DISCIPLINARE PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI DA PARTE DEL PERSONALE

(approvato con delibera del Consiglio direttivo del 29 gennaio 2018 e quindi modificato dal Consiglio direttivo con delibera n. 219/15 adottata nella seduta del 28 ottobre 2024)

C.F./P.I. 00123590226
PALAZZO ACI - via Renato Lunelli nn. 2-4
38121 TRENTO - Tel. +39 0461 433100 - 133
info@acitrento.it - automobileclubtrento@pec.aci.it
www.acitrento.it - www.facebook.com/actrento

Art. 1 – Oggetto, finalità ed ambito di applicazione

Il presente Disciplinare regolamenta l'utilizzo degli strumenti informatici (postazioni di lavoro fisse e mobili, posta elettronica, internet ed intranet) che l'Ente mette a disposizione del personale ed ha la finalità di garantire la *privacy* dei dipendenti e prevenire usi indebiti degli stessi strumenti, in conformità alle indicazioni e linee guida fornite dal Garante per la *privacy*.

Il presente Disciplinare si applica a tutto il personale in servizio, anche a quello di ACIT srl. Le disposizioni che seguono si estendono, in quanto compatibili, a tutti coloro che, in qualità di utenti esterni, gestiscono ed utilizzano gli strumenti informatici forniti dall'Ente, sulla base di un rapporto di lavoro, di *stage* o tirocinio ovvero di fornitura o appalto di servizi.

Art. 2 – Prescrizioni interne sulla sicurezza dei dati e dei sistemi

L'Ente adotta un sistema di identificazione e di autorizzazione con il quale vengono riconosciuti e profilati gli utenti.

L'Ente prevede delle misure minime di sicurezza:

a) ai dipendenti in servizio è affidata una postazione di lavoro fissa; è facoltà assegnare postazioni mobili, anche in alternativa alla postazione fissa, o telefoni di servizio; è responsabilità del dipendente usare le dotazioni di lavoro in modo protetto ed esclusivamente per motivi di lavoro;

b) l'accesso alla postazione di lavoro è controllata da un codice segreto (password), in alcuni casi accompagnato da un codice utente (user-id), utilizzabili solo dall'utente;

c) il predetto codice (password) deve essere inserito con le cautele necessarie per conservarne la segretezza e deve essere periodicamente modificato dall'utente;

d) l'accesso alla postazione di lavoro deve essere bloccato ogni qualvolta ci si allontani da essa (digitando sulla tastiera "CTRL+ALT+CANC");

e) qualsiasi operazione effettuata con credenziali identificate dal sistema (user-id) verrà ricondotta al titolare delle medesime credenziali, indipendentemente dalla postazione di lavoro utilizzata, salvo prova contraria;

f) non è consentito al personale la modifica delle caratteristiche *hardware* e *software* impostate sulla postazione di lavoro, salvo autorizzazione esplicita dell'amministratore di sistema;

g) in caso di furto o smarrimento di strumenti informatici/telefonici, il dipendente al quale gli stessi strumenti sono affidati, oltre che denunciare l'accaduto all'Autorità, deve tempestivamente darne comunicazione all'Ente;

h) ogni dipendente è tenuto ad assumere comportamenti tali da ridurre il rischio di attacco al sistema informativo; è obbligatorio controllare costantemente la presenza e il regolare funzionamento del *software* antivirus aziendale e sospendere le attività in presenza di malevoli (cd. *malware*) informando tempestivamente l'esperto informatico;

i) in caso di assenza improvvisa o prolungata del dipendente, qualora il Responsabile di riferimento ne ravvisi urgenza e necessità, egli può accedere ai dati aziendali presenti nella postazione di lavoro del dipendente assente; a tal fine, deve essere utilizzata la *password* custodita in busta chiusa e sigillata.

Art. 3 – Accesso ed utilizzo di internet

L'Ente consente l'accesso ad Internet a tutti i dipendenti.

Internet e i servizi di rete devono essere utilizzati esclusivamente per fini lavorativi. L'Ente stabilisce inoltre che:

a) è consentita l'effettuazione di adempimenti *online* nei confronti di Pubbliche Amministrazioni e di concessionari di servizi pubblici o per tenere rapporti con istituti bancari e assicurativi, nei tempi strettamente necessari allo svolgimento delle transazioni;
b) è vietato "scaricare" o "prelevare" dalla rete Internet (cd. *download*) file musicali o multimediali; quando espressamente consentito dall'Ente, il personale è tenuto al rispetto della regolamentazione sul diritto d'autore, per quanto riguarda eventuali programmi scaricati dalla rete internet.
c) sono altresì vietate operazioni di invio di file alla rete internet se non per motivi di servizio (cd. *upload*).

Art. 4 – Utilizzo della posta elettronica nominativa

L'indirizzo di posta elettronica deve essere utilizzato esclusivamente per fini di lavoro. L'Ente stabilisce inoltre che:
a) non è consentito utilizzare la posta elettronica per ragioni personali; sono proibiti utilizzi impropri quali l'invio di messaggi diffamatori, osceni, di profanazione, lettere minatorie o di offesa razziale, messaggi commerciali o di propaganda, le cosiddette "catene di S. Antonio", nonché l'utilizzo della posta elettronica con modalità di forum;
b) il personale, nelle comunicazioni a mezzo posta elettronica con i vari livelli organizzativi, deve rispettare, di norma, gli ordinari riporti amministrativi; in ogni caso, ciascun dipendente è tenuto ad utilizzare un linguaggio appropriato ed una forma espositiva adeguata, secondo il comune sentire;
c) l'invio di messaggi di posta elettronica ad un elevato numero di destinatari è consentito solo qualora richiesto da specifiche esigenze di lavoro; è fatto salvo, in ogni caso, l'invio di circolari o analoghi messaggi usualmente indirizzati a tutto il personale o a specifici gruppi di posta;
d) si applicano all'utilizzo della posta elettronica le ordinarie regole di riservatezza e di segreto per ragioni d'ufficio; i documenti di lavoro possono essere inviati ad indirizzi di posta elettronica esterni solo se necessario per l'attività lavorativa;
e) in caso di file allegati, deve essere rispettata la capacità delle infrastrutture adottate al fine di non causare l'indisponibilità dei sistemi e dei dati;
f) il personale è tenuto a non aprire file allegati di incerta provenienza e dalla dubbia o doppia estensione (ad esempio: .exe, .pif); a non dare seguito a messaggi con dubbi oggetti e provenienza e a non fornire informazioni riguardanti dati personali e/o credenziali di autenticazione, se non dopo aver esperito i controlli del caso;
g) ciascun dipendente può delegare un altro dipendente quale "fiduciario", al fine di verificare i contenuti dei messaggi di posta elettronica in caso di assenza improvvisa o prolungata e per improrogabili necessità legate alla attività lavorativa;
h) ciascun dipendente, in caso di cessazione del rapporto di lavoro, è tenuto ad eliminare i messaggi di posta elettronica il cui contenuto non ritenga utile per assicurare la continuità funzionale delle attività svolte.

Art. 5 – Utilizzo della posta elettronica condivisa

L'Ente, per particolari esigenze lavorative, può istituire caselle di posta elettronica condivise interne (ad esempio segreteria, amministrazione, direzione e simili) al fine di garantire assistenza, formazione, regolamentazione ed informazione su particolari tematiche di interesse.
In merito alla posta condivisa, l'Ente stabilisce che:
a) il dipendente che risponde alle richieste avanzate attraverso le caselle di posta condivise dovrà apporre in calce alle stesse il proprio nominativo o la propria sigla, al fine di garantire la massima trasparenza per l'utente;

b) le risposte fornite tramite le caselle di posta elettronica condivise possono essere consultate da ciascun dipendente che abbia accesso alla stessa casella di posta;
c) le risposte fornite sono archiviate con le stesse modalità e gli stessi tempi previsti per le caselle di posta elettronica nominativa.

Art. 6 – Controlli sull'utilizzo di internet, della posta elettronica e della telefonia

L'Ente adotta idonei strumenti di controllo graduato, atti a indirizzare i singoli dipendenti verso un uso corretto e pertinente della posta elettronica, di internet e del telefono e forme di controllo anonimo, su dati aggregati, riferiti a specifiche aree lavorative o strutture organizzative.
A fronte di un rilevato utilizzo anomalo, il controllo può concludersi con un avviso generalizzato avente come scopo quello di invitare i dipendenti ad attenersi scrupolosamente alle istruzioni impartite circa l'utilizzo degli strumenti di lavoro.
In caso di successivi ripetuti utilizzi anomali, saranno effettuati controlli individuali sui dipendenti afferenti alle specifiche aree lavorative ed agli stessi dipendenti interessati al controllo.

Art. 7 – Utilizzo da parte dei dipendenti di dispositivi personali.

L'utilizzo di dispositivi di proprietà dei dipendenti (BYOD – Bring Your Own Device) per l'esecuzione di attività aziendali, inclusa la ricezione di OTP (One-Time Password) per la firma elettronica, è consentito in conformità con le linee guida di sicurezza stabilite dall'Ente.
I dipendenti sono tenuti a garantire che i loro dispositivi personali siano protetti da adeguate misure di sicurezza, come l'uso di *software* aggiornati e la protezione del dispositivo tramite PIN, password o altro sistema con effetti analoghi.
Non è invece consentito l'utilizzo di dispositivi di proprietà dei dipendenti per l'esecuzione di attività personali, salve le ipotesi normativamente previste e quelle di effettiva e documentabile necessità.

Art. 8 – Sanzioni e responsabilità

Il mancato rispetto o la violazione delle regole contenute nel presente Disciplinare è perseguibile con le sanzioni disciplinari previste dalla contrattazione collettiva, nonché con le azioni civili, penali e contabili previste dalla normativa vigente.