DELIBERAZIONE N. 7

Oggetto: regolamento sull'utilizzo delle risorse informatiche - adozione

L'anno duemiladiciannove, il giorno 30 del mese di ottobre;

Il Presidente

VISTO lo Statuto dell'Ente e, in particolare, l'articolo 8, comma 3, lettera d), dello Statuto Nazionale LILT;

VISTO il regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, in materia di trattamento dei dati personali;

VISTO il provvedimento del 1° marzo 2007 con il quale il Garante per la Protezione dei dati Personali interviene in materia di corretto utilizzo della posta elettronica e della rete internet da parte dei lavoratori nell'ambito delle funzioni lavorative, dettando regole in materia di trattamento dei dati dei dipendenti da parte dei datori di lavoro;

VISTE in particolare, le funzioni e le responsabilità previste da detto regolamento:
- del titolare del trattamento dei dati personali (artt. 24 e ss. del citato regolamento UE 2016/679);
- del responsabile del trattamento dei dati personali (artt. 28 e ss. del citato regolamento UE 2016/679);
- del responsabile della protezione dei dati personali (di seguito anche Data Protector Officer – DPO, di cui agli artt. 37, 38 e 39 del citato regolamento UE 2016/679);

CONSIDERATO che il mutato assetto normativo in materia impone l'adozione di misure operative per un corretto trattamento dei dati personali, in applicazione del citato regolamento UE 2016/679, entro il termine del 25 maggio 2018;

LILT
LEGA ITALIANA PER LA LOTTA CONTRO I TUMORI
prevenire è vivere

SEDE CENTRALE

VISTA la deliberazione del Presidente Nazionale n. 7 del 23 maggio 2019 ratificata con deliberazione del Consiglio Direttivo Nazionale della LILT n.10 del 12 giugno 2018 con la quale è stato incaricato il Direttore Generale della LILT di curare la gestione di tutte le misure necessarie per l'attuazione il coordinamento ed il corre;
to funzionamento del presente modello organizzativo;

VISTO il regolamento sull'utilizzo delle risorse informatiche della Sede Centrale della LILT proposto dal Direttore Generale allegato alla presente delibera di cui ne fa parte integrante;

RITENUTO pertanto necessario adottare il citato regolamento sull'utilizzo delle dotazioni informatiche della LILT da applicare a tutti gli utenti autorizzare ad utilizzare le risorse informatiche, telematiche ed i dispositivi aziendali in genere a qualsiasi titolo messi a disposizione da parte della LILT;

DELIBERA

- di approvare il "Regolamento sull'utilizzo delle risorse informatiche" che, allegato al presente provvedimento, ne costituisce parte integrante e sostanziale;
- di sottoporre la presente deliberazione al Consiglio Direttivo Nazionale nella prossima riunione, per la relativa ratifica, ai sensi dell'art. 8, comma 3, lettera d) dello Statuto Nazionale della LILT;
- di trasmettere via email copia del presente provvedimento per favorirne la massima diffusione a tutto il personale e di pubblicarlo sul sito web della LILT – sezione "Amministrazione Trasparente";
- di dare atto che il presente provvedimento non comporta oneri di spesa.

Il Presidente
Prof. Francesco Schittulli

INDICE

INTRODUZIONE

1. CAMPO DI APPLICAZIONE....3
2. DEFINIZIONI....3
3. UTILIZZO DEGLI STRUMENTI AZIENDALI....4
4. MODALITÀ DI ACCESSO E DI UTILIZZO....6
5. UTILIZZO E CONSERVAZIONE DI SUPPORTI RIMOVIBILI....8
6. UTILIZZO DELLA POSTA ELETTRONICA....9
7. USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI....12
8. PROTEZIONE ANTIVIRUS....13
9. UTILIZZO DI SMARTPHONE, CELLULARE, TABLET, FAX, TELEFONI E FOTOCOPIATRICI AZIENDALI....13
10. INTERVENTI TECNICI SUGLI STRUMENTI AZIENDALI....15
11. OSSERVANZA DELLE DISPOSIZOINI IN MATERIA DI PRIVACY....16
12. SISTEMI DI CONTROLLO GRADUALI....17
13. AMMINISTRATORE DI SISTEMA....18
14. SANZIONI....18
15. AGGIORNAMENTO E REVISIONE....19

Il presente documento contiene le regole di comportamento (di seguito "**Policy sull'utilizzo delle dotazioni tecnologiche ed informatiche della Lilt")** per l'utilizzo delle dotazioni tecnologiche e informatiche della LILT – Lega Italiana per la Lotta Contro i Tumori (di seguito anche solo **"LILT"** oppure il "**Titolare**"), con particolare riferimento alle misure di sicurezza indicate dalla vigente normativa applicabile:

- Regolamento UE 2016/679 - Regolamento Europeo in materia di protezione dei dati personali (GDPR);
- D.Lgs. 196/2003 - Codice in materia di protezione dei dati personali - integrato con le modifiche introdotte dal D.Lgs 101/2018 (Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016);
- normativa di carattere nazionale
- linee guida della Autorità Garante per la protezione dei dati personali, ove applicabili e non espressamente o implicitamente abrogate.

Con l'adozione della presente Policy, in particolare, si intende contribuire alla massima diffusione della cultura della sicurezza dei sistemi informativi ed informatici e, al tempo stesso, evitare che comportamenti inconsapevoli degli Utenti autorizzati a utilizzare le risorse aziendali possano costituire una minaccia alla sicurezza del patrimonio informativo e dei sistemi informatici della LILT, ovvero dare luogo a eventuali responsabilità civili, penali ed amministrative del Titolare conseguenti alla violazione di specifiche disposizioni di legge e/o regolamentari, nonché nuocere all'immagine della LILT stessa.

Nel rispetto delle "*Linee guida del Garante per posta elettronica e Internet*", adottate dall'Autorità Garante per la protezione dei dati personali il 1 Marzo 2007, la presente **Policy** pone, in particolare, alcune opportune limitazioni all'utilizzo

personale delle risorse informatiche e di ogni dispositivo aziendale concesso in uso ai dipendenti - a tempo pieno o parziale, a tempo determinato ed indeterminato - senza distinzione di ruolo e/o livello, ed in genere a tutti i collaboratori, a prescindere dal rapporto contrattuale intrattenuto con la LILT (a mero titolo di esempio: collaboratori a progetto, stagisti, consulenti, dipendenti di aziende esterne legate da contratti di fornitura di servizi, etc.).

Nella presente **Policy** questi soggetti sono definiti Utenti autorizzati o "**Utenti**".

La presente Policy entrerà in vigore il giorno successivo alla data di invio ai dipendenti tramite posta elettronica. Con l'entrata in vigore del presente regolamento, tutte le disposizioni in precedenza adottate in materia, in qualunque forma comunicate, dovranno ritenersi abrogate e sostituite dalla presente.

Copia della presente Policy verrà messa a disposizione all'interno dell'intranet dell'Ente.

La presente **Policy** può essere soggetta a revisione periodica da parte della LILT, anche su indicazione del DPO (Data Protection Officer).

1. CAMPO DI APPLICAZIONE

1.1 La **Policy** sull'utilizzo delle dotazioni tecnologiche ed informatiche della LILT si applica a tutti gli Utenti autorizzati ad utilizzare le risorse informatiche e telematiche ed i dispositivi aziendali in genere – come di seguito specificati in dettaglio (collettivamente: "**Strumenti Aziendali**") – a qualsiasi titolo messi a disposizione da parte della LILT.

1.2 La presente Policy deve essere osservata da tutti gli Utenti, come sopra definiti, in possesso di dotazioni tecnologiche e informatiche.

2. DEFINIZIONI

Utente internet (base): persona autorizzata ad accedere alla lista dei siti istituzionali preventivamente selezionati dall'Ente;

Utente internet (ampio): persona autorizzata ad accedere al servizio internet al di là dei siti istituzionali preventivamente selezionali dall'Ente, con l'unico limite di filtri predeterminati che si attivano in modo automatico durante la navigazione;

White list: elenco di siti direttamente e immediatamente accessibili da tutti gli utenti internet (base);

Internet Provider: azienda che fornisce alla Società il canale di accesso alla rete internet;

Postazione di lavoro: personal computer collegato alla rete tramite il quale l'utente accede ai servizi;

Log: archivio delle attività di consultazione in rete.

3. UTILIZZO DEGLI STRUMENTI AZIENDALI

3.1 Gli Utenti devono custodire con la massima diligenza gli Strumenti Aziendali concessi in uso dalla LILT al fine di proteggere il patrimonio aziendale e ridurre al minimo sia i rischi di danneggiamento dei sistemi informativi e informatici, sia i rischi di distruzione o perdita dei dati ivi contenuti.

3.2 Gli Strumenti Aziendali devono essere usati solo ed esclusivamente in relazione all'espletamento delle funzioni assegnate ed agli incarichi ricoperti, per scopi legati all'attività della LILT e non per scopi personali. Ogni utilizzo non inerente all'attività lavorativa è serveramente vietato.

3.3 L'accesso ai sistemi informatici della LILT può avvenire solo attraverso il personal computer e/o attraverso gli altri Strumenti aziendali a ciò abilitati, concessi in dotazione all'Utente ed utilizzando specifiche credenziali di accesso.

3.4 È proibita l'installazione e l'uso di programmi diversi da quelli ufficialmente approvati e/o installati dalla LILT, fatta eccezione per specifiche, particolari e comprovate esigenze, da comunicarsi preventivamente al Responsabile ICT e formalmente approvate dal Dirigente responsabile.

3.5 Tale divieto comprende l'istallazione e l'uso di qualsiasi applicazione, anche regolarmente acquistata dall'Utente, i programmi shareware e/o freeware, ogni

eventuale software scaricato da Internet o proveniente da CD/DVD ovvero ogni altro software eventualmente posseduto a qualsiasi titolo.

3.6 In ogni caso, fatto salvo quanto disciplinato sopra per ciò che concerne l'installazione per specifiche, particolari e comprovate esigenze, non è consentito agli Utenti modificare le caratteristiche software e/o hardware impostate per gli Strumenti Aziendali ed i sistemi informatici in genere della LILT. L'inosservanza della presente disposizione, oltre a mettere a rischio la sicurezza e la funzionalità dei sistemi informatici della LILT, potrebbe esporre l'Utente e l'Ente a gravi responsabilità civili e penali, in caso di violazioni di diritti di proprietà intellettuale sui software e della normativa relativa ai crimini informatici.

3.7 Gli Utenti sono tenuti a cancellare i file obsoleti e/o inutili dagli Strumenti Aziendali concessi loro in dotazione. Particolare attenzione deve essere prestata alla possibile duplicazione di dati ed al *versioning* dei file, per evitare rischi legati alla gestione degli archivi ed alla corretta conservazione di dati aggiornati. Per questi motivi, è vietata la creazione di banche dati (di qualsiasi dimensione) sui propri Strumenti Aziendali, fatti salvi i casi espressamente autorizzati in tal senso.

3.8 Il personal computer deve essere spento al termine di ogni sessione di lavoro, ovvero in caso di prolungata assenza dalla postazione di lavoro. Ogni qual volta gli Utenti debbano allontanarsi dalla propria postazione di lavoro, anche per breve tempo, devono aver cura di:

- prevenire l'accesso ai dati personali trattati o ad informazioni confidenziali, attivando la funzione di "blocco" - con riattivazione per mezzo di password - e disattivando le applicazioni in uso in quel momento;
- non lasciare supporti aziendali per la memorizzazione dei dati (Hard disk removibili, CD/DVD, chiavi USB, etc.) incustoditi ed alla portata di chiunque.

3.9 Per evitare comunque l'accessibilità ai dati personali degli Utenti da parte di terzi non autorizzati, dopo 3 minuti di inattività è previsto il blocco automatico

del personal computer, con l'obbligo di reinserire da parte degli Utenti la propria password per poter effettuare nuovamente l'accesso.

3.10 Gli Utenti dovranno segnalare tempestivamente al Responsabile ICT ed al Dirigente responsabile l'eventuale furto, danneggiamento o malfunzionamento del personal computer assegnatogli.

3.11 Inoltre, in caso di furto, gli Utenti dovranno sporgere, entro le 24 ore dallo stesso, regolare denuncia alle Autorità competenti, fornendone tempestivamente copia al Dirigente responsabile attraverso i consueti canali ufficiali in utilizzo previsti dalla LILT.

3.12 L'Ente rende noto che il personale incaricato del servizio di assistenza tecnica è stato autorizzato a compiere interventi nel sistema informativo diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad esempio aggiornamento, sostituzione, implementazione di prammi, ecc.).

3.13 Il personale incaricato del servizio di assistenza tecnica ha facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, Spyware, malware ecc.

4. MODALITÀ DI ACCESSO E DI UTILIZZO

4.1 Per accedere ai servizi informatici da una postazione di lavoro, l'Utente dovrà utilizzare un codice identificativo e una password.

4.2 Qualsiasi interazione tra il sistema informatico aziendale e gli Utenti è possibile unicamente in seguito alla loro identificazione e autenticazione, effettutate tramite l'inserimento di tali apposite credenziali d'accesso personali.

4.3 Le credenziali di accesso vengono assegnate agli Utenti sulla base dell'effettiva necessità di utilizzo dei sistemi informatici aziendali. Le credenziali consistono in:

- un codice per l'identificazione dell'Utente (*User ID*), composto dall'iniziale del nome seguita dal cognome (es: m.rossi)

- una parola chiave riservata (*password*) *standard* che dovrà essere modificata obbligatoriamente dall'Utente al primo accesso.

4.4 A ciascun *User ID* è associato un profilo di accesso alla rete ed alle informazioni aziendali, definito per ciascun Utente in relazione alle funzioni assegnate ed agli incarichi ricoperti.

4.5 Le credenziali di accesso dovranno essere obbligatoriamente disattivate, dietro richiesta del Servizio Risorse Umane, nel caso in cui:

- non vengano utilizzate per un periodo superiore a tre (3) mesi;
- l'Utente non abbia più necessità di accesso al sistema informatico aziendale ovvero non possieda più una simile autorizzazione.

4.6 Al fine di garantire una corretta gestione delle credenziali di accesso, l'Utente dovrà rispettare le seguenti previsioni:

- le *password* sono strettamente personali e non sono cedibili a terzi, per nessun motivo;
- le *password* debono essere conservate nella massima riservatezza e con la massima diligenza;
- non devono essere utilizzate le credenziali degli altri utenti, neanche se fornite volontariamente o laddove se ne abbia casualmente conoscenza;
- le *password* devono essere autonomamente modificate al momento del primo utilizzo ovvero alla scadenza periodica, preimpostata centralmente dal Servizio ICT;
- le *password* impostate dall'Utente non devono contenere riferimenti agevolmente riconducibili alla sua persona; devono essere composte da almeno otto (8) caratteri alfanumerici oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito dalla tecnologia al momento operante;
- l'mpostazione della *password* è definita e regolata dal sistema di autenticazione della LILT.

4.7 Chiunque venga a conoscenza delle credenziali di accesso di un altro utente è obbligato a informarne l'utente stesso e il Responsabile al fine di porovvedere al cambio della password.

4.8 È assolutamente proibito operare nel sistema informatico aziendale autenticandosi per mezzo di credenziali di accesso diverse da quelle assegnate.

4.9 Tutti gli utenti sono obbligati a mantenere il più stretto riserbo sui dati trattati e conosciuti durante l'utilizzo di tutti gli Strumenti Aziendali; inoltre, l'immissione/modifica di dati va eseguita con la massima prudenza.

4.10 L'Utente è civilmente responsabile per qualunque danno arrecato all'Ente e all'internet provider e/o a terzi in dipendenza della mancata osservazione di quanto previsto dalla presente Policy.

5. UTILIZZO E CONSERVAZIONE DI SUPPORTI RIMOVIBILI

5.1 È vietato l'installazione e l'utilizzo di supporti rimovibili personali (floppydisk, CD, DVD riscrivibili e non, supporti USB, ecc.), salvo che non vi sia stata una preventiva formale autorizzazione da parte del Titolare ed unicamente a fini connessi alla attività lavorativa.

5.2 L'Utente è responsabile della custodia dei supporti rimovibili aziendali, se in dotazione, nonché dei dati e delle informazioni aziendali in essi contenuti. Tutti i supporti rimovibili (*Hard disk* removibili, CD/DVD, supporti USB di vario genere, ecc.), contenenti dati e informazioni aziendali devono essere trattati con particolare cautela, per evitare che il loro contenuto possa essere accessibile da parte di soggetti non autorizzati, ovvero modificato, trafugato o distrutto.

5.3 In particolare, i supporti rimovibili, se in dotazione, non possono essere lasciati incustoditi e devono essere sempre opportunamente riposti in sicurezza (ad esempio, in armadi e/o cassetti chiusi a chiave) alla fine di ogni sessione di lavoro.

5.4 I supporti esterni assegnati in dotazione dalla LILT ed utilizzati per l'eventuale archiviazione dei dati definiti "particolari" ai sensi dell'art. 9 del Regolamento Regolamento UE 2016/679 – Regolamento Europeo in materia di protezione dei dati personali ("GDPR") - non possono essere:

- riutilizzati per altri scopi;
- smaltiti autonomamente in caso di malfunzionamento.

5.5 A tal riguardo, l'Utente dovrà riconsegnare i supporti rimovibili in dotazione al Servizio ICT, che provvederà alla cancellazione permanente e sicura dei dati sensibili in essi contenuti e, ove necessario, alla loro distruzione fisica.

5.6 Nel caso in cui sia necessario reimpiegare per altri scopi supporti rimovibili utilizzati per l'archiviazione di dati particolari, il responsabile incaricato provvederà alla cancellazione definitiva dei dati, precedentemente ivi contenuti, assicurando che non possano essere recuperati in alcun modo.

6. UTILIZZO DELLA POSTA ELETTRONICA

6.1 L'indirizzo di posta elettronica (*account; e-mail*) aziendale assegnato all'Utente è uno strumento di lavoro; la posta deve essere quotidianamente consultata. Ad ogni dipendente della LILT viene assegnata una casella di posta elettronica aziendale. Il nome dell'*account* di norma coincide con il "nome utente" seguito dal dominio LILT (es. m.rossi@lilt.it).

6.2 I Dirigenti possono richiedere al Servizio ICT l'attribuzione/creazione di caselle di posta elettronica personali per collaborazioni esterne temporanee, caselle di gruppo e liste di distribuzione.

6.3 È fatto pertanto divieto di utilizzare l'indirizzo di posta elettronica aziendale per finalità diverse da quelle strettamente legate all'attività lavorativa.

6.4 A tal proposito, a titolo puramente esemplificativo, l'Utente non potrà utilizzare la posta elettronica aziendale per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali 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*;
- l'invio di messaggi di tipo offensivo o sconveniente, come ad esempio messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici etc. e comunque ogni altra tipologia di messaggio che possa arrecare danno all'immagine ed alla reputazione della LILT;

- la partecipazione a "catene" telematiche. In caso di ricezione di tali e-mail, l'Utente dovrà tempestivamente avvisare il Responsabile ICT, evitando di visualizzare il contenuto del messaggio;
- scopi commerciali o di profitto personale nonché per qualsiasi tipo di attività illegale.

6.5 I messaggi di posta elettronica devono contenere un avvertimento ai destinatari del seguente tenore letterale:

"il presente messaggio contiene informazioni di natura confidenziale rivolte esclusivamente al destinatario sopra indicato. Ai fini dello svolgimento dell'attività lavorativa le eventuali risposte potranno essere conosciute da altri soggetti nell'ambito dell'organizzazione del mittente, nei limiti del necessario e in ossequio del principio di minimizzazione del trattamento. Questo messaggio di posta elettronica e il suo contenuto sono riservati e confidenziali e destinati esclusivamente al soggetto indicato nell'indirizzo. Nel caso abbiate ricevuto il presente messaggio per errore, siete pregati di darne immediata notizia al mittente e quindi di cancellare definitivamente il messaggio di posta elettronica."

6.6 Pur non essendo consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per fini personali, è pressoché impossibile escludere a priori la presenza occasionale di informazioni non attinenti all'attività lavorativa in comunicazioni ricevute dall'esterno e/o inviate dagli Utenti. In tali casi, gli Utenti dovranno immediatamente cancellare qualsiasi dato non relativo all'attività aziendale.

6.7 È assolutamente vietato aprire messaggi di posta elettronica e/o eseguire il download di file di provenienza incerta. In simili casi, gli Utenti dovranno dare immediata notizia del messaggio di posta elettronica e degli eventuali file ricevuti al Dirigente Responsabile, evitando di compiere qualsiasi tipo di azione. In ogni caso, gli Utenti dovranno prestare la massima attenzione nell'aprire i file allegati ai messaggi di posta elettronica, prima del loro utilizzo.

6.8 Gli Utenti dovranno mantenere in ordine la casella di posta elettronica aziendale loro assegnata, cancellando periodicamente i messaggi inutili o archiviando gli obsoleti, nonché eliminando gli allegati ingombranti e non rilevanti, per evitare che sia raggiunta la dimensione massima prevista e consentita dal proprio profilo.

6.9 Tutti i messaggi di posta elettronica aziendali, inviati o ricevuti, dovranno essere gestiti esclusivamente attraverso gli applicativi standard in dotazione.

6.10 Al fine di garantire la prosecuzione dell'attività aziendale, in caso di assenza dal lavoro per qualsivoglia ragione, l'Utente è tenuto ad attivare la funzionalità "*out of office*" prevista dall'applicativo standard di posta elettronica aziendale in dotazione. Tale funzionalità consentirà di indicare l'indirizzo di posta elettronica di uno o più colleghi, cui rivolgersi durante il periodo di assenza dell'Utente, ed ogni altra informazione utile.

6.11 In caso di assenza non programmata o di particolare urgenza, sempre al fine di garantire la continuità dell'attività lavorativa, il Responsabile ICT incaricato, previa autorizzazione del Dirigente Responsabile, provvederà ad accedere alla casella di posta elettronica, esclusivamente per attivare la funzione "*out of office*".

6.12 In caso di assenza improvvisa o prolungata, l'Utente delegherà esclusivamente il proprio diretto superiore gerachico, ovvero il Responsabile ICT, alla verifica del contenuto delle *e-mail* ricevute nel periodo di assenza, con l'obbligo di trasmettere ai responsabili degli uffici, eventualmente interessati, ogni informazione ritenuta rilevante per lo svolgimento dell'attività lavorativa. In tali casi, l'Utente comunicherà al proprio diretto superiore gerachico ovvero al Responsabile ICT incaricato le credenziali di accesso (*sub* paragrafo 4), in modo da permettere lo svolgimento delle operazioni di recupero ed inoltro delle *e-mail* rilevanti.

L'accesso alla casella *e-mail* dell'Utente avverrà, in ogni caso, ad opera del Responsabile ICT incaricato (ed alla presenza del diretto superiore gerarchico, qualora sia il soggetto delegato dall'Utente), dietro espressa autorizzazione del Dirigente Responsabile.

6.13 Nei casi di assenza improvvisa o prolungata dell'Utente e/o di cessazione del rapporto di lavoro, laddove la LILT abbia necessità di accedere ai dati ed alle informazioni contenuti nei dispositivi aziendali utilizzati dall'Utente, in via eccezionale, il Responsabile ICT incaricato, con la presenza del diretto superiore gerarchico e previa autorizzazione del Dirigente Responsabile,

effettuerà l'accesso a tale dispositivo, al solo fine di recuperare file e altri contenuti di interesse per la LILT.

6.14 Delle attività descritte in questa sottosezione dovrà essere redatto apposito verbale e, ove possibile, informato l'Utente alla prima occasione utile. Al ritorno al lavoro, l'Utente dovrà impostare nuove *password* di accesso agli Strumenti Aziendali.

7. USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

7.1 Ogni postazione lavorativa deve essere collegata alla rete aziendale della LILT. Eventuali eccezioni vanno esplicitamente autorizzate dal Servizio ICT e autorizzate dal Titolare.

7.2 L'accesso alla rete aziendale (LAN o WIFI) avviene con gli Strumenti aziendali concessi in dotazione dalla LILT e previo inserimento delle proprie credenziali da parte dell'Utente. Come descritto nel capitolo *sub* 4, ciascun Utente accede alle risorse di rete con i diritti associati al proprio profilo aziendale.

7.3 Le credenziali di accesso alla rete, le cui regole di complessità sono definite dal Servizio ICT, hanno scadenza predefinita; il sistema procederà automaticamente alla richiesta di aggiornamento. È vietato modificare la propria configurazione, a meno di specifiche esigenze di servizio che vanno formalmente approvate dal Dirigente Responsabile.

7.4 È proibito l'utilizzo della rete internet per finalità diverse da quelle strettamente legate all'attività lavorativa.

7.5 A titolo puramente esemplificativo, l'Utente non potrà utilizzare la rete Internet:

- per l'*upload* o il *download* di *software* gratuiti (*freeware, shareware*) e di qualsiasi *file* non strettamente attinenti all'attività lavorativa;
- per effettuare la registrazione e/o l'accesso a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- per la partecipazione a *social network*, forum non relativi all'attività lavorativa, ovvero utilizzare *chat line* (esclusi gli strumenti appositamente ed eventualmente autorizzati dal Titolare), anche utilizzando pseudonimi

(o *nick-names*), se non espressamente autorizzati dal responsabile di ufficio.

7.6 Per garantire l'efficacia dei *backup* periodici a cura del Servizio ICT - e quindi di eventuali operazioni di ripristino dei dati - gli Utenti devono creare, utilizzare e depositare i propri *files* di lavoro nelle *directory* di rete assegnate (es. *workcom*, cartelle di progetto, di ufficio, ecc.).

7.7 È vietato depositare sulle *directory* di rete assegnate *files* personali (es. musica, filmati, foto, ecc.), che non siano strettamente e direttamente legati all'attività lavorativa.

7.8 Le medesime regole valgono per il c.d. "*file sharing aziendale*" (es. *workcom*), ovvero l'utilizzo di *files* presenti in *directory* di rete condivise tra più utenti o gruppi.

7.9 I dischi e/o le altre unità di memorizzazione locali (es. *Hard Disk* del proprio *personal computer* aziendale assegnato) non sono soggette alle periodiche *policy* di salvataggio e *backup* da parte del Servizio ICT. Pertanto, va effettuata, periodicamente, a cura diretta degli Utenti stessi, la pulizia dei *files* inutilizzati o duplicati, sia sui *personal computer* in dotazione che sulle cartelle di rete assegnate.

8. PROTEZIONE ANTIVIRUS

8.1 L'Utente deve prestare la massima diligenza nell'uso degli Strumenti Aziendali, in modo tale da ridurre i rischi - rappresentati da virus e *software* simili - alla sicurezza del sistema informatico aziendale e dei dati trattati dal Titolare.

8.2 I sistemi informatici sono protetti da un *software* antivirus aggiornato centralmente quotidianamente. Nel caso in cui il sistema di protezione rilevi la presenza di un *software* pericoloso (virus, *malware*, *trojans*, etc.) senza essere in grado di rimuoverlo, l'Utente dovrà immediatamente rivolgersi al Servizio ICT.

9. UTILIZZO DI SMARTPHONE, CELLULARE, TABLET, FAX, TELEFONI E FOTOCOPIATRICI AZIENDALI

9.1 Lo *smartphone*, il cellulare, il *tablet*, il fax, il telefono e la fotocopiatrice aziendali sono strumenti di lavoro e non sono utilizzabili per finalità personali, salva diversa esplicita autorizzazione. È vietato, di conseguenza, l'utilizzo di *smartphone*, cellulari e *tablet* aziendali per finalità non attinenti all'attività lavorativa.

9.2 I telefoni fissi e mobili *wi-fi* della LILT possono essere esclusivamente utilizzati per telefonate di lavoro.

9.3 L'Utente, in qualità di dipendente o collaboratore a qualsiasi titolo di LILT, è l'unico soggetto autorizzato ad utilizzare lo *smartphone*, il cellulare ed il *tablet* aziendali. Si fa pertanto espresso divieto di cedere - anche solo temporaneamente - in uso o comunque far anche temporaneamente utilizzare, a titolo oneroso o gratuito, lo *smartphone*, il cellulare e/o il *tablet* a familiari e, più in generale, a terzi soggetti.

9.4 L'Utente è tenuto a comunicare alla LILT eventuali guasti, malfunzionamenti, smarrimenti o furti dello *smartphone*, del cellulare e del *tablet* aziendali, in modo da consentire alla LILT di adottare idonee misure per garantire la sicurezza e/o il recupero dei dati aziendali contenuti nel dispositivo guasto, perduto o rubato.

9.5 La concessione in uso dello *smartphone*, del cellulare e del *tablet* aziendali è limitata al periodo di vigenza del contratto di lavoro ed è subordinata alla prosecuzione del rapporto di lavoro medesimo con la LILT.

9.6 La LILT si riserva il diritto di sospendere e/o revocare definitivamente la concessione, in caso di sospetto uso non autorizzato dello *smartphone*, del cellulare e del *tablet* aziendali ovvero di intervenuta modifica delle funzioni dell'Utente assegnatario.

9.7 In caso di sospensione o revoca della concessione per qualunque motivo, l'Utente è tenuto a restituire prontamente lo *smartphone*, il cellulare e/o il *tablet* aziendali, dietro semplice richiesta di LILT.

9.8 Viste le funzionalità e l'operatività attuale degli *smartphone*, dei cellulari e dei *tablet*, molto simili a quelle di un *personal computer* (es. memorizzazione dati, ricezione *e-mail*, navigazione Internet, etc.), l'Utente dovrà osservare ogni prescrizione dettata dalla presente **Policy**, in quanto applicabile e compatibile, ed in particolare:

- l'obbligo di impostare lo *smartphone*, il cellulare ed il *tablet* in modo che sia necessario digitare il PIN per accedere alla memoria interna dei dispositivi ed alla possibilità di usufruire delle funzionalità dell'apparecchio (es. per effettuare telefonate). Il PIN dovrà essere aggiornato con la stessa periodicità delle *password* relative ai dispositivi fissi, come disciplinate al paragrafo *sub* 4;
- il divieto di utilizzare in modo improprio i sistemi di registrazione video e audio offerti dall'apparato aziendale.

10. INTERVENTI TECNICI SUGLI STRUMENTI AZIENDALI

10.1 Al fine di garantirne la piena funzionalità degli Strumenti Aziendali e la sicurezza e salvaguardia dei dati e delle informazioni di rilevanza per la LILT, sono previsti periodici interventi di natura tecnica e/o manutentiva sui sistemi informatici aziendali da parte del Servizio ICT (es. aggiornamento/sostituzione/installazione di programmi). A tale scopo, il Servizio ICT ha la facoltà di collegarsi e visualizzare da remoto il *desktop* delle singole postazioni di lavoro (*personal computer*).

10.2 L'intervento viene effettuato su iniziativa del Servizio ICT, su preventiva richiesta dell'Utente o, in caso di oggettiva necessità, a seguito della rilevazione di problemi di sicurezza nel sistema informatico aziendale. In quest'ultimo caso sarà data preventiva comunicazione all'Utente, salvo che questo non pregiudichi irrimediabilmente la necessaria tempestività ed efficacia dell'intervento tecnico. In ogni caso, qualora il Servizio ICT si connetta in remoto ad una postazione di lavoro, sullo schermo del *personal computer* in dotazione verrà visualizzato un avviso per tutta la durata del collegamento.

Detti interventi tecnici potrebbero comportare l'accesso, in qualunque momento, ai dati trattati dagli Utenti, ivi compresi gli archivi di posta elettronica, nonché la verifica dei dati di traffico internet sui siti *web*. Nel corso degli interventi di manutenzione, il Servizio ICT è tenuto a segnalare tutti gli elementi idonei, anche solo potenzialmente, a creare un danno alla LILT ovvero un pregiudizio per la sicurezza dei sistemi e dei dati aziendali, nonché a cancellare tutti i dati non attinenti alle attività lavorative, fatto salvo il caso in cui questi,

costituendo prova di illecito, debbano essere comunicati alle Autorità competenti.

10.3 Il personale incaricato dell'assistenza tecnica può, inoltre, in qualunque momento, procedere alla rimozione, sia dai *personal computer* in dotazione degli Utenti sia dalle unità di rete, di qualsiasi *file* o applicazione ritenuti pericolosi per i sistemi informatici. In tali casi, verrà data preventiva comunicazione all'Utente, a meno che ciò non pregiudichi la necessaria tempestività ed efficacia dell'intervento.

10.4 Periodicamente, e/o a valle dei *backup* programmati, il Servizio ICT effettua operazioni di cancellazione di file inutilizzati da più di 2 anni sulle cartelle di rete.

11. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA PRIVACY

11.1 Gli Strumenti aziendali considerati nella presente **Policy** costituiscono tutti strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, anche ai sensi e per gli effetti dell'art. 4, comma secondo, della Legge n.300/1970

11.2 Gli Strumenti aziendali considerati nella presente **Policy** costituiscono tutti strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, anche ai sensi e per gli effetti dell'art. 4, comma secondo, della Legge n.300/1970[1].

Conseguentemente, le informazioni raccolte sulla base di quanto indicato nella **Policy** possono essere utilizzate per tutte le finalità connesse al rapporto di lavoro, essendo stata data informazione ai lavoratori sulle corrette modalità di uso degli strumenti stessi, sugli interventi che potranno venir compiuti sul sistema informatico aziendale, ovvero sul singolo strumento, nonché sui conseguenti sistemi di controllo che possano venire eventualmente operati, fermo restando il rispetto della vigente normativa in materia di protezione dei dati personali applicabile.

11.3 Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso agli Utenti apparati *hardware* o strumenti *software* aventi come scopo precipuo il loro utilizzo quali strumenti per il controllo a distanza

1 Per quanto già detto, se, invece, in base agli applicativi, ai software e, quindi alle finalità definite, tali strumenti possono determinare un controllo a distanza, sarà necessario esperire la procedura sindacale od autorizzativa del 1° comma dell'art. 4 Legge n. 300/1970.

dell'attività dei lavoratori; peraltro, laddove l'adozione di tali apparati risultasse necessaria per finalità altre, ad esempio per esigenze organizzative e produttive, di sicurezza del lavoro e/o di tutela del patrimonio aziendale, la LILT provvederà conformemente a quanto disposto dall'art. 4, comma primo, della Legge n.300/1970, dandone opportuna informazione agli Utenti stessi[2].

12. SISTEMI DI CONTROLLO GRADUALI

12.1. In caso di problemi di sicurezza del sistema informativo e/o anomalie nell'uso degli Strumenti Aziendali, ovvero se sussistesse il rischio di violazione della presente **Policy** e/o gli estremi per l'esercizio del diritto di difesa in sede giudiziaria e/o per ottemperare ad una specifica richiesta dell'Autorità giudiziaria, la LILT, tramite il Responsabile ICT incaricato, potrà effettuare controlli nel pieno rispetto della legge e dei principi di pertinenza e non eccedenza.

12.2. Nei suddetti casi, la LILT eseguirà *in primis* un controllo sui dati aggregati relativi all'intera struttura o limitati alle aree di attività interessate da tali anomalie e malfunzionamenti. I controlli potranno concludersi con avvisi generalizzati diretti agli Utenti dell'area o settore in cui fosse stata rilevata l'anomalia, nei quali si evidenziasse l'utilizzo irregolare degli strumenti aziendali; in tal caso si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite.

12.3. Nel caso di successive e reiterate anomalie, la LILT potrà esercitare, tramite il Responsabile ICT incaricato, anche controlli su base individuale, relativamente a Utenti o categorie di Utenti specifici e per periodi di tempo strettamente limitati alla finalità innanzi illustrata.

12.4. In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati. Saranno tuttavia possibili anche controlli a campione, per verificare che non vi

2 Vedi nota precedente. Qualora si configuri un uso di strumenti aziendali che non può rientrare nelle ipotesi del comma 2° dell'art. 4 Legge n. 300/1970, la LILT dovrà applicare la procedura di accordo sindacale o autorizzazione preventive previste dal 1° comma dell'art. 4 Legge n. 300/1970.

siano violazioni della presente **Policy**, delle norme di sicurezza o di disposizioni normative.

12.5. In situazioni di maggiore criticità ed effettivo pericolo per i sistemi informatici aziendali, la LILT potrà compiere ulteriori controlli, per le sole finalità espressamente consentite dalla legge e, in ogni caso, nel pieno rispetto della normativa *pro tempore* vigente.

13. AMMINISTRATORE DI SISTEMA

13.1. In conformità alle prescrizioni del Garante per la Protezione dei Dati Personali (*cfr.* Provvedimento 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"), il Titolare ha provveduto ad attribuire le funzioni di Amministratore di Sistema a soggetti specificatamente identificati, il cui elenco completo e sempre aggiornato.

13.2. La designazione di tali soggetti è stata preceduta da adeguata valutazione delle caratteristiche di capacità, esperienza ed affidabilità dai medesimi possedute, anche in rapporto alla sicurezza dei dati personali trattati. Gli Amministratori di Sistema, inoltre, hanno ricevuto specifiche indicazioni da parte del Titolare in ordine alle funzioni assegnate e sono sottoposti a periodica verifica circa il rispetto delle misure di sicurezza previste per i dati trattati.

13.3. Agli Amministratori di Sistema sono attribuite funzioni di gestione e manutenzione delle risorse informatiche entro un ambito di operatività circoscritto. Può, altresì, essere loro attribuita la facoltà di eseguire attività di monitoraggio e controllo delle risorse informatiche stesse, in piena conformità a quanto previsto dalla presente **Policy** e dalla vigente normativa.

14. SANZIONI

14.1. Gli Utenti hanno l'obbligo di conoscere, ben comprendere e rispettare la presente **Policy**. La violazione delle relative prescrizioni potrà condurre la LILT ad adottare provvedimenti disciplinari, ivi incluso il licenziamento, nonché ad

esperire azioni civili e penali nei confronti degli Utenti, nel rispetto delle disposizioni di legge e del CCNL applicabile.

14.2. Si ricorda, inoltre, agli Utenti che l'uso illecito delle risorse Informatiche, telematiche e Strumenti aziendali di LILT può comportare l'insorgere di responsabilità - anche di carattere penale - secondo le leggi vigenti, con particolare riguardo alla normativa in materia di delitti informatici (artt. 615 ter - 615 quinquies c.p.; artt. 617 quater e 617 quinquies c.p.; 635 bis ss. c.p.; e art. 640 quinquies c.p.) e diritto di autore (Legge n. 633/1941).

14.3. È fatto obbligo a tutti gli Utenti di osservare le disposizioni contenute nella presente **Policy**. Restano in vigore, se non abrogati esplicitamente e se non contrastanti con quanto qui regolamentato, tutti i precedenti Ordini di Servizio, aventi il medesimo oggetto, emanati nel tempo dai Direttori Generali e/o dai Presidenti e/o dai Consigli di Amministrazione della LILT.

15. AGGIORNAMENTO E REVISIONE

15.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dal Dirigente responsabile in collaborazione con l'Amministratore di Sistema.

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