



## Comune di Iglesias

Allegato E : Disciplina sulla sicurezza della rete e dei dati  
nel lavoro a distanza

Al Lavoratore

**OGGETTO: Disciplina sulla sicurezza della rete e dei dati comma 2 art. 63 CCNL 2019-2021**

Art. 1 – Ambito di applicazione.....	2
Art. 2 – Principi generali.....	2
Art. 3 Dotazioni informatiche ai dipendenti nell'ambito delle modalità di lavoro a distanza.....	3
Art. 4 Modalità di accesso ai servizi informatici dell'Amministrazione .....	3
Art. 5 Gestione delle password e degli account.....	3
Art. 6 Protezione antivirus e antimalware.....	4
Art. 7 Utilizzo delle periferiche e delle cartelle condivise .....	4
Art. 8 Dispositivi di archiviazione salvaguardia dei dati.....	4
Art. 9 Utilizzo di Internet .....	4
Art. 10 Gestione di posta elettronica .....	5
Art. 11 Controlli, responsabilità e sanzioni .....	5
Art. 12 aggiornamenti delle regole tecniche .....	5

**Art. 1 – Ambito di applicazione**

1. Il presente documento individua le specifiche tecniche minime di custodia e sicurezza dei dispositivi elettronici e dei software, nonché le regole necessarie a garantire la protezione dei dati e delle informazioni del Comune di \_\_\_\_\_. In particolare, disciplina le modalità di accesso ed utilizzo degli strumenti informatici, di internet, della posta elettronica, eventualmente messi a disposizione del Comune ai dipendenti nell'esercizio della loro prestazione lavorativa a distanza a cui sia stato concesso l'uso di risorse informatica di proprietà dell'amministrazione.

2. Gli strumenti informatici sono costituiti dall'insieme delle risorse informatiche dell'Amministrazione, ovvero dalle risorse infrastrutturali e del patrimonio informativo digitale (dati).

3. Le risorse infrastrutturali sono costituite dalle componenti hardware e software.

4. Il patrimonio informativo è l'insieme delle banche dati in formato digitale ed in generale di tutti i documenti prodotti tramite l'utilizzo delle risorse infrastrutturali.

5. Le prescrizioni del presente documento si applicano ai dipendenti dell'amministrazione coinvolti nell'esercizio delle proprie prestazioni lavorative in modalità agile.

**Art. 2 – Principi generali**

1. L'amministrazione promuove l'utilizzo degli strumenti informatici, di internet, della posta elettronica e della firma digitale quali mezzi utili a perseguire con efficacia ed efficienza le proprie finalità istituzionali, e specificatamente l'obiettivo di introduzione del "lavoro a Distanza", quale modalità flessibile di esecuzione del

rapporto di lavoro subordinato finalizzata ad incrementare la produttività e agevolare la conciliazione dei tempi di vita e di lavoro in accordo con le linee guida e i principi delineati dalla normativa vigente.

2. L'amministrazione promuove ogni opportuna misura organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati di proprietà dell'amministrazione anche nell'ambito dello svolgimento dell'attività di lavoro a distanza.

3. Ogni dipendente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche con particolare riferimento ai servizi, ai programmi cui ha accesso e ai dati trattati a fini istituzionali. È altresì responsabile del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione della normativa per la tutela dei dati personali. Sono vietati comportamenti che possono creare un danno, anche di immagine, all'amministrazione.

4. Ogni dipendente coinvolto nell'esercizio della propria prestazione di lavoro in modalità a distanza, indipendentemente dalla posizione che ricopre all'interno della macrostruttura organizzativa dell'amministrazione è vincolato ad applicare le norme descritte nel presente documento.

5. Gli strumenti informatici messi a disposizione del lavoratore a distanza (ad es. computer portatile, accessori, software, etc.) di proprietà dell'amministrazione e i servizi informatici e telematici, devono essere custoditi ed utilizzati in modo appropriato e diligente ed è responsabile della propria postazione di lavoro. A tal fine l'amministrazione attraverso l'ufficio competente in materia di sistemi informativi supporta i lavoratori a distanza.

### **Art. 3 Dotazioni informatiche ai dipendenti nell'ambito delle modalità di lavoro a distanza**

1. Al dipendente in modalità di lavoro a distanza è resa disponibile una postazione di lavoro virtuale.

2. Al dipendente in modalità di lavoro a distanza sono attribuite le credenziali di autenticazione per l'accesso ai servizi informatici dell'amministrazione. Di regola le credenziali in questione sono quelle già possedute dal dipendente per ragioni d'ufficio.

### **Art. 4 Modalità di accesso ai servizi informatici dell'Amministrazione**

1. Il dipendente che effettua la propria prestazione lavorativa in modalità di lavoro a distanza accede ai servizi informatici resi disponibili dall'amministrazione.

2. Per l'utilizzo dei servizi di cui al comma 1, il dipendente accede mediante VPN SSL e un sistema di autenticazione, eventualmente a doppio fattore.

3. Il dipendente che effettua la propria prestazione lavorativa in modalità di lavoro a distanza dispone dei servizi applicativi utili allo svolgimento dell'attività lavorativa in coerenza con l'accordo individuale di lavoro stipulato con l'amministrazione.

4. La postazione di lavoro virtuale di cui al comma 3 è utilizzata anche durante l'espletamento dell'attività lavorativa presso l'ordinaria sede di servizio.

### **Art. 5 Gestione delle password e degli account**

1. Le credenziali per l'accesso alle postazioni di lavoro oppure ai servizi informatici sono costituite da un codice identificativo personale (username o user id) e da una parola chiave (password) ed in alcuni casi da un codice PIN.

2. La password e/o il PIN di qualunque strumento/servizio deve essere strettamente personale, segreta. Ogni dipendente è responsabile civilmente e penalmente della custodia e della segretezza delle proprie credenziali (D.lgs. 196/2003 e s.m.i.), le quali sono incedibili.

3. È consentito l'accesso alla postazione di lavoro o ad un servizio informatico esclusivamente utilizzando le proprie credenziali di autenticazione.

4. È compito dell'ufficio personale comunicare all'ufficio competente in materia di sistemi informativi, eventuali variazioni del personale in lavoro a distanza al fine di aggiornare, creare, modificare e cancellare gli account, nonché eventuali autorizzazioni sui sistemi.

#### **Art. 6 Protezione antivirus e antimalware**

1. Ogni dipendente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico dell'amministrazione mediante virus, malware o mediante ogni altro software aggressivo, quali l'apertura di messaggi di posta elettronica e dei relativo allegati di provenienza sospetta o non conosciuta e affidabile.
2. Ad ogni dipendente si raccomanda di verificare la presenza e il regolare funzionamento del software antivirus e antimalware installato sul proprio computer.

#### **Art. 7 Utilizzo delle periferiche e delle cartelle condivise**

1. Per periferica condivisa si intende stampante, scanner, o qualsiasi altro dispositivo elettronico che può essere utilizzato in contemporanea da più uffici. Per cartella condivisa (o area di lavoro condivisa o condivisione) si intende uno spazio disco disponibile sui server centrali, per la memorizzazione di dati e programmi accessibili ad un gruppo di utenti preventivamente autorizzati, oppure anche ad un solo utente nel caso di utilizzo a scopo di backup.
2. I dipendenti autorizzati possono accedere ad una determinata area di lavoro condivisa nella quale si indica, il nome dell'area condivisa da creare/modificare e gli utenti interessati alla scrittura dei dati oppure alla sola lettura degli stessi.
3. Il dipendente è tenuto ad utilizzare le unità di rete per la condivisione di informazioni strettamente professionali; non può pertanto collocare, anche temporaneamente, in queste aree qualsiasi file che non sia attinente allo svolgimento dell'attività lavorativa. Il dipendente è tenuto, altresì, alla periodica revisione dei dati presenti in tutti gli spazi assegnati, con cancellazione dei files che non necessitano di archiviazione e che non siano più necessari ai fini procedurali. Particolare attenzione deve essere prestata alla duplicazione dei dati al fine di evitare, salvo casi eccezionali, un'archiviazione superflua.

#### **Art. 8 Dispositivi di archiviazione salvaguardia dei dati**

1. Ogni dipendente è responsabile della custodia dei dati di lavoro presenti sulla propria postazione di lavoro informatica. I dipendenti hanno cura di conservare copia della documentazione di lavoro nelle aree condivise predisposte con il supporto dell'ufficio dei sistemi informativi.

#### **Art. 9 Utilizzo di Internet**

1. Nell'ambito della propria infrastruttura informatica, l'amministrazione si riserva di applicare diversi profili di navigazione, a seconda dell'attività professionale svolta. Attraverso tale profilazione saranno consentite le attività di accesso navigazione registrazioni a siti web scaricamento ascolto e visione di file audio video in modo personalizzato e correlato con la propria attività lavorativa e comunque sempre in maniera dipendente dalle risorse di banda disponibili al momento nella rete.
2. Ogni variazione all'applicazione del profilo di navigazione standard deve essere formalizzata al responsabile dell'area, il quale motiva la richiesta indicando eventualmente se questa debba essere limitata nel tempo.
3. Sono applicate politiche per la sicurezza della rete di trasmissione dati attraverso sistemi di filtraggio dei contenuti e pagine web, i quali bloccano o quantomeno limitano la navigazione su categorie di siti ben specifiche che siano potenzialmente illegali secondo la normativa vigente o comunque ledenti la dignità umana. Non è consentito scambiare materiale protetto dalla normativa vigente in tema di tutela del diritto d'autore e utilizzare sistemi di scambio dati/informazioni con tecnologie *peer to peer* o sistemi di *anonymous proxy*.
4. La categorizzazione di cui al quarto comma, è effettuata anche con l'ausilio di strumenti automatici e pertanto può contenere errori o inesattezze e può essere integrata o corretta mediante segnalazione all'ufficio competente in materia di sistemi informativi.

5. I dati di navigazione dei dipendenti sono raccolti mediante *log* a norma di legge e possono essere utilizzati ma non diffusi dall'ufficio competente in materia di sistemi informativi per il monitoraggio delle funzionalità tecniche, per la risoluzione di problematiche, per scopo di sicurezza e per raccolta di dati statistici aggregati ed anonimi, aventi il fine di migliorare la qualità e la fruibilità delle informazioni e dei servizi informatici e telematici.

6. I log sono conservati 180 giorni per consentire la consultazione alle autorità competenti in caso di abusi e poi automaticamente cancellati. In ogni caso l'accesso a tali dati è consentito esclusivamente previa richiesta formale delle autorità competenti nei casi e con le procedure previste dalla legge vigente.

#### **Art. 10 Gestione di posta elettronica**

1. La casella di posta elettronica assegnate dall'amministrazione al lavoratore a distanza è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili corretto utile delle stesse.

2. In ogni caso non è consentito utilizzare tecniche di *mail spamming*, utilizzare il servizio di posta elettronica per inoltrare contenuti non attinenti alle materie di lavoro; trasmettere con dolo, virus, worms, trojan o altro codice maligno, finalizzati ad arrecare danni e malfunzionamenti ai sistemi informatici.

#### **Art. 11 Controlli, responsabilità e sanzioni**

1. L'amministrazione si riserva di effettuare verifiche sul corretto utilizzo della posta elettronica, di Internet, nel rispetto delle normative vigenti e del presente documento.

2. La violazione da parte dei dipendenti dei principi e delle norme contenute nel presente documento comporta l'applicazione delle sanzioni previste disposizioni contrattuali vigenti in materia previo espletamento del procedimento disciplinare.

#### **Art. 12 aggiornamenti delle regole tecniche**

1. Le disposizioni generali contenute nel presente documento possono essere soggette ad aggiornamenti, integrazioni e/o correzioni, in relazione all'evolversi della tecnologia all'entrata in vigore di sopravvenute posizioni di legge o all'evolversi delle esigenze dell'amministrazione.

Con la sottoscrizione del presente documento, il lavoratore attesta di aver preso conoscenza in modo puntuale del contenuto del medesimo

Data \_\_\_\_\_

**Firma del Datore di Lavoro**

\_\_\_\_\_

**Firma del Lavoratore**

\_\_\_\_\_