravi dei costi di natura telematica (navigazione impropria su Internet).

In particolare, ed a mero titolo esemplificativo, la TL si riserva il diritto di avere accesso alla memoria dei personal computer e dei supporti di dati estraibili, anche mediante meccanismi cosiddetti di "remote control", nonché di accedere, alle informazioni o ai documenti registrati o inviati tramite gli Strumenti Informatici.

Il Responsabile dei Sistemi Informativi/AMMINISTRATORE DI SISTEMA riporterà al Consiglio di Amministrazione della TL qualora dovesse riscontrare un abuso nell'utilizzo degli Strumenti Informatici aziendali da parte di un dipendente della stessa. Il Consiglio di Ammnistrazione della TL potrà adottare gli opportuni provvedimenti di carattere disciplinare nei riguardi del dipendente inadempiente.

La TL nel corso dei controlli contemplati nella presente Regolamento, potrebbe acquisire dati personali dell'utilizzatore o di soggetti terzi relativi all'utilizzo degli Strumenti informatici. Tali dati personali saranno trattati allo scopo di verificare il corretto utilizzo delle attrezzature aziendali e non saranno diffusi né comunicati a terzi all'esterno di TL., salvo che ciò sia necessario alla tutela, anche giudiziale, dei diritti e degli interessi della stessa.

Come previsto dall'art. 7 della legge 300/70, si porta a conoscenza di tutti gli utilizzatori che le prescrizioni contenute nel presente Regolamento hanno carattere vincolante per i dipendenti della TL e devono essere considerate aggiuntive rispetto alle norme disciplinari già in vigore presso la stessa. Eventuali violazioni del presente Regolamento (così come della normativa a cui lo stesso rinvia) possono avere gravi ripercussioni sulla TL ed i suoi dipendenti e comportare, nei confronti del dipendente inadempiente, l'applicazione di sanzioni disciplinari, in conformità alle disposizioni di legge e del contratto collettivo applicabile.

Possono essere adottate misure disciplinari anche nei confronti di qualsiasi superiore che richieda o approvi tali comportamenti, ovvero sia a conoscenza degli stessi e non agisca prontamente per correggerli. I comportamenti che costituiscono violazione del presente Regolamento possono violare,

nel contempo, anche disposizioni di legge tali da comportare per il dipendente inadempiente conseguenze di natura civile e penale (di carattere pecuniario o detentivo). Anche la TL può essere perseguita e sanzionata in conseguenza della condotta dei suoi dipendenti. Ai dipendenti potrà venire richiesto di risarcire i danni derivanti dalla violazioni del presente Regolamento, sulla base delle procedure stabilite dal contratto collettivo applicabile. Il presente Regolamento verrà affisso e pubblicato, ai sensi degli artt. 7 e ss. della legge 300/70 in un luogo accessibile a tutti.