REGOLAMENTO CONSORTILE:

ART. 4 STATUTO LAVORATORI

ED UTILIZZO DI

STRUMENTI INFORMATICI

INDICE

1. Premessa

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete internet dai personal computer, espone Co.va.r 14 e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto di autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'ente stessa.

Premesso, quindi, che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, Co.va.r 14 ha adottato il seguente Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Detto Regolamento sarà oggetto di successive revisioni ed estensioni ad altre tematiche relative alla privacy ed alla sicurezza dei dati, che sono attualmente oggetto di specifico esame.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite in sede di lettera di designazione a persona autorizzata al trattamento dei dati personali.

Considerato inoltre che Co.va.r 14, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha da tempo deciso di mettere a disposizione dei propri collaboratori che ne necessitassero per il tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti (computer portatili, telefonici cellulari, palmari, ecc.) sono state inserite nel Regolamento alcune clausole relative alle modalità ed ai doveri che ciascun collaboratore deve osservare nell'utilizzo di tale strumentazione.

2. ENTRATA IN VIGORE DEL REGOLAMENTO E PUBBLICITÀ

Il nuovo Regolamento è in vigore dal 20 aprile 2018.

Copia del Regolamento, oltre ad essere affisso nella bacheca consortile, verrà inviato a ciascun dipendente sulla mail consortile.

3. OBIETTIVI

Il presente Regolamento ha l'obiettivo di:

- definire i criteri per l'assegnazione a personale dipendente e non, di risorse ICT ad uso individuale e i relativi flussi autorizzativi;
- disciplinare le modalità di corretto utilizzo e conservazione delle risorse ICT sopra indicate;

- definire le modalità per la conservazione e l'utilizzo dei dati relativi all'uso delle risorse e servizi informatici consortili;
- stabilire ruoli e responsabilità dei soggetti coinvolti.

4. AMBITO DI APPLICAZIONE

Il presente Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e di livello, nonché a tutti i collaboratori dell'ente a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratori a progetto, in stage, ecc.).

5. RIFERIMENTI A LEGGI E REGOLAMENTI

- D.Lgs 196/03;
- Deliberazione 1° marzo 2007, n. 13- Lavoro: le linee guida del Garante per la posta elettronica e Internet" (Gazzetta Ufficiale n. 58 del 10 marzo 2007) e s.m.i.;
- Regolamento Europeo 2016/679;
- Raccomandazione 5/15 del Comitato dei Ministri avente ad oggetto il trattamento dei dati personali in ambito occupazionale;
- Garante Privacy " Linee guida per posta elettronica e internet" del 01.03.2007;
- Direttiva n. 2/2009 del Dipartimento della Funzione Pubblica ad oggetto: " Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro"
- Parere del Garante dell'11 ottobre 2018, Reg dei provvedimenti n. 464 dell' 11/10/2018: "parere sullo schema di disegno di legge "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo".

6. DEFINIZIONI

Ai fini del presente Regolamento si intende per :

Utente	ogni dipendente e collaboratore (lavoratore somministrato, in stage, ecc.) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "persona autorizzata al trattamento ".
Mezzi di telecomunicazione	sistemi mobili con tecnologia che consentono lo svolgimento di funzioni di telefonia e/o trasmissione dati e/o funzioni video

Risorse ICT ad uso individuale (o risorse ICT)	le risorse e servizi informatici e i mezzi di telecomunicazione forniti dall'ente per uso individuale
Tablet	sistema mobile con tecnologia che garantisce la trasmissione dati e funzioni video
Risorse e servizi informatici	qualsiasi tipo di hardware, mezzi di comunicazione elettronica, rete di trasmissione dati, software, informazioni in formato elettronico e, in generale, applicativi
Fax	servizio telefonico consistente nella trasmissione (invio e ricezione) di immagini fisse (tipicamente copie di documenti).

7. ART. 4 STATUTO LAVORATORI

Premessa

Il Co.va.r 14:

- Ha il diritto/ dovere di precisare ai sensi dell'art 4 comma 2 dello statuto dei lavoratori gli strumenti che l'ente ritiene necessari per svolgere la prestazione lavorativa;
- ha il diritto/dovere di indicare in modo chiaro e dettagliato le indicazioni sul corretto utilizzo degli strumenti messi a disposizione e se, in quale misura e con quali modalità possano essere effettuati eventuali controlli;
- non effettua controlli a distanza dell'attività dei dipendenti, ai sensi art. 4 dello Statuto dei lavoratori (L. n. 300/1970), mediante sistemi hardware e software finalizzati, ad esempio:
    - alla lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
    - all'analisi occulta di computer portatili eventualmente affidati in uso;
- privilegia, rispetto alle misure repressive, quelle organizzative e tecnologiche volte a prevenire utilizzi impropri degli strumenti, minimizzando in ogni evenienza l'uso dei dati riferibili ai dipendenti e comunque nel rispetto dei principi di necessità, pertinenza e non eccedenza, tenendo conto altresì della disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali;

- si impegna a rispettare la protezione dei dati personali attraverso il pieno rispetto del Regolamento Europeo 2016/679 nonchè delle linee Guida del Garante Italiano e del Gruppo dei Garanti europei 29.

7.1 SUGLI STRUMENTI NECESSARI A RENDERE L'ATTIVITÀ LAVORATIVA EX ART 4 COMMA 2 STATUTO LAVORATORI

A seguito dell'entrata in vigore dell'art. 23, D. Lgs. 14 settembre 2015 n. 151, che ha modificato l'art. 4, L. 20 maggio 1970 n. 300, è stata riformata la disciplina relativa agli impianti audiovisivi e agli altri strumenti da cui derivi anche la possibilità di controllo a distanza dei lavoratori.

Ai sensi del comma 2 del novellato art. 4 gli strumenti utilizzati dai lavoratori, per rendere la prestazione lavorativa nonché quelli finalizzati ad attestare gli accessi e presenze, **dai quali può derivare anche la possibilità di un controllo a distanza** non richiedono, per la loro applicazione, la sussistenza di esigenze organizzative, produttive, di sicurezza o di tutela del patrimonio consortile e non necessitano del preventivo accordo sindacale né dell'autorizzazione degli Uffici ministeriali (DTL o MINISTERO).

Gli strumenti che Co.va.r 14 considera necessari a svolgere la prestazione lavorativa, sono:

a) Smartphone;
b) Il personal computer (fisso e/o portatile) con i relativi software operativi e/o applicazioni istallate;
c) La rete informatica consortile;
d) La posta elettronica consortile con dominio @covar14;
e) I dispositivi di archiviazione hardware (c.d."storage");
f) Le periferiche consortili annesse (stampanti, fax, masterizzatori, supporti, magnetici, schede di connessione W-LAN, UMTS, ecc.);
g) Gli apparati di comunicazione fissi (telefoni, ecc.);
h) Tablet.

L'utilizzo degli strumenti sopra indicati può comportare l'acquisizione, da parte dell'Ente, dei dati relativi alla quantità della prestazione lavorativa svolta, nonché alle modalità e procedure di esecuzione della stessa.

Tali strumenti di lavoro sono affidati esclusivamente per l'esercizio delle funzioni assegnate, pertanto, non debbono essere utilizzati per uso personale o comunque estraneo all'attività

consortile, né modificati, ferma restando la possibilità di esplicita e preventiva autorizzazione da parte dell'Amministrazione.

Per maggiori dettagli sulle modalità di utilizzo degli strumenti sopra elencati si vedano i paragrafi successivi.

8. MODALITA' OPERATIVE DEGLI STRUMENTI ELETTRONICI

8.1 SOGGETTI CHE POSSONO UTILIZZARE GLI STRUMENTI ELETTRONICI

L'utilizzo delle risorse informatiche in generale, della posta elettronica e di Internet in particolare, come già anticipato, sono accordati al dipendente, all'apprendista, al collaboratore, allo stagista. L'utilizzo delle risorse (sistemi hardware, programmi e applicazioni software, apparati di rete, risorse di stampa, telefoni fissi, cellulari e tablet) è concesso solo in quanto strumenti di esecuzione delle normali prestazioni di lavoro o strumenti atti all'apprendimento del lavoro.

A tal fine, il lavoratore deve sempre mantenere comportamenti improntati alla massima diligenza, ed evitare abusi dei servizi e/o utilizzi contrari alle norme di legge, dei regolamenti consortili e alle regole definite dal presente Regolamento.

Non devono essere in nessun caso modificate o aggirate le configurazioni per la sicurezza o per il funzionamento, predisposte dalle funzioni tecniche sui dispositivi.

L'accesso alle, e l'utilizzo delle, risorse ICT dovrà essere limitato allo stretto indispensabile e comunque senza pregiudicare l'attività lavorativa e/o l'esecuzione contrattuale.

Non è consentito visualizzare, utilizzare e/o salvare file come musica, fotografie, film, materiale offensivo, illecito, inappropriato o in ogni caso contrario alla morale su server, aree condivise, strumenti di collaborazione di programmi informatici o su risorse informatiche consortili.

Le persone autorizzate alla manutenzione dei sistemi informatici hanno l'obbligo di svolgere solo le operazioni strettamente necessarie per adempiere al loro incarico, con divieto di svolgere attività di controllo a distanza, anche di propria iniziativa.

8.2 RISERVATEZZA DELLE INFORMAZIONI

La responsabilità di proteggere il patrimonio informativo consortile in coerenza con le norme di legge in vigore e con le procedure consortili coinvolge tutto il personale relativamente alle attività di competenza.

Tutti i supporti (chiavi USB, CD/DVD, elaboratori, ecc.) in uso al personale devono essere richiesti al personale IT.

Non è ammesso l'utilizzo di supporti personali.

Le periferiche di massa contenenti informazioni riservate devono essere protette in modo adeguato, conservandole ad esempio, quando non utilizzate, in vani chiusi a chiave, preservando la sicurezza della chiave stessa. In assenza di specifiche autorizzazioni, non devono, inoltre, venire duplicate e consegnate a terzi.

Il patrimonio informativo consortile registrato su dischi, nastri, ecc. non deve essere rimosso dal suo normale ambiente di conservazione in assenza di specifiche autorizzazioni della competente unità della funzione ICT. Gli elaborati e i supporti magnetici utilizzati all'esterno degli ambienti di lavoro devono essere conservati sotto la responsabilità dell'interessato e comunque riportati in sede per la loro archiviazione o distruzione.

Il reimpiego dei supporti di memorizzazione (hard disk, ecc.) può avvenire a condizione che il contenuto precedente non sia recuperabile (ad esempio cancellato tramite ripetute formattazioni o con funzionalità di prodotti specifici). In caso contrario, il supporto di memorizzazione deve essere distrutto.

8.3 REGOLE DI UTILIZZO

Al fine di garantire la funzionalità, la sicurezza ed il corretto impiego degli strumenti elettronici ed, al contempo, al fine di assicurare la protezione dei dati personali dei dipendenti, prevenire possibili contenziosi nonché contemperare le esigenze di un corretto svolgimento dell' attività lavorativa con quelle di tutela della sfera personale dei dipendenti si ritengono necessari i seguenti accorgimenti su:

A) GESTIONE DELLA PASSWORD

1. PROCEDURE CORRETTE

- modificare al primo accesso la password così che da quel momento, sia conosciuta solo dall'utente stesso;

- mantenere la password segreta nei confronti di chiunque compresi i colleghi di lavoro;
- sostituire la password anche in caso di semplice sospetto circa la venuta meno della sua segretezza;
- comporre le password con almeno 8 caratteri di cui almeno 4 delle seguenti tipologie :
    a) un carattere maiuscolo (da A a Z)
    b) un carattere minuscolo (da a a z)
    c) una cifra numerica (da 0 a 9)
    d) un carattere non alfanumerico, come ad esempio: !,$,#.
- modificare la password ogni 90 giorni.

L'utilizzo combinato del nome utente e della password attribuisce in modo univoco al singolo dipendente la responsabilità delle operazioni compiute.

2 PROCEDURE VIETATE:

- utilizzare password già in uso precedentemente;
- inserire all'interno della password anche solo parzialmente il nome dell'utente;
- impiegare le password utilizzate in ambito lavorativo in altre attività o situazioni richiedenti l'utilizzo di una password;
- ogni condotta che possa comprometterne la segretezza.

8.4 UTILIZZO POSTAZIONI DI LAVORO

1 . PROCEDURE CORRETTE

- utilizzare gli Strumenti ICT per il perseguimento di fini strettamente connessi agli incarichi lavorativi, e comunque coerentemente al tipo di attività svolta ed in linea con le disposizioni normative vigenti.;
- spegnere l'elaboratore ed eventuali periferiche (stampanti, scanner …) prima di lasciare l'ufficio al termine dell'attività lavorativa e, in generale, rispettare le istruzioni impartite dai produttori.

- attivare manualmente, prima di assentarsi dal proprio posto di lavoro, il blocco del personal computer seguendo queste istruzioni: cliccare contemporaneamente i tasti CTRL-ALT-CANC (DEL per i portatili), quindi cliccare sul pulsante "blocca computer";
- far eseguire le operazioni di manutenzione/riparazione degli Strumenti ICT solo da parte del personale autorizzato dalla Direzione ICT;
- archiviare la documentazione di lavoro, se possibile, all'interno di cartelle di rete ad accesso controllato sottoposte a programma di backup;

2. PROCEDURE VIETATE

- accedere al sistema informatico e mantenersi all'interno di esso per motivi non lavorativi o non di servizio;
- usare le risorse o i servizi in violazione di normative comunitarie, leggi, regolamenti, provvedimenti, prescrizioni, o per commettere attività illecite o discriminanti;
- modificare le configurazioni impostate;
- installare ed utilizzare prodotti software che non siano stati autorizzati dalla Direzione;
- installare, utilizzare software che consentano l'intercettazione automatica del traffico o la violazione delle password;
- usare le risorse o i servizi per scopi commerciali, promozionali, pubblicitari, senza aver ottenuto l'autorizzazione dalla propria direzione consortile;
- utilizzare eccessivo spazio disco o assorbire capacità di banda nei sistemi di telecomunicazione, attraverso la generazione o l'invio di mail non strettamente correlate all'attività lavorativa, o in generale, attraverso il trasferimento di file o messaggi di dimensioni eccessive;
- inviare o depositare sui server o sul disco del proprio computer materiale di natura illegale o discriminante;
- mascherare la propria identità all'interno dei sistemi informatici;
- utilizzare le credenziali di autenticazione di altri utenti, per qualsivoglia ragione;
- tentare di violare password o altri sistemi di protezione o tentare di superare le restrizioni imposte dal sistema;

- riprodurre o distribuire materiale consortile senza autorizzazione;
- copiare o modificare files, redatti da altri utenti, senza autorizzazione;
- alterare i dati, tentare di introdurre o diffondere virus, trojan, backdoor, dataminer o altri codici malefici;
- interferire con il corretto funzionamento o danneggiare le attrezzature di rete;
- intercettare o alterare qualunque tipo di dato o di comunicazione digitale.
- navigare su siti non correlati con la prestazione lavorativa (white list);
- effettuare download di programmi e files estranei al lavoro, salvo espressa autorizzazione scritta della Direzione (file musicali, video, audio) ;
- partecipare a forum (es.: facebook, etc), accedere e utilizzare chat line, partecipare ad aste on-line non correlate con l'attività operativa (es.: e-bay) in assenza di espressa autorizzazione scritta della Direzione;
- scaricare, copiare, conservare, diffondere file a contenuto offensivo, discriminatorio, pedofilo, o di altro contenuto illecito penalmente o civilmente;
- accedere a siti di gioco, pornografici o con finalità ludiche;
- attivare strumenti di chat in videochiamata (es.: skype/msn messenger) in assenza di espressa autorizzazione scritta della Direzione.

In caso di cambiamenti di unità organizzative o, in ogni caso, di trasferimenti dei dipendenti, le eventuali risorse ICT ad essi precedentemente assegnate sono sottoposte nuovamente a processo autorizzativo.

8.5 UTILIZZO PC PORTATILI E DISPOSITIVI PORTATILI (SMARTPHONE, TABLET)

1. PROCEDURE CORRETTE

- conservare in un luogo sicuro a fine giornata lavorativa;
- in caso di viaggi in aereo il portatile deve essere sempre trasportato come bagaglio a mano;

- quando il portatile viene lasciato in albergo deve essere consegnato al deposito valori o, quantomeno, riposto in una valigia o in un armadio chiusi a chiave;
- avvertire tempestivamente, in caso di furto di un elaboratore portatile, l'Ufficio IT, che darà le opportune indicazioni;
- prestare particolare attenzione all'utilizzo di elaboratori portatili in luoghi pubblici, quali ad esempio locali, stazioni e mezzi di trasporto;
- verificare, in caso di prolungato distacco dalla rete consortile, la disponibilità di aggiornamenti per il software antivirus e antiransomware;
- segnalare immediatamente al reparto IT il malfunzionamento dei beni consortili;
- attivare manualmente, prima di assentarsi dal proprio posto di lavoro, l'utente è tenuto ad il blocco del personal computer seguendo queste istruzioni: cliccare contemporaneamente i tasti CTRL-ALT-CANC (DEL per i portatili), quindi cliccare sul pulsante "blocca computer"; per sbloccare il computer sarà necessario utilizzare la password dell'utente;
- inviare, ricevere, conservare SMS, whatsapp, MMS per fini personali e/O offensivi e/o discriminatori;
- utilizzare un "codice di blocco" per prevenire l'uso improprio dei telefoni cellulari consortili assegnati, con un PIN il più lungo possibile, in uso e l'accesso ai dati in esso contenuti;
- utilizzare gli apparati per scattare fotografie personali, registrare filmati, scaricare musica e giochi.

Co.va.r 14 procederà, ogni anno alla fine del mese di aprile, previa comunicazione ad hoc il 30 di marzo, ad ordinare la cancellazione dei dati personali conservati sui beni consortili, in uso ad ogni dipendente, che non siano stati precedentemente cancellati.

2.PROCEDURE VIETATE

- concedere il proprio elaboratore portatile, tablet, smartphone in uso a terzi
- configurare mail consortili su dispositivi personali

3. DISATTIVAZIONE O CESSAZIONE DEL RAPPORTO DI LAVORO

L'ente si riserva la facoltà di disabilitare l'utilizzo dei mezzi sopra elencati resi disponibili. Tali mezzi, infatti, sono strumenti consortili messi a disposizione del dipendente/collaboratore al fine di consentirgli lo svolgimento della propria mansione ma, come tutti gli strumenti di lavoro, essi rimangono nella completa e totale disponibilità dell'ente.

In caso di disattivazione o di cessazione del rapporto di lavoro gli strumenti vanno riconsegnati al Titolare del trattamento/Ufficio IT

Al momento della restituzione dei beni o entro 15 giorni dalla restituzione, l'ente invita l'interessato (ex dipendente) ad estrarre dai beni consortili ogni possibile dato personale. L'ente mediante un soggetto autorizzato, redige apposito verbale sull'attività realizzata. Il verbale va sottoscritto anche dall'ex dipendente.

Concluso il suddetto termine, tutti i beni contenuti in supporti consortili verranno considerati dati consortili.

***

In caso di cambiamenti di unità organizzative o, in ogni caso, di trasferimenti dei dipendenti, le eventuali risorse ICT ad essi precedentemente assegnate sono sottoposte nuovamente a processo autorizzativo

8.6 PERIFERICHE DI MASSA (USB PEN-DRIVE)

1. PROCEDURE CORRETTE

- utilizzare solo periferiche di archiviazione di massa richieste al reparto IT;
- proteggere le periferiche tramite PIN minimo di 8 caratteri;
- non comunicare il PIN a terzi;
- formattare la periferica prima di riconsegnarla
- riconsegnare la/le periferiche all'IT al termine del loro utilizzo.

2. PROCEDURE VIETATE

- utilizzare periferiche di archiviazione di massa private e non richieste all'IT;
- comunicare il PIN a terzi;

Tutte le periferiche di archiviazione di massa dovranno essere censite ed i relativi PIN, o chiavi di ripristino, saranno custoditi all'interno di un file/directory protetto/a da password conservato dal responsabile IT, in modo tale da risalire al soggetto affidatario della periferica di massa.

Ad ogni cambio utente dovrà essere cambiato il PIN, o chiave di ripristino o password, con conseguente formattazione della periferica stessa.

9 PROTEZIONE FIREWALL, ANTIVIRUS, ANTIMALWARE, ANTIRANSOMWARE

1. PROCEDURE CORRETTE

- tenere sempre attivati ed aggiornati i software firewall, antivirus, antimalware, antiransomware installati sul pc ;
- avvisare immediatamente l'Ufficio IT in ogni caso di anomalia;
- segnalare all'Ufficio IT il distacco dalla rete consortile del portatile per un periodo superiore a 15 giorni;
- seguire le istruzioni specificatamente indicate in caso di avviso da parte del software antimalware, in particolare, in caso di minaccia rilevata come non risolvibile procedere a:
    - disconnettere il cavo di rete e di alimentazione e nel caso di PC portatile o palmare spegnerlo;
    - contattare Direzione IT.

***

In ogni caso è responsabilità della Direzione IT mantenere aggiornato il software antimalware, generalmente attraverso un processo automatizzato mentre l'utente è connesso alle risorse di rete.

2. PROCEDURE VIETATE

- Disabilitare o eludere il software antimalware antivirus sulla propria postazione.

10 INTERNET

1. PROCEDURE CORRETTE

- utilizzare la rete internet dalle 13.00 alle 14.00;

2. PROCEDURE VIETATE

- navigare su siti illeciti, contrari alla morale e/o discriminatori per sesso e razza.
- utilizzare social network, webchat salvo specifica autorizzazione della Direzione

11 POSTA ELETTRONICA

1. PROCEDURE CORRETTE

- utilizzare la mail per fini personali durante la pausa pranzo dalle ore 13.00 alle ore 14.00;
- modificare la password almeno ogni 90 giorni ed immediatamente qualora si sospetti che essa sia venuta a conoscenza di terzi;
- gestire la casella di posta elettronica, la cui dimensione è stabilita in funzione delle necessità operative, in modo opportuno, eliminando i messaggi personali non necessari all'attività lavorativa, contenendo la dimensione degli stessi e dei relativi allegati. Ciò al fine di conseguire un più efficace impiego del servizio di posta elettronica, e nel contempo non sovraccaricare i relativi sistemi di sicurezza;
- cancellare immediatamente la mail in caso di messaggi sconosciuti o insoliti;
- memorizzare solo le email necessarie alla propria attività;
- utilizzare sempre i formati compressi (zip, rar etc) per inviare allegati pesanti

***

Co.va.r 14 procederà, ogni anno nel mese di aprile, previa comunicazione ad hoc il 30 di marzo, ad ordinare la cancellazione delle mail personali conservate sull'indirizzo di posta elettronica consortile, in uso ad ogni dipendente, che non siano state precedentemente cancellate.

Al termine di tale periodo le suddette mail verranno, in ogni caso, considerate mail consortili.

Le mail consortili verranno conservate 10 anni per finalità amministrative, contabili e gestionali.

2 PROCEDURE VIETATE

- utilizzare la posta elettronica per inviare a terzi documenti di lavoro o file strettamente riservati;
- partecipare o continuare catene telematiche (es Catene di sant'antonio)
- inviare o memorizzare messaggi il cui contenuto sia illegale, oltraggioso o osceno ovvero possa costituire o incitare alla discriminazione per ragioni di sesso, razza, lingua, religione, origine etnica, opinioni ed appartenenza sindacale e/o politica;
- inviare documenti consortili se non nei limiti delle proprie mansioni, responsabilità ed esigenze di progetto;
- aprire messaggi di posta elettronica o allegati di tipo "eseguibile" (formato " . exe") salvo in caso di certezza assoluta del mittente;
- partecipare, salvo autorizzazione del proprio responsabile, a dibattiti, forum, mailing-list, ecc., attivate esternamente all'ente;
- usare false identità durante lo scambio di messaggi;
- rispondere o aprire link contenuti in messaggi di posta che:
    - contengono un messaggio generico di richiesta di informazioni personali per motivi non ben specificati (ad es. scadenza, smarrimento, problemi tecnici);
    - fanno uso di toni intimidatori‖, quali ad esempio la minaccia del blocco della carta di credito o del conto corrente in caso di mancata risposta dell'utente. Le banche e gli istituti di credito, infatti, non richiedono mai per posta elettronica informazioni attinenti il conto personale o depositi. Le suddette precauzioni hanno lo scopo di evitare che sia rubata l'identità e che siano eseguite operazioni ad insaputa dell'utente vittima.

3.PROCEDURE IN CASO DI ASSENZA

In caso di assenza programmata (ad esempio per ferie o attività di lavoro fuori sede che pregiudichino la visibilità della posta elettronica) è opportuno impostare all'interno di client di posta elettronica o facendo richiesta all'IT messaggi di risposta automatici per permettere ai mittenti delle mail di essere consapevoli dell'assenza dall'ente nonché di ricevere indicazioni in merito a possibili referenti alternativi.

In ogni caso qualora l'ente al fine di perseguire finalità strettamente consortili dovesse avere necessità di accedere alla posta consortile del soggetto assente si segue la procedura per le assenze improvvise.

Qualora, in caso di assenza improvvisa e/o prolungata, ricorrano improrogabili necessità legate all'attività lavorativa per cui si debba conoscere il contenuto dei messaggi di posta elettronica, il Responsabile di Funzione/Direzione di appartenenza dell'utente può richiedere all'Amministratore di sistema che venga effettuato il reset della password dell'utente stesso. Di tale attività deve essere redatto, a cura del suddetto Responsabile, apposito verbale e deve essere informato l'utente interessato, preventivamente o, ove ciò non sia possibile, alla prima occasione utile.

In ogni caso, l'ente al fine di perseguire le finalità strettamente consortili ha previsto un sistema di delega.

In particolare ciascun dipendente può nominare un fiduciario anche tramite la funzionalità della casella di posta " accesso e delega", in caso di attivazione.

12 CESSAZIONE DEL RAPPORTO DI LAVORO

In caso di licenziamento o dimissioni del dipendente l'ente provvede alla disattivazione (chiusura) dell'account consortile riferita all'ex dipendente entro 15 giorni dalla data del licenziamento o delle dimissioni.

Contestualmente l'amministratore di sistema attiva un risponditore automatico volto a comunicare la chiusura dell'account dell'ex dipendente durante 15 giorni e ad invitare il mittente a ri-inviare la mail ad altro soggetto specificatamente individuato.

Durante il suddetto periodo temporale, ossia 15 giorni, l'ente in contraddittorio con altro soggetto dell'ufficio di appartenenza dell'ex dipendente, potrà verificare nella mail consortile dell'ex dipendente l'eventuale presenza di email ed, in tal caso, potrà constatare il solo nominativo del mittente, senza aprire alcuna mail, al fine di poterlo contattare in per finalità consortili.

Nell'arco dei 15 giorni l'ente invita l'interessato (ex dipendente) ad estrarre dalla posta elettronica ogni possibile dato personale. L'ente mediante un soggetto autorizzato, redige apposito verbale sull'attività realizzata. Il verbale va sottoscritto anche dall'ex dipendente.

Al termine dei 15 giorni la mail dell'ex dipendente va completamente disattivata ossia chiusa.

13 TELEFONI FISSI, FAX, STAMPANTI E FOTOCOPIATRICI

1. PROCEDURE CONSENTITE

- l'uso privato, purché occasionale, non prolungato e limitato alle situazioni di effettiva necessità, degli apparati di telefonia fissa e cellulare assegnati in uso;
- cancellare, nel caso in cui gli apparati debbano essere restituiti o inviati in manutenzione, dalle memorie degli apparati stessi qualsiasi dato personale proprio o di soggetti terzi.
- ritirare prontamente la stampa dai vassoi delle stampanti / fotocopiatori comuni.
- archiviare in apposita cartella il documento precedentemente scansionato e procedere a cancellare la mail

2. PROCEDURE VIETATE

- effettuare o ricevere telefonate personali e comunque non attinenti ai compiti affidati;
- comunicare i numeri telefonici a call center, società di servizi di informazione o di intrattenimento in abbonamento via SMS, comunità virtuali, ecc;
- l'uso di fax, stampanti e fotocopiatori per fini personali;
- utilizzare, in ogni caso, gli apparati per attività non pertinenti con lo svolgimento delle mansioni affidate.

14 ACCESSO AI DATI TRATTATI – AMMINISTATORE DI SISTEMA O SUO DELEGATO

Il personale incaricato alla gestione tecnica degli strumenti informatici può:

a) accedere ai dati trattati dall'utente tramite posta elettronica, navigazione in rete per motivi di sicurezza, protezione del sistema informatico e del patrimonio consortile (ad es.,

contrasto virus, malware, intrusioni telematiche, fenomeni quali spamming, phishing, spyware, ecc.), ovvero per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa e/o su segnalazione di presunti comportamenti illeciti. Fatta eccezione per gli interventi urgenti che si rendano necessari per affrontare situazioni di emergenza e sicurezza, il personale incaricato accederà ai dati su richiesta dell'utente e/o previo avviso al medesimo. Ove sia necessario per garantire la sicurezza, l'assistenza tecnica e la continuità della normale attività operativa, il personale incaricato avrà anche la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni;

b) nei casi indicati alla lett. a) che precede, effettuare tutte le operazioni di configurazione e gestione necessarie a garantire la corretta funzionalità del sistema informatico consortile (ad es. rimozione di file o applicazioni pericolose);

c) procedere a controlli finalizzati a garantire l'operatività e la sicurezza del sistema, nonché il necessario svolgimento delle attività lavorative, es. mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. L'eventuale controllo sui file di log da parte del personale incaricato alla gestione tecnica degli strumenti informatici non è comunque continuativo ed è limitato:
   - per la posta elettronica all'indirizzo del mittente e del destinatario, alla data e all'ora dell'invio e della ricezione e all'oggetto;
   - per la navigazione in internet al nome dell'utente, all'identificativo della postazione di lavoro (indirizzo IP), alla data e ora di navigazione, al sito visitato e al totale degli accessi effettuati;

d) può accedere ai dati contenuti negli strumenti informatici restituiti dall'utente all'ente per cessazione del rapporto, sostituzione delle apparecchiature, ecc. Sarà cura dell'utente la cancellazione preventiva di tutti i dati personali eventualmente ivi contenuti.

In ogni caso, l'ente effettua trattamenti tecnicamente finalizzati a consentire il regolare e corretto svolgimento dei servizi e-mail e internet anche ai fini connessi al rapporto di lavoro.

15 POSSIBILITA' DI CONTROLLI E LORO GRADUALITA'

Al fine di prevenire le succitate criticità e rischi, l'ente si riserva la facoltà di effettuare rilevazioni, in forma aggregata e anonima, in merito alla corretta applicazione dei principi e delle regole consortili.

Le modalità di svolgimento delle sopraindicate rilevazioni garantiranno il rispetto dei principi di pertinenza e non eccedenza, evitando qualunque immotivato accesso a dati personali contenuti nelle risorse informatiche consortili.

In caso di anomalie riscontrate nell'utilizzo delle risorse informatiche, la competente unità della funzione ICT effettua le operazioni necessarie ad identificare la causa del problema in esame.

In ogni caso saranno effettuati controlli graduali: in via preliminare, sempre in forma aggregata e anonima, sui dati relativi all'utilizzo delle risorse informatiche consortili riferiti a gruppi di lavoro.

Le rilevazioni verranno effettuate in maniera tale da salvaguardare l'anonimato, saranno oggetto di un reporting ai Privacy Officer circa le anomalie rilevate relativamente al corretto utilizzo delle risorse informatiche consortili.

Qualora le predette rilevazioni mostrino anomalie nell'utilizzo delle risorse informatiche, il Privacy Officer di riferimento invia a tutti i propri collaboratori un avviso che inviti loro ad attenersi alle regole di comportamento per l'utilizzo delle risorse informatiche consortili, fermo restando l'eventuale successivo approfondimento delle verifiche e, ove necessario, l'accertamento di **responsabilità individuali.**

In ogni caso, non saranno effettuati controlli prolungati, costanti od indiscriminati.

I dati sull'utilizzo di internet e della posta elettronica consortile sono registrati e archiviati in banche dati informatiche a cura della competente unità della funzione ICT. La gestione e la sicurezza delle banche dati è realizzata in conformità alle disposizioni vigenti in materia di tutela dei dati personali. I relativi trattamenti, sono eseguiti da personale incaricato. Il Titolare del trattamento è Co.va.r 14.

I dati registrati sono conservati per il tempo strettamente necessario al perseguimento delle finalità per le quali sono stati registrati e comunque per un periodo non superiore a 12 mesi, trascorsi i quali si procede alla relativa cancellazione, fatti salvi in ogni caso specifici obblighi di legge (ad es. Richiesta dell'Autorità Giudiziaria) o specifiche necessità di tutela e difesa degli interessi consortili.

I dati personali di un singolo dipendente, eventualmente anche sensibili, ricavabili dai dati registrati sono trattati, nei limiti in cui ciò sia indispensabile, per un periodo di tempo anche superiore, comunque non eccedente alle finalità, in caso di:

- richiesta scritta, ordinanza, decreto o altro provvedimento da parte della magistratura, del Garante per la Protezione dei Dati Personali o delle Forze dell'Ordine o altra Authority, nell'ambito dell'esercizio delle loro funzioni istituzionali;

- azioni legali avanzate nei confronti dell'ente da parte di terzi che ritenessero violati i propri diritti in materia di privacy;
- presunzione di comportamenti illeciti o rilevanti violazioni di Regolamenti consortili e/o obblighi.

In tali casi, in relazione alle specifiche casistiche di propria competenza, le competenti unità nell'ambito delle funzioni legale e risorse umane (rispettivamente per le tematiche di natura civile o penale e per le tematiche giuslavoristiche) nel valutare le azioni da intraprendere, individueranno anche gli eventuali dati da reperire:

- d'intesa con il Competente Privacy Officer;
- nel rispetto delle disposizioni di legge applicabili;
- tenendo in considerazione la complessità, onerosità e fattibilità tecnica delle attività da compiersi ai fini del loro reperimento in relazione anche alla natura e provenienza della richiesta.

La richiesta è quindi inoltrata alla competente unità della funzione ICT.

16 CASI DI INOTTEMPERANZA

Il rispetto delle prescrizioni contenute nella presente normativa costituisce parte essenziale delle obbligazioni contrattuali alle quali gli utenti devono attenersi secondo la diligenza richiesta nello svolgimento dell'attività lavorativa.

L'eventuale utilizzo improprio delle risorse informatiche consortili rappresenta violazione degli obblighi derivanti dal rapporto di lavoro e, conseguentemente, illecito disciplinare perseguibile secondo quanto previsto dal CCNL applicabile.

Per l'utilizzo dei dati tracciati con gli strumenti di cui al presente regolamento a tutti i fini connessi al rapporto di lavoro si rinvia altresì alla specifica informativa effettuata ai sensi dell'art. 4, comma 3, della legge n. 300 del 1970 che si considera parte integrante del presente Regolamento.

Data *Firma*

_____ _____