Allegato alla deliberazione del CdA n. 25 del 26/10/2017

REGOLAMENTO PER L'UTILIZZO DEI SISTEMI INFORMATICI E DI COMUNICAZIONE DI CR.FORMA – AZIENDA SPECIALE SERVIZI DI FORMAZIONE DELLA PROVINCIA DI CREMONA

ART. 1 – PRINCIPI GENERALI

La progressiva diffusione delle nuove tecnologie informatiche ed in particolare il libero accesso alla rete Internet tramite dispositivi elettronici (personal Computer, tablet, smartphone..) espone Cr.Forma ai rischi di un coinvolgimento sia patrimoniale che penale, creando problemi alla sicurezza e all'immagine dell'Ente stesso.
Premesso quindi che l'utilizzo delle risorse informatiche e telematiche del nostro Ente deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, Cr.Forma adotta il presente Regolamento finalizzato ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.
Tali prescrizioni si aggiungono ed integrano le specifiche istruzioni contenute nel Codice della privacy di Cr.Forma elaborato in attuazione del D. Lgs. n. 196 del 30 giugno 2003 in materia di protezione dei dati personali.

ART. 2 – UTILIZZO DEI TELEFONI FISSI

Ogni postazione di lavoro è dotata di un telefono fisso di ultima generazione attraverso il quale effettuare chiamate verso gli altri telefoni interni dell'ente. Gli apparecchi in dotazione ai dipendenti sono abilitati ad effettuare chiamate esterne locali, interurbane, nazionali e verso cellulari. Gli apparecchi possono essere abilitati ad effettuare chiamate internazionali previa autorizzazione del Direttore Generale. Al fine di controllare la spesa per la telefonia Cr.Forma adotta strumenti di monitoraggio dei costi che comunque garantiscono la privacy dell'utilizzatore.

L'utilizzo del cellulare personale è limitato ad un utilizzo funzionale all'espletamento dell'attività lavorativa. L'effettuazione o il ricevimento di telefonate personali deve essere limitato e non deve creare disservizi nell'espletamento della mansione lavorativa o danni all'immagine dell'Ente. Le stesse regole valgono con riferimento al ricevimento di telefonate personali sui telefoni fissi dell'Ente.

ART. 3 – UTILIZZO DEL PERSONAL COMPUTER E DELLE PERIFERICHE CONNESSE

Il Personal Computer affidato al dipendente / collaboratore è uno strumento di lavoro ed è di esclusiva proprietà dell'Ente, messo a disposizione al solo fine dello svolgimento delle proprie mansioni. Ogni utilizzo non attinente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
L'accesso al personal computer è protetto da una password personale che è assegnata/definita al fine di impedire una facile individuazione. Deve essere composta da almeno 8 caratteri, non deve coincidere con lo user-id e non deve coincidere con nome/cognome/data di nascita dell'utente o loro combinazioni.
Il dipendente/collaboratore, dopo l'assegnazione, è tenuto a modificare autonomamente al primo utilizzo la propria Password di accesso e a custodirla con la massima diligenza senza divulgarla a terzi. La password deve essere modificata ogni sei mesi. In caso di trattamento di dati sensibili la password deve essere modificata ogni tre mesi.
Su ciascun personal computer sono installati i software gestionali/programmi funzionali all'espletamento dell'attività lavorativa. Non è consentito installare o salvare autonomamente altri software/programmi e contenuti personali (Fotografie, File audio, File video ecc..) in quanto ciò può causare il grave pericolo di propagazione di virus informatici e l'alterazione della stabilità delle applicazioni del computer stesso. In caso di violazione della presente disposizione i software non autorizzati verranno automaticamente rimossi ed ogni violazione verrà segnalata alla Direzione Generale per i provvedimenti conseguenti. Il dipendente può richiedere l'installazione di un nuovo software attinente l'attività lavorativa rivolgendosi al Referente informatico incaricato presso ciascuna sede che provvederà all'installazione previo espletamento dell'iter autorizzatorio da parte del Direttore Generale.
Al personal computer possono essere collegati alcuni dispositivi esterni quali ad esempio memorie esterne, chiavette USB, lettori e/o masterizzatori, macchine fotografiche digitali, IPOD, lettori MP3, memory card ecc. ma solo se forniti dall'ente. E' consentito l'utilizzo di periferiche esterne personali ma è fatto divieto di installare software applicativi da chiavetta USB o da qualunque altro supporto esterno, inclusi applicativi via web anche se gratuiti.

Qualsiasi sospetto di presenza di virus informatici sul proprio personal computer deve essere immediatamente segnalato ai Referenti informatici di ciascuna sede.
I Personal Computer e i monitor, devono essere sempre spenti al termine dell'attività lavorativa prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. Ciò al fine non solo del risparmio energetico ma soprattutto al fine di evitare l'indebito utilizzo da parte di terzi ad un computer di fatto connesso al sistema e accessibile a chiunque. In tali frangenti ogni responsabilità sarà addebitata al dipendente/collaboratore titolare della password. Si ricorda che, onde evitare accessi indesiderati, è possibile bloccare la propria postazione prima di allontanarsi dalla stessa mediante i tasti "crtl" + "alt" + "canc" ed il successivo click su "blocca computer".
Gli aggiornamenti del sistema operativo sono necessari, oltre che essere un obbligo di legge, al fine di proteggere il PC e l'intera rete. Agli aggiornamenti provvede solo ed esclusivamente il referente informatico di ciascuna sede.

Non è consentito a nessuna postazione di lavoro, fissa o mobile che sia, disinstallare o disattivare sistemi di protezione (antivirus, personal firewall) o aggirare politiche di sicurezza definite da Cr.Forma a livello centralizzato.

Il dipendente/collaboratore ha il compito, inoltre, di assicurarsi, a fine turno o ogni qual volta si debba allontanare dall'Ufficio, di chiudere con le apposite chiavi date in dotazione gli archivi di cui fa uso per assicurare la riservatezza dei dati ivi contenuti e di non disattivare la disconnessione al pc che parte in automatico dopo pochi minuti dal termine dell'utilizzo dello strumento.

Art. 4 - SALVATAGGIO DEI DATI (Backup)

L'amministratore di sistema esegue giornalmente il salvataggio di alcuni dati contenuti in locale e dei dati contenuti su server e procede al salvataggio su supporti magnetici.
Tutto ciò che è presente sul desktop di ciascun PC non è sottoposto a back-up. Pertanto su ogni pc sono configurate determinate cartelle dove ogni utente è obbligato ad effettuare il salvataggio dei dati che vengono sottoposti a procedure di back-up.
E' vietato sottoporre a back-up cartelle con contenuti personali.

ART. 5 UTILIZZO DI ATTREZZATURE INFORMATICHE (PERSONAL COMPUTER PORTATILI, TABLET, VIDEOPROIETTORI, PENNE INTERATTIVE PER LIM)

La richiesta da parte del dipendente/collaboratore di attrezzature informatiche aziendali per lo svolgimento della propria mansione va formalizzata e annotata su apposito registro detenuto dal personale ausiliario che è il solo personale autorizzato al rilascio del materiale informatico. Ciò vale sia nel settore DDIF, sia nel settore degli autofinanziati, sia dell'apprendistato, sia del restauro.
L'utente è responsabile di tutte le attrezzature informatiche assegnategli che devono essere custodite con diligenza sia durante gli spostamenti sia durante l'utilizzo sul luogo di lavoro.

A tutti i dispositivi informatici comprese le LIM si applicano le medesime regole di utilizzo previste per i personal computer connessi in rete di cui all'art. 3 del presente Regolamento. Tutti gli eventuali file elaborati e salvati sui dispositivi verranno automaticamente rimossi allo spegnimento.
L'utilizzo di dispositivi personali per lo svolgimento della propria attività (tablet, PC..) è ammesso. Se su tali dispositivi sono caricati dati afferenti ad allievi e in caso di consultazione/utilizzo del registro elettronico devono essere applicate a cura dell'utilizzatore le misure minime di protezione dei dati (cambio password, antivirus…) e in caso di smarrimento o di sospetti un accesso improprio va fatta segnalazione a Cr.Forma.
Il collegamento alla rete di Cr.Forma dei dispositivi personali non di proprietà dell'Ente (ad esempio consulenti, tirocinanti, docenti ecc) deve essere motivato ed è possibile solo previa autorizzazione del referente informatico.

ART. 6 - SISTEMI DI PROTEZIONE ANTIVIRUS

Il sistema di protezione contro virus informatici è monitorato dal personale incaricato. L'aggiornamento dell'antivirus sui PC connessi in rete avviene in modo automatico.

Ogni utente deve tenere comportamenti atti a ridurre il rischio di attacco al sistema informatico di Cr.Forma mediante virus o mediante ogni altro software aggressivo.
Nel caso in cui sul proprio personal computer o portatile in uso compaia la segnalazione dell'antivirus della possibile presenza di un virus, il dipendente è tenuto a darne tempestiva comunicazione al referente informatico della propria sede e a sospendere immediatamente ogni elaborazione in corso senza spegnere il computer, al fine di permettere l'effettuazione delle operazioni di bonifica.

ART. 7 UTILIZZO DELLA POSTA ELETTRONICA DI CR.FORMA

La casella di posta elettronica viene assegnata dal Referente informatico all'utente ed è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
E' fatto divieto di utilizzare le caselle di posta elettronica **@crforma.it** per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list non attinenti alla propria attività lavorativa, salvo diversa ed esplicita autorizzazione.
In caso di ricezione di messaggi che potrebbero avere provenienza dubbia (es. mail spam) gli stessi non dovranno essere aperti ma immediatamente cancellati e della ricezione dovrà essere informato il referente informatico della sede di appartenenza.
La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti previa verifica della necessità di salvataggio.
Sono stati introdotti limiti alla dimensione di ciascuna casella postale superati i quali viene automaticamente bloccata dal sistema la casella di posta elettronica.
Si ricorda a tutti i dipendenti/collaboratori assegnatari di una casella di posta elettronica che gli allegati alle mail in ingresso ed in uscita non possono superare la dimensione massima di 5 MB.
Gli allegati ai messaggi di posta elettronica devono rispettare le seguenti caratteristiche:
a) non possono contenere di norma file Audio (Es. AIFF, MIDI, MPEG Sun/Next, WAW, CD, Ogg Vorbis Audio File, ASF, Windows Media File..)
b) non possono contenere di norma file Video (Es. AVI, DVM, MPEG, Quicktime, ShockWave File, Windows Media ASX File, ecc)
c) non possono assolutamente contenere file eseguibili e file con "codici sorgente".
Il sistema di posta elettronica di Cr.Forma è configurato su Outlook. E' vietato configurare sul personal computer assegnato in uso altri account di posta elettronica personali utilizzando Outlook.

E' opportuno apporre la propria firma in calce ad ogni e-mail secondo gli standard definiti dall'Ente in modo da essere sempre chiaramente identificabili ed agevolare le comunicazioni anche telefoniche.

Le singole password di accesso al sistema di posta elettronica di Cr.Forma sono definite ed attribuite inizialmente dall' Amministratore del Sistema. Il dipendente può inoltrare richiesta di modifica della password ai referenti informatici di ciascuna sede.
In caso di assenze prolungate dall'ufficio il personale è tenuto a richiedere al referente informatico della sede di appartenenza l'attivazione di un messaggio automatico che indichi il periodo di assenza e segnali eventualmente un altro destinatario al quale inviare i messaggi di lavoro urgenti. E' concesso al datore di lavoro, nel caso si rendesse necessario, utilizzare la casella di posta elettronica attribuita al lavoratore assente dando comunque comunicazione al mittente della assenza del lavoratore a cui è indirizzato il messaggio di posta elettronica.

ART. 8 UTILIZZO DELLA POSTA ELETTRONICA CERTIFICATA DI CR.FORMA

La Posta Elettronica Certificata (PEC) è un'estensione della posta elettronica tradizionale, la quale consente di avere un riscontro certo, con valenza legale, dell'avvenuta consegna del messaggio. Allo scopo Cr.Forma ha istituito una casella PEC (**crforma@pec.it**), conforme alla normativa vigente, per la ricezione e l'invio di messaggi e allegati che necessitino di riscontro di ricevuta.

Il Direttore Generale autorizza uno o più utilizzatori della PEC per i quali valgono le regole definite al precedente art. 7. L'utilizzatore dovrà custodire la password con diligenza e riservatezza.

ART. 9 NAVIGAZIONE SUL WEB

Per policy aziendale è vietato:

- la navigazione in Internet per scopi personali eccetto durante il periodo di pausa;
- la registrazione a siti per motivi diversi da quelli strettamente legati all'attività lavorativa stessa;
- la partecipazione a Forum non professionali, l'utilizzo di chat, di bacheche elettroniche e le registrazioni in guest book, anche utilizzando pseudonimi (o nicknames).
- la partecipazione a social-network di qualunque natura (facebook, myspace, instagram…) tranne quelli promossi e autorizzati dalla Direzione Generale.

E' consentita la consultazione della posta elettronica privata durante la pausa lavorativa.
La password di accesso al WI FI funzionale all'espletamento dell'attività lavorativa viene concessa solo per l'utilizzo di tablet o PC. Ulteriori accessi ai fini esclusivamente didattici o lavorativi devono essere autorizzati dal Direttore Generale.
Il datore di lavoro può effettuare controlli sull'utilizzo dei sistemi di navigazione, avvertendo in maniera anticipata il lavoratore, per questioni di sicurezza. Nell'atto della navigazione il dipendente potrebbe involontariamente scaricare virus che potrebbero danneggiare l'utilizzo della rete aziendale o compromettere la sicurezza delle informazioni memorizzate con sistemi informatici. In caso venissero riscontrate azioni illecite, il datore di lavoro si riserva di provvedere ad azioni disciplinari nei confronti del lavoratore a cui possono essere imputate(in maniera lampante) le predette azioni illecite in conformità alle procedure previste dal C.C.N.L. e lo statuto dei lavoratori.

Art. 10 – PROGRAMMI DI MESSAGGISTICA ISTANTANEA E SOCIAL NETWORKING

Tra gli strumenti messi a disposizione da Cr.Forma ai propri dipendenti e collaboratori vi sono strumenti di messaggistica istantanea quali Facebook e Skype che permettono lo scambio di comunicazioni e files in maniera immediata.

L'utilizzo di tali strumenti è disciplinato in maniera identica in tutto e per tutto all'utilizzo della posta elettronica.

E' fatto tassativo divieto associare un qualunque account del dominio @CRFORMA.IT a qualsiasi strumento di messaggistica istantanea e/o chat e/o social networking.

Pertanto la registrazione a tali servizi a carattere semi professionale, (su tali strumenti è possibile rimanere in contatto con tecnici specialisti di settore ma anche con amici e parenti) è consentita solo con l'utilizzo di un account personale non riconducibile in alcun modo a Cr.Forma e accettando le norme comportamentali previste per la posta elettronica, poichè, in qualità di pubblici dipendenti, si è tenuti a una condotta che non leda in alcun modo il buon nome e l'immagine propria, dei colleghi e dell'ente.

ART. 11 – UTILIZZO DELLE CARTELLE DI RETE

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Su queste unità sono svolte regolari attività di controllo, amministrazione e backup da parte del personale incaricato e di Lineacom.
E' fatto particolare divieto di salvare file (anche compressi) di formato:
- Multimediale (aif, asf, au, avi, mid, midi, miv, mov, mp2, mp3, mp4, mpe, mpeg, mpg, qt, rmi, snd, wav, wm, wma, wmv, mp3a, mp3b, ogg, 3gp)
- Eseguibili (exe, cmd, reg, vbs)
- Posta elettronica (pst, pab, eml, msg, idx, mbx, mmf, dbx)
- giochi, screen saver e comunque ogni file non attinenti all'attività lavorativa
- immagini in formato BMP (tali immagini devono essere convertite in formato JPG, JPEG al fine di occupare il minor spazio possibile).

Ad ogni utente è attribuita su File Server una cartella personale e una di gruppo a cui possono accedere gli utenti del medesimo settore e/o servizio per la condivisione dei file, laddove se ne ravvisi la necessità.

Per motivi di sicurezza è vietato condividere in altro modo cartelle fra utenti sul proprio PC, poiché possono costituire delle minacce ai dati custoditi, oltre a non ottemperare alle disposizioni di cui al D. Lgs. n. 196/2003.
L'Amministratore del Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza della rete dati sia sui PC degli incaricati sia sulle unità di rete.
Costituisce buona regola la periodica pulizia degli archivi personali su ogni personal computer (almeno ogni sei mesi), con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E', infatti, assolutamente da evitare un'archiviazione ridondante.
La lunghezza dei nomi dei file conservati sui server non deve superare i 25 caratteri.
E' sconsigliato, per motivi di performance e per evitare che temporanee interruzioni nel collegamento facciano perdere il lavoro, operare direttamente su Server. L'utente è invitato a lavorare sul disco fisso del proprio PC e a trasferire, se necessaria la condivisione, il proprio lavoro sul Server.

ART. 12 – REATI INFORMATICI E LORO PREVENZIONE

Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, posizioni filosofiche.
E' fatto divieto all'utente scaricare e/o installare software e programmi per l'attività professionale, così pure scaricare musica, film, filmati, materiale didattico e ogni altro file coperto da diritti d'autore.

L'uso dell'indirizzo di posta elettronica assegnato da Cr.Forma comporta l'utilizzo del nome dell'Azienda. Il materiale e i contenuti inviati sono diretta responsabilità dell'utente, che deve evitare che propri comportamenti in rete possano ledere l'immagine interna ed esterna dell'ente e/o dei colleghi, o ne possano comportare l'insorgere di qualsiasi tipo di responsabilità (civile/penale/amministrativa ecc).

E' tassativamente vietato l'utilizzo di un linguaggio non conforme alle comuni regole della buona educazione nelle comunicazioni via mail, siano esse interne o esterne. Sono vietati insulti, improperi, espressioni oscene, frasi a chiaro riferimento sessuale, anche nelle comunicazioni a carattere ufficiale, e qualunque altra espressione volta a ledere la dignità personale, il buon nome dei collaboratori interni ed esterni, dell'Ente e di qualunque altra persona fisica o giuridica con la quale si entri in contatto.

Altresì è fatto divieto, in quanto illecito penalmente perseguibile, di inviare mail con link a siti a carattere pedopornografico e di allegare file multimediali della stessa natura, e comunque qualunque contenuto violi norme civili, amministrative o penali di diritto nazionale, comunitario ed internazionale

È fatto divieto di utilizzare i sistemi di posta elettronica istituzionale per sollecitare o fare proseliti per finalità commerciali, di propaganda in favore di organizzazioni esterne, catene di lettere, ovvero per altre finalità estranee all'attività istituzionale.

È fatto divieto di utilizzare i sistemi di posta elettronica istituzionale per inviare o ricevere materiali protetti dal diritto d'autore, segreti commerciali, informazioni finanziarie proprietarie, o altro materiale appartenente ad organizzazioni diverse dall'ente, salvo che tali attività costituiscano parte integrante di doveri verso i cittadini. La mancata osservanza del diritto d'autore ovvero di accordi di licenza può condurre ad azioni disciplinari dell'organizzazione ovvero ad azioni legali dei legittimi titolari del diritto d'autore

L'accesso ai portali della Pubblica Amministrazione da parte del personale di Cr.Forma (portale Inps, Inail, Gefo, portale Istituto di credito..) è soggetto a specifica autorizzazione da parte del Direttore Generale. L'accesso ai singoli portali viene richiesto per iscritto al Custode della Password di ciascuna sede che trasmette la password di accesso previo espletamento dell'iter autorizzatorio con il Direttore Generale. E' fatto espresso divieto di trasmettere autonomamente a soggetti terzi le password di accesso ai software gestionali e ai portali che deve essere custodita con diligenza anche al fine della prevenzione di reati informatici.

Art. 13 - OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

E’ obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, così come altresì indicato nella lettera di incarico per il trattamento dei dati di cui al D. Lgs. n. 196 del 30 giugno 2003.
Il mancato rispetto o la violazione delle regole contenute nel D.Lgs. n. 196 del 30 giugno 2003 è perseguibile con le azioni civili e penali previste.
Il mancato rispetto delle norme contenute nel presente regolamento può comportare l’applicazione di sanzioni disciplinari, in ottemperanza alle disposizioni disciplinari di cui ai CCNL.