FILCA FEDERAZIONE ITALIANA LAVORATORI COSTRUZIONI E AFFINI CISL

FILCA CISL
00184 Roma
Via del Viminale, 43
Tel.: +39 06 4870634

Fax: +39 06 4818884
+39 06 4870647
federazione.filca@cisl.it
www.filca.cisl.it

REGOLAMENTO PER L'UTILIZZO DELLA STRUMENTAZIONE INFORMATICA E DELLA RETE INTERNET

INDICE

FILCA CISL
00184 Roma
Via del Viminale, 43
Tel.: +39 06 4870634

Fax: +39 06 4818884
+39 06 4870647
federazione.filca@cisl.it
www.filca.cisl.it

CAPO I –PRINCIPI

1. SCOPO

Lo scopo del presente disciplinare interno (di seguito anche solo il "Regolamento") è di definire l'ambito di applicazione, le modalità e le norme sull'utilizzo della strumentazione informatica da parte degli utenti assegnatari (dipendenti, collaboratori etc.), al fine di tutelare i beni ed evitare condotte inconsapevoli e/o scorrette che potrebbero esporre il Titolare a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi.

L'insieme delle norme comportamentali ivi incluse, pertanto, è volto a conformare il Titolare ai principi di diligenza, informazione e correttezza nell'ambito dei rapporti di lavoro, con l'ulteriore finalità di prevenire eventuali comportamenti illeciti degli utenti, pur nel rispetto dei diritti ad essi attribuiti dall'ordinamento giuridico italiano.

A tal fine, pertanto, si rileva che gli eventuali controlli ivi previsti escludono finalità di monitoraggio diretto ed intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa, con particolare riferimento al Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati – di seguito anche solo GDPR)), alla Legge n. 300/1970 (c.d. Statuto dei Lavoratori) alla luce delle modifiche intervenute ad opera del D.lgs. 14 settembre 2015, n. 151 ed ai provvedimenti appositamente emanati dall'Autorità Garante (si veda in particolare Provv. 1° marzo 2007 oggi vigente).

2. APPLICABILITÀ

Il presente regolamento si applica a tutto il personale del Titolare nonché al personale esterno assegnatario di beni e risorse informatiche ovvero utente di servizi e risorse informative di pertinenza del Titolare.

3. TERMINI E DEFINIZIONI

– Il Titolare: l'organizzazione/struttura e/o comunque il titolare dei beni e delle risorse informatiche ivi disciplinate, il quale opererà per mezzo dei soggetti che ne possiedono la rappresentanza.

– Il DPO: Data Protection Officer - il responsabile della protezione dei dati personali

– Chat: servizio offerto da Internet, che mediante apposito software permette a più interlocutori di conversare scambiandosi messaggi scritti che appaiono in tempo reale sul monitor di ciascuno;

– Client: personal computer collegato in rete a un altro computer (server), sul quale risiedono i dati che il primo utilizza;

– Computer portatile: elaboratore elettronico trasportabile con facilità;

– E-mail: messaggio inviato tramite posta elettronica;

– Estensione: set di uno o più caratteri (in genere tre) che segue il nome di un file di un computer e ne identifica il genere;

– Log: registrazione ufficiale di eventi;

– Password: parola o sigla di riconoscimento fornita dall'utente al computer per poter accedere a un sistema operativo a un programma o a un file;

– Peer to peer: sistema di computer collegati gli uni agli altri senza la connessione ad un server;

– Personal Computer: elaboratore elettronico destinato all'uso interno;

FILCA CISL
00184 Roma
Via del Viminale, 43
Tel.: +39 06 4870634

Fax: +39 06 4818884
+39 06 4870647
federazione.filca@cisl.it
www.filca.cisl.it

– Phishing: l'attività criminale di mandare e-mail o costituire un sito web al fine di ingannare qualcuno e carpire informazioni (es. numeri di carta di credito o password).

– Rete: sistema di trasmissione delle informazioni costituito da linee di collegamento e da stazioni che possono essere costituite da elaboratori, terminali o unità di memoria;

– Server: computer collegato in rete ad altri computer (client), sul quale risiedono i dati che questi utilizzano;

– Smartphone: apparecchio elettronico che combina le funzioni di un telefono cellulare e di un computer palmare.

– Spamming: mandare messaggi a diverse persone tramite e-mail o internet generalmente a fini commerciali;

– Tablet: elaboratore elettronico compatto con interfaccia touch;

– Utente: colui che si serve di un'attrezzatura per svolgere delle attività;

– Malware: qualsiasi tipo di software dannoso creato al fine di infettare computer o dispositivi mobile, per rubare informazioni commerciali o private, password, oppure per impedire agli utenti di accedere ai propri dispositivi;

– Ransomware: è un tipo di malware che limita l'accesso del dispositivo che infetta. In seguito, è richiesto un riscatto per rimuovere la limitazione;

– Cryptolocker: appare come un semplice allegato di posta elettronica, ma in realtà è un ransomware creato allo scopo di cifrare i dati del computer della vittima, di fatto bloccandolo. Viene poi richiesto il pagamento di un riscatto per ripristinare i dati cifrati;

– VPN: la Virtual Private Network (o, tradotta, rete virtuale privata), è una rete di telecomunicazioni privata, in quanto per accedervi sono richiesti un account e una password, instaurata mediante un ponte di connessione virtuale tra i soggetti che la utilizzano e uno dei server della VPN;

– Rete B2B: descrive le transazioni commerciali elettroniche tra imprese, ad esempio anche con i propri fornitori.

4. TITOLARITÀ DEI BENI E DELLE RISORSE INFORMATICHE

I beni e le risorse informatiche, i servizi ICT e le reti informative costituiscono esclusiva proprietà del Titolare.

Il loro utilizzo, pertanto, è consentito solo per finalità di adempimento delle mansioni lavorative affidate ad ogni Utente in base al rapporto in essere. È fatta eccezione per dispositivi affidati all'utente come benefit aziendale.

Si precisa sin d'ora che qualsivoglia dato e/o informazione trattato per mezzo dei beni e delle risorse informatiche di proprietà del Titolare sarà dallo stesso considerata come avente natura riservata.

5. RESPONSABILITÀ PERSONALE DELL'UTENTE

Ogni Utente è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidatigli dal Titolare.

A tal fine ogni Utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con il Titolare, è tenuto a tutelare (per quanto di propria competenza) il patrimonio da utilizzi impropri e non autorizzati per iscritto dal Titolare e/o dal Responsabile, danni o abusi anche derivanti da negligenza, imprudenza o imperizia. L'obiettivo è quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse.

Ogni Utente, pertanto, è tenuto, in relazione al proprio ruolo e alle mansioni in concreto svolte, ad operare a tutela della sicurezza informatica, riportando al proprio responsabile e senza ritardo eventuali rischi di cui è a conoscenza ovvero violazioni del presente Regolamento.

Sono vietati comportamenti che possano creare un danno, anche di immagine, al Titolare.

FILCA CISL
00184 Roma
Via del Viminale, 43
Tel.: +39 06 4870634

Fax: +39 06 4818884
+39 06 4870647
federazione.filca@cisl.it
www.filca.cisl.it

CAPO II – MISURE ORGANIZZATIVE

6. AMMINISTRATORI DEL SISTEMA

Il Titolare conferisce all'amministratore di sistema interno il compito di sovrintendere i beni e le risorse informatiche. I principali compiti, a titolo meramente esemplificativo e non esaustivo, sono:

1) gestire l'hardware e il software di tutta la strumentazione informatica di appartenenza del Titolare;

2) gestire la creazione, l'attivazione, la disattivazione e tutte le relative attività amministrative degli account di rete e dei relativi privilegi di accesso alle risorse, previamente assegnati agli utenti;

3) monitorare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi affidati agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;

4) creare, modificare, rimuovere o utilizzare qualunque account o privilegio purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;

5) rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;

6) provvedere alla sicurezza informatica dei sistemi informativi, nel rispetto di quanto prescritto dal GDPR;

7) utilizzare le credenziali di accesso di amministratore del sistema per accedere, anche da remoto, ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un Utente in caso di prolungata assenza, irreperibilità o impedimento dello stesso. Nel caso si tratti di intervenire su account di applicativi gestiti centralmente dalla confederazione o aventi amministratori di sistema esterni, la richiesta deve provenire dal Titolare e/o dal Responsabile per iscritto;

8) rimuovere i file installati, scaricati o, comunque, presenti sul computer, sugli applicativi affidati all'utente, sui server o su unità *storage* di backup della struttura, per la cui installazione e conservazione non era stata precedentemente richiesta ed ottenuta espressa autorizzazione scritta da parte del Titolare e/o del Responsabile

7. ASSEGNAZIONE DEGLI ACCOUNT E GESTIONE DELLE PASSWORD

Creazione e gestione degli Account

Un account Utente consente l'autenticazione dell'utente e di conseguenza ne disciplina l'accesso alle risorse informatiche, per singola postazione lavorativa.

La gestione di tali account segue quanto sotto espressamente previsto:

- l'accesso al proprio account avviene tramite l'utilizzo delle "credenziali di autenticazione" (es. "Username" e "Password"), comunicate all'Utente dall'amministratore di sistema, che le genera, attraverso modalità che ne garantiscano la segretezza;

- le credenziali di autenticazioni costituiscono dati da mantenere strettamente riservati e non è consentito comunicarne gli estremi a terzi;

- se l'Utente ha il sospetto che le proprie credenziali di autenticazione siano state identificate da qualcuno, o il sospetto di un utilizzo non autorizzato del proprio account e delle risorse a questo associate, lo stesso è tenuto a modificare immediatamente la password e/o a segnalare la violazione all'amministratore del sistema nonché al Responsabile privacy di riferimento;

- ogni Utente è responsabile dell'utilizzo del proprio account Utente;

FILCA CISL
00184 Roma
Via del Viminale, 43
Tel.: +39 06 4870634
Fax: +39 06 4818884
+39 06 4870647
federazione.filca@cisl.it
www.filca.cisl.it

Nel caso, invece, la struttura necessiti conoscere il contenuto dei messaggi di posta elettronica dell'utente resosi assente per cause improvvise o per improrogabili necessità legate all'attività lavorativa, si procederà come segue:

- la verifica del contenuto dei messaggi sarà effettuata per il tramite del responsabile diretto;
- al suo rientro l'utente, riceverà una email che lo informerà dell'attività svolta dal responsabile IT e dal responsabile di area;
- sarà preventivamente richiesto all'utente di farlo lui stesso, se possibile, tramite web mail.

Gestione e utilizzo delle password

Dopo la prima comunicazione delle credenziali di autenticazione da parte dell'amministratore di sistema, l'Utente ha il compito di modificare, al suo primo utilizzo, la propria password, procedendo allo stesso modo ogni volta al verificarsi del sospetto che sia venuta a conoscenza di altri.

L'Utente, nel definire il valore della password, deve rispettare le seguenti regole:

- utilizzare almeno 8 caratteri alfanumerici, inclusi i caratteri speciali (#, %, etc.);
- utilizzare almeno tre delle seguenti categorie: un carattere maiuscolo, un carattere minuscolo, un numero, un carattere non alfanumerico tipo "@#§£$%...";
- evitare di includere parti del nome, cognome e/o comunque elementi a lui agevolmente riconducibili;
- evitare l'utilizzo di password comuni e/o prevedibili;
- proteggere con la massima cura la riservatezza della password ed utilizzarla entro i limiti di autorizzazione concessi.

Qualora vi sia richiesta inviata per iscritto all'amministratore di sistema, di reset password di un utente a qualsiasi titolo, perché, per esempio, sussiste il dubbio che terzi ne siano venuti a conoscenza o perché dimenticata, l'amministratore di sistema procederà a riassegnare una nuova password temporanea al fine di consentire all'utente l'accesso ai sistemi presso cui è accreditato, con l'impegno di modificarla subito dopo nei termini sopra individuati.

Si ricorda che scrivere la password su post-it o altri supporti (ivi compresa la sua memorizzazione sul telefono/smartphone) non è conforme alla normativa e costituisce violazione del presente Regolamento.

Cessazione degli Account

In caso di interruzione del rapporto con l'Utente, le credenziali di autenticazione di cui sopra verranno disabilitate.

8. POSTAZIONI DI LAVORO

Per postazione di lavoro si intende il complesso unitario di Personal Computer (di seguito, PC), notebook, accessori, periferiche e ogni altro *device* concesso dal Titolare in utilizzo all'Utente. L'assegnatario di tali beni e strumenti informatici ha il compito di farne un uso compatibile con i principi di diligenza sanciti nel codice civile.

Al fine di disciplinare un corretto utilizzo di tali beni, il Titolare ha adottato le regole tecniche che di seguito si riportano:

- ogni PC, notebook (accessori e periferiche incluse), e altro *device*, sia esso acquistato, noleggiato o affidato in locazione, rimane di esclusiva proprietà del Titolare ed è concesso all'Utente per lo svolgimento delle proprie mansioni lavorative e comunque per finalità strettamente attinenti l'attività svolta;
- è dovere di ogni Utente usare i computer e gli altri dispositivi a lui affidati responsabilmente e professionalmente;

FILCA CISL
00184 Roma
Via del Viminale, 43
Tel.: +39 06 4870634

Fax: +39 06 4818884
+39 06 4870647
federazione.filca@cisl.it
www.filca.cisl.it

- il PC e gli altri dispositivi di cui sopra devono essere utilizzati con hardware e software autorizzati per iscritto dal Titolare e/o dal Responsabile.
- le postazioni non devono essere lasciate incustodite con le sessioni utenti attive, quando un Utente si allontana dalla propria postazione deve bloccare tastiera e schermo con un programma salvaschermo (screensaver) protetto da password o effettuare il log-out dalla sessione;
- l'Utente deve segnalare con la massima tempestività all'amministratore del sistema ovvero al proprio Responsabile di riferimento eventuali guasti tecnici, problematiche tecniche o il cattivo funzionamento delle apparecchiature;
- è fatto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici a soggetti terzi;
- il Titolare si riserva la facoltà di rimuovere qualsiasi elemento hardware la cui installazione non sia stata appositamente e preventivamente prevista o autorizzata per iscritto dal Titolare e/o dal Responsabile.

Gli apparecchi di proprietà personale dell'Utente quali computer portatili, telefoni cellulari, Tablet, hard disk esterni, penne USB, lettori musicali o di altro tipo, fotocamere digitali, ecc. non potranno essere collegati ai computer, reti LAN o alle reti informatiche, salvo preventiva autorizzazione scritta-da parte del Titolare e/o del Responsabile.

CAPO III – CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

9. PERSONAL COMPUTER, COMPUTER PORTATILI

Devono essere utilizzati per compiere mansioni lavorative.

Ne consegue che gli utenti sono tenuti al rispetto delle seguenti regole:

- non è consentito modificare la configurazione hardware e software del proprio PC se non previa esplicita autorizzazione del Titolare e/o del Responsabile o dell'amministratore di sistema;

- non è consentito rimuovere, danneggiare o asportare componenti hardware;

- non è consentito installare autonomamente programmi se non autorizzato espressamente dal Titolare e/o dal Responsabile o dell'amministratore di sistema;

- non è consentito mantenere copie dei dati personali sul proprio computer dopo lo svolgimento delle attività in carico all'utente. I file oggetto di elaborazione o creati dall'utente dovranno pertanto essere salvati o trasferiti verso la destinazione opportuna affinché non restino sulla memoria locale.

Per quanto concerne, invece, la gestione dei computer portatili, l'Utente ha l'obbligo di custodirli con diligenza e in luogo protetto durante gli spostamenti, rimuovendo gli eventuali file elaborati prima della sua riconsegna.

Non è consentito all'Utente caricare o inserire all'interno del portatile qualsiasi dato personale non attinente con l'attività lavorativa svolta. In ogni caso, al fine di evitare e/o ridurre al minimo la possibile circolazione di dati personali sull'apparecchio, si ricorda agli utenti di cancellare tutti i dati eventualmente presenti prima di consegnare il portatile agli uffici competenti per la restituzione o la riparazione. Nel caso in cui l'Utente vi conservi, contrariamente alle direttive impartitegli, dati di natura personale, il Titolare in nessun caso potrà essere ritenuto responsabile della salvaguardia o della perdita di tali dati.

L'amministratore di sistema ha la 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, etc. L'intervento viene effettuato esclusivamente su chiamata dell'Utente e in sua presenza.

Si ricorda che al termine dell'utilizzo di ogni strumento, questo deve essere adeguatamente spento al fine di evitare la conoscibilità dei contenuti da parte di terzi non autorizzati.

FILCA CISL
00184 Roma
Via del Viminale, 43
Tel.: +39 06 4870634

Fax: +39 06 4818884
+39 06 4870647
federazione.filca@cisl.it
www.filca.cisl.it

10. SOFTWARE

Premesso che l'installazione di software privi di regolare licenza non è consentita in nessun caso, gli utenti dovranno limitarsi ad utilizzare il software fornitogli con lo strumento informatico senza installare autonomamente alcun programma, che sia gratuito o meno.

Il Titolare richiama l'attenzione del proprio personale su alcuni aspetti fondamentali che l'Utente è tenuto ad osservare per un corretto utilizzo del software:

- il Titolare acquista le licenze d'uso dei software da vari fornitori esterni. L'Utente, pertanto, è soggetto a limitazioni nell'utilizzo di tali programmi e della relativa documentazione e non ha il diritto di riprodurlo in deroga ai diritti concessigli. Tutti gli utenti sono quindi tenuti a utilizzare il software entro i limiti specificati nei contratti di licenza;

- il Titolare, sulla scorta di quanto disposto dalle normative a tutela della proprietà intellettuale e del diritto d'autore, ricorda che le persone coinvolte nella riproduzione illegale del software sono responsabili sia civilmente che penalmente e quindi possono essere condannate al pagamento dei danni e anche alla reclusione;

- il Titolare non tollererà la duplicazione illegale del software.

11. DISPOSITIVI DI MEMORIA PORTATILI

Per dispositivi di memoria portatili si intendono tutti quei dispositivi che consentono di copiare o archiviare dati, file o documenti esternamente al computer. Sono considerati tali CD-ROM, DVD, penne o chiavi di memoria USB, fotocamere digitali, dischi rigidi esterni, etc.

L'utilizzo di tali supporti risponde alle direttive che di seguito si riportano:

- non è consentito utilizzare supporti rimovibili personali per lo scambio dati, se non preventivamente autorizzati per iscritto dal Titolare e/o dal Responsabile o dell'amministratore di sistema;

- è onere dell'Utente custodire i supporti magnetici contenenti dati particolari e giudiziari in armadi chiusi a chiave, onde evitare che il loro contenuto possa essere trafugato, alterato o distrutto.

- è onere dell'utente rimuovere tutti i dati non più necessari al termine dello svolgimento delle attività.

Si precisa che, ove autorizzati per iscritto in base a quanto sopra disposto, una volta connessi all'infrastruttura informatica del Titolare, i dispositivi saranno soggetti (ove compatibili) al presente Regolamento.

12. STAMPANTI, FOTOCOPIATRICI E FAX

L'utilizzo dei suddetti strumenti deve avvenire sempre per scopi professionali. Non è consentito un utilizzo per fini diversi o privati, salvo una specifica autorizzazione scritta da parte del Titolare e/o del Responsabile.

È richiesta una particolare attenzione quando si invia su una stampante condivisa documenti aventi ad oggetto dati personali o informazioni riservate; ciò al fine di evitare che persone non autorizzate possano venirne a conoscenza. Si richiede quindi di evitare di lasciare le stampe incustodite e ritirarne immediatamente le copie non appena uscite dalla stampante.

L'utilizzo dei fax per l'invio di documenti che hanno natura strettamente confidenziale, è generalmente da evitare. Nei casi in cui questo sia necessario, si deve preventivamente avvisare il destinatario, in modo da ridurre il rischio che persone non autorizzate possano venirne a conoscenza, e successivamente chiedere la conferma telefonica di avvenuta ricezione.

FILCA CISL
00184 Roma
Via del Viminale, 43
Tel.: +39 06 4870634

Fax: +39 06 4818884
+39 06 4870647
federazione.filca@cisl.it
www.filca.cisl.it

13. STRUMENTI DI FONIA MOBILE E/O DI CONNETTIVITÀ IN MOBILITÀ

Il Titolare mette a disposizione, a seconda del ruolo o della funzione del singolo Utente, impianti di telefonia fissa e mobile, nonché dispositivi - quali smartphone e tablet - che consentono di usufruire della navigazione in internet tramite rete dati e/o del servizio di telefonia tramite rete cellulare.

L'Utente dovrà attenersi ai limiti di traffico previsti dal Titolare, potendo in caso contrario la stessa richiedere il rimborso dei costi sostenuti per il superamento degli stessi.

Si informano gli utilizzatori dei servizi di fonia che il Titolare potrà richiedere ai provider di telefonia i dettagli necessari ad effettuare controlli sull'utilizzo ed i relativi costi di traffico effettuato nel tempo al fine di una corretta fatturazione.

I controlli saranno eseguiti secondo le modalità descritte all'art. 16 del presente Regolamento.

Il Titolare si riserva la facoltà, qualora l'esame del traffico di una singola utenza rilevi uno scostamento significativo rispetto alla media del consumo, di richiedere un tabulato analitico delle chiamate effettuate dalla SIM in carico all'Utente per il periodo interessato.

L'utilizzo dei dispositivi ivi disciplinati risponde alle regole che di seguito si riportano:

- ogni Utente assegnatario del dispositivo è responsabile dell'uso appropriato dello stesso, e, conseguentemente, anche della sua diligente conservazione.

- I dispositivi devono essere dotati di protezione d'accesso a seconda della modalità consentita dal dispositivo stesso (pin, riconoscimento biometrico o altro);

- in caso di danneggiamento l'Utente assegnatario dovrà darne immediato avviso al Titolare/Responsabile, in caso di furto o smarrimento del dispositivo mobile in oggetto l'Utente assegnatario dovrà fornire al Titolare tutte le informazioni funzionali alla presentazione dell'eventuale denuncia di furto; ove detti eventi siano riconducibili ad un comportamento negligente o imprudente dell'Utente e/o comunque a sua colpa nella custodia del bene, lo stesso sarà ritenuto unico responsabile dei danni derivanti;

- al fine di evitare e/o ridurre al minimo la possibile circolazione di dati personali sull'apparecchio, si ricorda agli assegnatari di cancellare tutti i dati eventualmente presenti prima di consegnare il cellulare agli uffici competenti per la restituzione o la riparazione;

- non è consentito all'Utente effettuare procedure di jailbreak, vale a dire modifiche volte a sbloccare i dispositivi, permettendo l'installazione di software e/o applicazioni coperte da copyright o di applicazioni non sicure e non controllate.

CAPO IV – GESTIONE DELLE COMUNICAZIONI TELEMATICHE

14. GESTIONE UTILIZZO DELLA RETE INTERNET

Ogni Utente potrà essere abilitato dal Titolare alla navigazione Internet. Con il presente Regolamento si richiamano gli utenti ad una particolare attenzione nell'utilizzo di Internet e dei servizi relativi, in quanto ogni operazione posta in essere è associata all'Indirizzo Internet Pubblico assegnato al Titolare stesso.

Internet è uno strumento messo a disposizione degli utenti per uso professionale. Ciascun lavoratore, pertanto, deve usare la rete Internet in maniera appropriata, tenendo presente che ogni sito web può essere governato da leggi diverse da quelle vigenti in Italia; l'Utente deve quindi prendere ogni precauzione a tale riguardo.

Le norme di comportamento da osservare nell'utilizzo delle connessioni ad Internet sono le seguenti:

FILCA CISL
00184 Roma
Via del Viminale, 43
Tel.: +39 06 4870634

Fax: +39 06 4818884
+39 06 4870647
federazione.filca@cisl.it
www.filca.cisl.it

a. l'utilizzo è consentito esclusivamente per scopi attinenti il proprio operato e, pertanto, non è consentito navigare in siti non attinenti a predetto scopo;

b. non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica, pedopornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;

c. non è consentito lo scambio e/o la condivisione (es. i c.d. sistemi di Peer-to-Peer) a qualsiasi titolo, anche se non a scopo di lucro, di materiale audiovisivo, cinematografico, fotografico, informatico, etc., protetto da copyright;

d. non è consentito sfruttare i marchi registrati, i segni distintivi e ogni altro bene immateriale di proprietà del Titolare in una qualsiasi pagina web o pubblicandoli su Internet, a meno che tale azione non sia stata approvata espressamente.

Per facilitare il rispetto delle predette regole, il Titolare si riserva, per mezzo dell'amministratore di sistema, la facoltà di configurare specifici filtri che inibiscono l'accesso ai contenuti ove non consentiti (con esclusione dei siti istituzionali) e che prevengono operazioni non correlate all'attività lavorativa (es. upload, restrizione nella navigazione, download di *file* o software).

L'eventuale conservazione di dati è effettuata per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza, come specificamente definite all'interno del Piano di Data Retention.

15. GESTIONE E UTILIZZO DELLA POSTA ELETTRONICA E DELLA INTRANET

Creazione e gestione degli Account di posta elettronica e accesso Intranet sui sistemi nazionali

L'accesso personale alla rete nazionale Cisl e la casella (e gli eventuali indirizzi aggiuntivi) di posta elettronica sul dominio "cisl.it" per dirigenti e operatori vengono richiesti per iscritto alla confederazione dalla struttura di riferimento degli interessati a firma del Titolare della struttura stessa. La persona per la quale viene effettuata la richiesta deve essere censita nella Banca Dati Dirigenti Quadri e Operatori nazionale (BDD) per i dati anagrafici e la posizione ricoperta. Nel caso di Enti e Associazioni territoriali e regionali la richiesta scritta proviene dal relativo livello nazionale o dal livello confederale del territorio o regione corrispondente.

Viene fatto carico alla struttura richiedente di comunicare qualsiasi variazione della posizione della persona per la quale si è richiesta l'apertura account che incida sul cambiamento di profilo o sulla chiusura dell'account personale esistente (es. modifica di carica o incarico, passaggio ad altra struttura, fuoriuscita dall'organizzazione ecc.).

Principi guida

Ad ogni Utente Titolare di un account, il Titolare può provvedere ad assegnare una casella di posta elettronica individuale mediante comunicazione scritta, al fine di garantirne la tracciabilità.

I servizi di posta elettronica devono essere utilizzati in coerenza con lo scopo della struttura: si ricorda a tutti gli utenti che l'account e-mail è uno strumento di proprietà del Titolare ed è conferito in uso per l'esclusivo svolgimento delle mansioni affidate.

Ad uno stesso Utente possono essere assegnate più caselle di posta elettronica che possono essere condivise con altri utenti dello stesso gruppo/dipartimento. Tali caselle devono essere utilizzate per la ricezione dei messaggi, mentre per le risposte o gli invii, è consigliabile utilizzare la casella di posta individuale assegnata.

Attraverso l'e-mail gli utenti rappresentano pubblicamente il Titolare e per questo motivo viene richiesto di utilizzare tale sistema in modo lecito, professionale e comunque tale da riflettere l'immagine.

Gli utenti sono responsabili del corretto utilizzo delle caselle di posta elettronica e sono tenuti ad utilizzarla in

FILCA CISL
00184 Roma
Via del Viminale, 43
Tel.: +39 06 4870634

Fax: +39 06 4818884
+39 06 4870647
federazione.filca@cisl.it
www.filca.cisl.it

modo conforme alle presenti regole. Gli stessi, pertanto, devono:

- conservare la password nella massima riservatezza e con la massima diligenza;

- mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti. Il limite della dimensione della casella postale è fissato in 5 Gb per Utente, salvo eccezioni autorizzate per iscritto dal Titolare e/o dal Responsabile;

- prestare attenzione alla dimensione dei file allegati alle mail, anche in considerazione del fatto che la maggior parte dei sistemi di posta più diffusi non consentono la ricezione di allegati di dimensioni superiori ai 10MB;

Rimuovere dalla propria mailbox, al termine delle attività svolte, eventuali file contenenti dati personali soggetti a privacy, in qualsiasi formato trattati, sia inviati che ricevuti. In ogni caso, indipendentemente dalla durata dell'attività connessa al file o messaggio di posta elettronica, si richiede comunque lo stretto rispetto dei termini indicati all'interno del Piano di Data Retention.

- accertarsi dell'identità del mittente e controllare a mezzo di software antivirus i file attachment di posta elettronica prima del loro utilizzo, allegati provenienti da mittenti sconosciuti non debbono essere aperti;

- rispondere ad e-mail pervenute solo da mittenti conosciuti e cancellare preventivamente le altre;

- collegarsi a siti internet i cui link sono contenuti all'interno di messaggi solo quando vi sia comprovata sicurezza sul contenuto degli stessi.

L'utente che riceve una e-mail a carattere violento, razzista o pornografico o che rappresenti forme di spamming o phishing, ha il dovere di avvertire rapidamente l'amministratore di sistema. È vietato trasmettere e-mail di tipo professionale al proprio indirizzo privato.

Non è consentito agli utenti, al contrario:

- utilizzare la casella di posta elettronica per inviare, ricevere o scaricare allegati contenenti video, brani musicali, etc., salvo che questo non sia funzionale all'attività prestata in favore del datore di lavoro (es: presentazioni o materiali video).

Rispetto all'utilizzo della posta elettronica certificata si applicano, ove compatibili, le presenti disposizioni.

Accesso alla casella di posta elettronica della persona assente

Saranno messe a disposizione di ciascun Utente, con modalità di agevole esecuzione, apposite funzionalità del sistema di posta elettronica che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le coordinate di altro soggetto cui trasmettere le comunicazioni e-mail di contenuto lavorativo o altre utili modalità di contatto in caso di assenza del lavoratore.

In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi *webmail*), il Titolare, perdurando l'assenza oltre un determinato limite temporale pari a 30 giorni, salvo richiesta specifica autorizzata dalla Struttura, disporrà lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l'amministratore di sistema), l'attivazione di un analogo accorgimento (risposta automatica), avvertendo l'assente.

Nel caso, invece, il Titolare necessiti conoscere il contenuto dei messaggi di posta elettronica dell'Utente resosi assente per cause improvvise, si procederà come segue:

- sarà preventivamente richiesto all'utente di farlo lui stesso, se possibile, tramite web mail.

- la verifica del contenuto dei messaggi sarà effettuata per il tramite del Titolare/Responsabile di riferimento insieme al DPO, l'utente riceverà una email che lo informerà dell'attività svolta sulla propria mailbox;

FILCA CISL
00184 Roma
Via del Viminale, 43
Tel.: +39 06 4870634

Fax: +39 06 4818884
+39 06 4870647
federazione.filca@cisl.it
www.filca.cisl.it

Disabilitazione e cessazione dell'indirizzo di posta elettronica

In caso di interruzione del rapporto in essere con l'utente assegnatario, l'indirizzo di posta elettronica verrà disabilitato a partire da 5 giorni successivi alla cessazione previa comunicazione all'interessato da parte del Responsabile/Titolare.

Il Titolare/Responsabile provvederà alla conservazione dei messaggi di posta ai fini della corrispondenza istituzionale e funzionali alle attività svolte per la durata di anni 10 come previsto dal Codice Civile all'art. 2214. Tale conservazione comporterà la conservazione altresì del nominativo indicato nella mail in entrata ed uscita. Trascorso tale termine la cancellazione sarà totale.

Variazione e cessazione degli Account di posta elettronica e accesso Intranet sui sistemi nazionali

È fatto obbligo alle strutture presso cui operano i detentori di account sulla Intranet nazionale di richiederne la cessazione alla confederazione, a firma del Titolare, al venir meno delle condizioni che ne hanno determinato l'apertura, in particolare per cessazione della carica nel caso dei dirigenti, per cessazione o variazione dell'incarico nel caso di operatori e quadri.

Nel caso di fine carica del Titolare, la cessazione viene richiesta per iscritto dal subentrante o dal Titolare delle strutture di livello superiore.

In caso di variazione di carica o incarico o di cambio di struttura, la struttura interessata provvederà a richiedere all'amministrazione confederale degli account o ove presenti agli amministratori delegati alla gestione account per il proprio ambito, la variazione del profilo per le differenti abilitazioni all'accesso in lettura o lettura e scrittura, ad aree riservate e applicazioni.

Le cessazioni o variazioni degli account verranno effettuate nei tempi necessari a garantire la chiusura delle attività e il subentro di chi succede nell'incarico, e, in caso di cessazione, anche a consentire il recupero di materiali e comunicazioni personali. Vengono fatte salve le richieste di cessazione immediata per motivi di comprovata urgenza da parte del Titolare (es. per pronunciamenti della magistratura interna, adesione ad altra organizzazione, propaganda diffamatoria ecc.).

16. SMART WORKING

Rispetto alle attività svolte da remoto, restano valide le condizioni ed i principi menzionati nel presente Regolamento e si specifica quanto segue.

L'Utente deve garantire la sicurezza della connessione dalla quale si collega alla rete o gestisce file o comunicazioni elettroniche, in particolare garantendo attive misure antintrusione.

Qualora l'Utente non sia in grado di garantire la sicurezza media della rete, può operare solo in locale senza alcun collegamento a reti esterne non protette. Ogni specifica richiesta ricevuta per iscritto dal Titolare e/o Responsabile in deroga al presente paragrafo, sarà gestita di volta in volta.

17. I CONTROLLI

I principi

Relativamente ai soli dipendenti, il Titolare, in linea con quanto prescritto dall'ordinamento giuridico italiano (art. 4, Statuto dei Lavoratori), esclude la configurabilità di forme di controllo aventi direttamente ad oggetto l'attività lavorativa dell'Utente.

Ciò nonostante non si esclude che, per ragioni organizzative e produttive, di tutela del patrimonio ovvero per esigenze dettate dalla sicurezza, si utilizzino sistemi informatici, impianti, apparecchiature o dispositivi dai quali

FILCA CISL
00184 Roma
Via del Viminale, 43
Tel.: +39 06 4870634

Fax: +39 06 4818884
+39 06 4870647
federazione.filca@cisl.it
www.filca.cisl.it

derivi la possibilità di controllo a distanza dell'attività dei lavoratori. In tal caso tali strumenti verranno valutati e subordinati rispetto alla normativa di settore ed i dati acquisiti con lo strumento verranno trattati secondo l'informativa privacy Dipendenti, distaccati e collaboratori, allegata al presente Regolamento.

Fermo restando il diritto del Titolare di effettuare controlli sull'effettivo adempimento della prestazione lavorativa nonché sul corretto utilizzo dei beni e servizi informatici (artt. 2086, 2087 e 2104 c.c.), i controlli posti in essere, saranno sempre tali da evitare ingiustificate interferenze con i diritti e le libertà fondamentali dei lavoratori e non saranno costanti, prolungati e indiscriminati, nel rispetto del principio di pertinenza e non eccedenza.

Il Titolare, nel riservarsi il diritto di procedere a tali controlli, informa che le modalità di effettuazione degli stessi sono ispirate al principio della "gradualità" così come di seguito più precisamente specificato.

Modalità di effettuazione dei controlli

I controlli consentono al Titolare di intervenire con verifiche qualora si riscontrino anomalie d'area o di unità, senza arrivare al dettaglio del soggetto singolo, almeno in una prima fase.

Secondo il principio della gradualità:

- I controlli saranno effettuati inizialmente solo su dati aggregati riferiti all'intera struttura ovvero a singole aree lavorative, aventi caratteristiche tali da precludere l'immediata identificazione dell'utente.

- Nel caso in cui si dovessero riscontrare violazioni del presente disciplinare interno, indizi di commissione di gravi abusi o illeciti o attività contrarie ai doveri di fedeltà e diligenza, verrà diffuso un avviso generalizzato, o circoscritto all'area o struttura lavorativa interessata, relativo all'uso anomalo degli strumenti informatici, con conseguente invito ad attenersi scrupolosamente alle istruzioni ivi impartite.

- In caso siano rilevate ulteriori violazioni, si potrà procedere con verifiche più specifiche e puntuali, anche su base individuale.

I controlli non autorizzati

In ogni caso il Titolare non può in alcun caso utilizzare sistemi da cui derivino forme di controllo a distanza dell'attività lavorativa che permettano di ricostruire l'attività del lavoratore.

Per tali s'intendono, a titolo meramente esemplificativo e non esaustivo:

- la lettura e la registrazione sistematica dei messaggi di posta elettronica, al di là di quanto necessario per fornire e gestire il servizio di posta elettronica stesso;

- la riproduzione e la memorizzazione sistematica delle pagine internet visualizzate da ciascun Utente, dei contenuti ivi presenti e del tempo di permanenza sulle stesse;

- la lettura e la registrazione dei caratteri inseriti dal lavoratore tramite tastiera o dispositivi analoghi;

- l'analisi occulta di computer portatili affidati in uso.

18. SANZIONI

L'eventuale violazione di quanto previsto dal presente Regolamento – rilevante anche ai sensi degli art. 2104 e 2105 c.c. - potrà comportare l'applicazione di sanzioni disciplinari in base a quanto previsto dall'art. 7 dello Statuto dei Lavoratori.

Il Titolare avrà cura di informare senza ritardo (e senza necessità di preventive contestazioni e/o addebiti formali) le autorità competenti, nel caso venga commesso un reato, o la cui commissione sia ritenuta probabile o solo sospettata, tramite l'utilizzo illecito o non conforme dei beni e degli strumenti informatici.

Si precisa, infine, che in caso di violazione accertata da parte degli utenti delle regole e degli obblighi esposti in questo disciplinare, il Titolare si riserva la facoltà di sospendere, bloccare o limitare gli accessi di un account,

FILCA CISL
00184 Roma
Via del Viminale, 43
Tel.: +39 06 4870634

Fax: +39 06 4818884
+39 06 4870647
federazione.filca@cisl.it
www.filca.cisl.it

quando appare ragionevolmente necessario per proteggere l'integrità, la sicurezza e/o la funzionalità dei propri beni e strumenti informatici.

19. COMUNICAZIONI

Il presente Regolamento viene reso disponibile agli utenti al momento dell'assegnazione di un account, è pubblicato sulla bacheca interna del Titolare ed è comunque disponibile sulla Intranet.

Le autorizzazioni e/o concessioni richieste dal presente regolamento ovvero poste nella facoltà degli utenti potranno essere comunicate al Titolare e/o al Responsabile per mezzo di qualsiasi strumento che ne garantisca la tracciabilità (es.: e-mail).

20. APPROVAZIONE DEL REGOLAMENTO

Il presente Regolamento è stato approvato dal Comitato Esecutivo della Filca-Cisl Nazionale in data 2 dicembre 2020.