REGOLAMENTO DELL'AZIENDA PER L'UTILIZZO DEL SISTEMA INFORMATICO (RIF. REG. UE 2016/679)

APPROVATO IN DATA .....

Edizione	Revisione	Data	Descrizione	Firma il Titolare	Firma il DPO
01	00	.....	Prima emissione		

Documento di nr. 7 pagine compresa la presente, realizzato su format di

Unica soc. coop. Gruppo Kosmos
Viale Lionello Matteucci, 82
02100 RIETI
Cod.Fisc. e Partita IVA 01154910572
PEC unicamail@pec.it

Sommario

0. PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, Tablet, Smartphone, ecc. espone l'Ente ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e soprattutto all'immagine dell'Ente stesso. Premesso quindi che l'utilizzo delle risorse informatiche e telematiche del nostro Ente deve sempre ispirarsi a principi di trasparenza, liceità, diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito del rapporto di lavoro, l'Ente ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

1. UTILIZZO DEL PERSONAL COMPUTER, TABLET, SMARTPHONE

Il Personal Computer, il tablet, ovvero lo smartphone (di seguito elaboratore) di proprietà dell'Ente che viene affidato al dipendente, sia a titolo esclusivo che in modalità condivisa, è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa o attività ad essa afferenti è vietato, in quanto può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e mai divulgata. La stessa password deve essere attivata per l'accesso alla rete, per lo screen saver e per il collegamento a Internet. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del responsabile del trattamento dei dati incaricato del supporto alla rete informatica. Il dipendente è custode delle parole chiave riservate, per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati nella sua area riservata, ivi compresi gli archivi di posta elettronica interna ed esterna. responsabile del trattamento dei dati incaricato del supporto alla rete informatica, nella sua funzione di Administrator (Admin) della rete potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere al titolare del trattamento, di accedere ai dati trattati da ogni incaricato al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato. Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa, scritta ed esplicita autorizzazione in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore. Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal responsabile dei sistemi informatici. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D.Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore. Non è consentito all'utente modificare le caratteristiche impostate sull'elaboratore, salvo previa, scritta ed esplicita autorizzazione. L'elaboratore deve essere spento al termine del servizio (fatto salvo gli eventuali turni di reperibilità) o in caso di assenze prolungate dal lavoro (almeno 60 minuti consecutivi). In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso; per tale motivo deve essere attivato lo screen saver e la relativa password. Non è consentita l'installazione – anche temporanea – sull'elaboratore di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio USB, masterizzatori, modem, ...), se non con previa, scritta ed esplicita autorizzazione. Ogni lavoratore deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente Admin nel caso in cui vengano rilevati virus ovvero mail sospette.

2. UTILIZZO DELLA RETE INTRANET

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup. Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente. Admin può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete senza preventivamente informare il dipendente. Costituisce buona regola (con periodicità non superiore all'anno solare) la pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente vietata l'archiviazione ridondante; la duplicazione dei dati elettronici, se non prevista dalla procedura di disaster recovery, costituisce violazione della presente se non diversamente dimostrata dal lavoratore. È cura del lavoratore effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla senza indugio dai vassoi delle stampanti comuni. Le stampe di dati elettronici a supporto dell'attività svolta devono essere distrutte al termine dell'attività, senza deroga alcuna. È infatti assolutamente vietata la stampa dei dati dal formato elettronico a quello cartaceo se non espressamente prevista dall'attività svolta; la stampa cartacea dei dati elettronici, se non prevista dalla procedura di disaster recovery, costituisce violazione della presente se non diversamente dimostrata dal lavoratore. È regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. Per i motivi sopra indicati la stampa di dati elettronici è da considerarsi non necessaria e, quindi, vietata se non diversamente dimostrato dal lavoratore. In caso di necessità la stampa in corso può essere annullata.

3. GESTIONE DELLE PASSWORD

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite da Admin. È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni novanta giorni.(N.B.: in molti sistemi la comunicazione di variazione può essere "generata" dallo stesso sistema informatico all'atto della modifica; molti sistemi permettono di "temporizzare" la validità delle password e, quindi, di bloccare l'accesso al personale computer e/o al sistema, qualora non venga autonomamente variata dall'incaricato entro i termini massimi: in questi casi vanno adattate le istruzioni contenute nel presente regolamento) La eventuale deroga alla modifica della password deve essere autorizzata preventivamente e per iscritto. Le password possono essere formate da lettere (maiuscole o minuscole), caratteri speciali e numeri a seconda anche dell'impostazione del software, ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema. Le password non devono mai contenere riferimenti agevolmente riconducibili all'incaricato e sono classificate secondo tre livelli di sicurezza:

- ALTO: password composta da almeno otto caratteri contenendo almeno una lettera maiuscola, una minuscola, un numero e un carattere speciale;
- MEDIO: password composta da almeno sei caratteri contenendo, in alternativa, una lettera maiuscola, una minuscola, un numero e un carattere speciale;
- BASSO: password che non rientra nei casi precedenti.

A deroga, la password deve essere immediatamente sostituita in tutti quei casi dove l'utente anche solo sospetti che la stessa abbia perso la segretezza. Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia a Admin.

4. UTILIZZO DEI SUPPORTI MAGNETICI

Tutti i supporti magnetici riutilizzabili (USB, dischetti, cassette, cartucce) di proprietà dell'Ente che contengono dati personali c.d. "sensibili" devono essere trattati con particolare cautela (es. cifratura con chiave algoritmica, archiviazione in cassaforte, ecc.) onde evitare che il loro contenuto possa essere recuperato. I supporti magnetici contenenti dati personali c.d. "sensibili" sono dati in custodia al lavoratore che ne è personalmente responsabile in caso di danneggiamento, smarrimento o furto.

5. UTILIZZO DI PC PORTATILI

L'utente è personalmente responsabile del PC portatile assegnatogli e deve custodirlo con la diligenza del "buon padre di famiglia" sia durante gli spostamenti sia durante l'utilizzo. Ai PC portatili si applicano le stesse regole di utilizzo previste per gli altri elaboratori, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna. I PC portatili, in caso di allontanamento, devono essere custoditi in un luogo protetto.

6. USO DELLA POSTA ELETTRONICA

La casella di posta, assegnata dall'Ente all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. È fatto divieto di utilizzare le caselle di posta elettronica c.d. "aziendale" per l'invio di messaggi non afferenti all'attività lavorativa o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione. È d'obbligo evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. La documentazione elettronica che costituisce per l'Ente "know-how" tecnico o protetto (tutelato in base all'art. 6 bis del r.d. 29.6.1939 n.1127) e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio, non può essere comunicata all'esterno ovvero elaborata senza preventiva autorizzazione.

6.1 IDENTIFICAZIONE DELL'INDIRIZZO ESTERNO DI POSTA ELETTRONICA

Prima di rispondere ovvero scrivere un messaggio tramite posta elettronica l'utente deve sempre accertarsi di identificare ovvero riconoscere la persona o l'Ente efferente a quel indirizzo di posta elettronica esterno.
Si ritengono attendibili gli indirizzi di posta elettronica certificata se censiti:

- ✓ nell'Indice nazionale dei domicili digitali delle imprese e dei professionisti (www.inipec.gov.it - art. 6-bis Codice Amministrazione Digitale D.Lgs. 82/2005)
- ✓ nell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (www.indicepa.gov.it - art. 6-ter Codice Amministrazione Digitale - D.Lgs. 82/2005).

Altresì, si ritengono attendibili gli indirizzi di posta elettronica ordinaria:

- ✓ rilasciati da enti e/o organizzazioni riconosciute;
- ✓ inseriti in siti internet di provenienza certa;
- ✓ forniti direttamente dall'interessato tramite comunicazione scritta (es. biglietto da visita, comunicazione ufficiale, ecc.).

6.2 COMPOSIZIONE DEL MESSAGGIO

Nella composizione del messaggio è fatto d'obbligo seguire le seguenti indicazioni, ovvero dimostrare di aver adempiuto ai requisiti minimi di semplicità, trasparenza, leicità e di correttezza imposti da una comunicazione formale:

- I messaggi inviati, ivi comprese le risposte (anche quelle automatiche) devono sempre prevedere la c.d. "firma" con l'indicazione dell'Ente, dalla persona titolare della casella di posta e della sua funzione nell'Ente. Inoltre la "firma" deve riportare le indicazioni previste dal Reg. UE 2016/679 in materia di protezione dei dati personali.
- È fatto divieto l'invio di messaggi di posta elettronica con il campo "Oggetto" vuoto o con diciture non pertinenti al testo del messaggio.
- Il testo del messaggio deve essere scritto con linguaggio semplice, chiaro e conciso evitando abbreviazioni e/o tipizzazioni (esempio xè anziché perché).
- Nel testo del messaggio deve sempre essere indicato il motivo per il quale lo stesso viene scritto e il motivo per cui lo stesso viene inviato ad altri soggetti presenti nei campi "To" o "Cc" (fatta salvo gli indirizzi di posta ricompresi nel campo "Ccn" – in copia nascosta).
- Se si richiede risposta la stessa deve essere esplicitata indicando, se del caso, anche le motivazioni.
- Se la comunicazione fa riferimento a pratiche / istanze identificate (es. protocollo), l'identificazione pseudonimizzata deve essere riportata nell'oggetto ed eventualmente nel testo del messaggio.

- Eventuali allegati devono essere esplicitati nel testo del messaggio e devono avere la dimensione minima adatta all'utilizzo dell'allegato.
- Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'Ente deve essere visionata od autorizzata dal Responsabile afferente in ogni modo opportuno a far riferimento alle procedure in essere per la corrispondenza ordinaria.
- Utilizzare sempre l'opzione di ricevuta di ritorno, ovvero lettura, del messaggio.
- La posta elettronica è canale di comunicazione preferenziale anche per le comunicazioni interne, mentre per il passaggio di dati su file tra funzioni interne all'ente è altamente sconsigliabile in quanto prevede una duplicazione del dato.
- È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo e, in casi di dubbi, consultare Admin.
- Non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti.
- È vietato re-inoltrare messaggi di posta elettronica in modalità c.d. "catena di Sant'Antonio". Se si dovessero ricevere messaggi di tale tipo, si deve informare Admin senza indugio. Non si devono in alcun caso attivare gli allegati di tali messaggi.
- Stesse accortezze vanno seguite per i messaggi di Posta Elettronica Certificata (PEC).

7. USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

L'elaboratore abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa. È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato da Admin.

È fatto divieto assoluto di accedere a siti internet:

- ✓ a carattere social ovvero blog (es. Facebook, Linkedin, Twitter, ecc.);
- ✓ gestori di webmail non afferenti all'Ente;
- ✓ di vendita on-line;
- ✓ con contenuti a carattere razziale, omofobo, xenofobo o pornografico;
- ✓ con contenuti che possano essere previsti quale reato in sede penale.

È tassativamente vietata:

- ✓ l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati e con il rispetto delle normali procedure di acquisto;
- ✓ ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- ✓ la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

8. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

È obbligatorio attenersi alle disposizioni in materia di protezione dei dati personali e relative misure minime di sicurezza, come indicate nella valutazione preliminare d'impatto, nel codice di condotta e nel registro delle attività dell'Ente in revisione corrente ai sensi del Reg. UE 2016/679.

9. NON OSSERVANZA DEL PRESENTE REGOLAMENTO

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite in conformità al codice di condotta ed agli altri regolamenti applicabili.

10. VALIDITA', PUBBLICITA', AGGIORNAMENTO E REVISIONE DEL REGOLAMENTO

Tutti gli utenti possono proporre, quando ritenuto necessario ma con modalità non vincolante per l'Ente, integrazioni ovvero modifiche al presente Regolamento. Il presente Regolamento entra in vigore il giorno successivo alla sua validazione, ne viene data adeguata pubblicità a tutte le parti interessate ed è soggetto a verifica, ovvero revisione, con frequenza non superiore all'anno. Il presente Regolamento rimane in vigore fino a sua revisione ovvero comunicazione contraria.

Luogo e Data .....

Il Titolare del trattamento .....