ORDINE DEI MEDICI CHIRURGHI E DEGLI ODONTOIATRI
DELLA PROVINCIA DI FIRENZE

REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI

(Deliberazione Consiglio Direttivo n. 302 del 13/12/2023)

PRINCIPI GENERALI

Con il presente Regolamento sono disciplinate le condizioni di utilizzo delle risorse informatiche e dei dispositivi fissi e mobili (personal computer, smartphone, tablet, modem/router, etc.), qualora utilizzate come strumenti informatici, che l'Ente mette a disposizione del personale dipendente e non dipendente (di seguito "utenti") per l'esecuzione delle funzioni istituzionali di competenza, non solo all'interno dei locali dell'Ente, ma anche in modalità remota o agile (smart working).

Scopo del Regolamento è la tutela dei beni di proprietà dell'Ente consegnati in uso agli utenti, al fine di evitare condotte inconsapevoli e/o scorrette, che possono esporre l'Ente a rischi connessi con la sicurezza, oltre ad eventuali danni patrimoniali a terzi o di immagine.

Sono disciplinate, tra l'altro, le modalità con le quali l'Ente può accertare e inibire le condotte illecite degli utilizzatori degli strumenti e dei servizi informatici messi a disposizione (Internet, posta elettronica e accesso alle risorse di archiviazione di massa quali server, hard disk, ecc.).

I criteri che devono essere seguiti dagli utenti per utilizzare gli strumenti informatici e di telefonia mobile sono:

- rispetto delle leggi e norme vigenti, in particolare le leggi in materia di sicurezza dei dati, tutela della privacy, tutela del copyright e modalità di accesso e uso dei sistemi informatici e telematici;
- rispetto delle norme e procedure lavorative generali, definite dalle strutture competenti dell'Ente;
- rispetto delle norme e procedure specifiche definite dall'Ufficio Informatica dell'Ente.

Gli strumenti informatici oggetto delle presenti istruzioni sono gli apparati ed i servizi di proprietà (o affidati in uso) dell'Ente, messi a disposizione degli utenti per svolgere quotidianamente il proprio lavoro: i PC, sia fissi che portatili, gli smartphone, la connessione ad Internet e gli strumenti di scambio di comunicazioni e file, la posta elettronica e la posta elettronica certificata, i programmi e gli applicativi in uso agli utenti tutti e qualunque altro strumento riconducibile ad attività informatica quali portali web, piattaforme e applicativi messi a disposizione da e per l'Ente.

Attenersi alle regole descritte in questo documento è un preciso obbligo dell'utente che utilizza gli strumenti informatici che gli sono stati assegnati.

I responsabili degli uffici devono verificare la corretta e puntuale messa in pratica delle disposizioni di cui al presente regolamento, al fine di garantire sui sistemi informativi dell'Ente la riservatezza dei dati, la loro integrità e la loro disponibilità.

Il presente Regolamento contiene quelle che, allo stato dell'arte, sono le misure adeguate ai sensi del regolamento UE 2016/679 (GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

La puntuale applicazione del presente regolamento e delle norme da questo richiamate permette all'Ente di garantire un uso dello strumento informatico a norma di legge, attenendosi anche a quanto riportato nella Circolare dell'Agenzia per l'Italia Digitale – AGID n.

2 del 18 aprile 2017 relativa a «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)».
Condotte non conformi al presente regolamento saranno valutate dall'Ente, anche ai fini disciplinari.
Gli strumenti informatici e i dispositivi mobili sono forniti all'utente per finalità esclusivamente lavorative. Non è quindi permesso utilizzare tali strumenti per altre finalità non connesse all'attività lavorativa o in modi che violino le leggi italiane ed europee in materia di sicurezza sul luogo di lavoro o, in generale, tutte le altre leggi applicabili alla Pubblica Amministrazione.
Ciascun utente è direttamente responsabile dell'utilizzo efficace, efficiente ed eticamente corretto degli strumenti, dei servizi e dei sistemi informativi. L'uso inappropriato o illegale del proprio PC e relativi strumenti, programmi e applicativi può comportare severe violazioni, anche di natura penale, con le eventuali conseguenti azioni legali nei confronti del soggetto che abbia commesso illecito.
Eventuali violazioni delle procedure di accesso e sicurezza dei sistemi informativi di cui un utente venga a conoscenza devono essere immediatamente segnalate all'Ente.
Inoltre, il presente Regolamento recepisce le indicazioni del Codice di comportamento dei dipendenti pubblici di cui al DPR 16 aprile 2013 come modificato dal DPR 13 giugno 2023, n. 81 che ha introdotto:
- l'art. 11-bis "utilizzo delle tecnologie informatiche" e
- l'art. 11-ter "utilizzo dei mezzi di informazione e social media".

In ottemperanza dell'art. 4, comma 1, Legge n. 300/1970, le norme del presente Regolamento non sono finalizzate all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma sono finalizzate a permettere a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali.
È garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli artt. 15-16-17-18-20-21-78 del Regolamento UE 2016/679.

UTILIZZO DEL PERSONAL COMPUTER
I personal computer, siano essi portatili o fissi, ed i relativi programmi e/o applicazioni affidati al dipendente sono strumenti di lavoro. Pertanto, ciascun dipendente è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione.

Gli utenti sono tenuti all'applicazione delle disposizioni e delle procedure di Legge e di lavoro dell'Ente relativamente alla custodia delle dotazioni, al fine di proteggere le apparecchiature informatiche assegnate da furti e dall'uso da parte di persone non autorizzate. Ogni utente è inoltre responsabile dell'adozione di precauzioni adeguate alla sicurezza e la tutela delle apparecchiature informatiche dell'Ente non sorvegliate. Tali disposizioni sono volte anche ad evitare accessi non autorizzati alle predette apparecchiature.
Gli utenti sono altresì tenuti a rispettare le disposizioni previste dalla normativa vigente in materia di tutela della salute e della sicurezza nei luoghi di lavoro (D.lgs 9 aprile 2008, n. 81 e smi) e le indicazioni specifiche fornite dagli organi dell'Ente competenti in materia.
Il PC deve essere utilizzato dagli utenti con la dovuta cura. In particolare, l'utente deve:
- assicurarsi che il proprio PC abbia attivata una procedura di autenticazione all'accensione;
- non lasciare il proprio PC acceso e incustodito quando il proprio utente è connesso e quindi l'accesso ai dati e alle applicazioni è garantito;
- assicurarsi che, allontanandosi dalla propria postazione, sia attivato lo screensaver fornito dal sistema operativo che richiede una password per essere disattivato;
- eseguire il processo di logout alla fine della sessione di lavoro e spegnere il pc a fine giornata lavorativa oppure con altra cadenza compatibile con il lavoro in modalità agile;

- salvare obbligatoriamente il proprio lavoro (file, dati e documenti) sulle risorse cloud/server aziendali o sulle piattaforme gestionali a disposizione dell'Ente, al fine di eliminare il rischio di perdita dei dati, e di avere accesso al proprio materiale di lavoro da qualsiasi postazione dell'Ente;
- nel caso di dati che debbano indispensabilmente essere salvati sulle unità locali del PC, l'utente è tenuto ad eseguire a propria cura il backup manuali degli eventuali dati locali (che non sono sotto altre procedure di backup);
- non modificare le caratteristiche hardware e software impostate sul proprio PC, salvo previa autorizzazione da parte dell'Ufficio Informatica;
- non utilizzare gli strumenti di archiviazione (risorse CLOUD, dispositivi USB, hard-disk removibili non forniti dall'Ente) per fini personali;
- non duplicare o diffondere software o file illegali (musica, film, ecc.) o software personali;
- non duplicare o diffondere il software aziendale senza specifica autorizzazione.

Al fine di evitare il rischio di intrusione e diffusione di malware, ovvero software creati con il solo scopo di causare danni più o meno gravi al sistema su cui vengono eseguiti (rientrano in questa categoria virus, worm, spyware e altri programmi dannosi), che costituiscono una delle minacce più frequenti alla sicurezza, è necessario che il personale si attenga alle seguenti norme:

- verificare periodicamente l'effettivo funzionamento dei software di protezione appositamente installati sul sistema e non disattivarli in nessuna occasione e per nessuna ragione. I software di protezione vengono aggiornati automaticamente tramite la rete interna dell'Ente; è indispensabile, pertanto, collegare sistematicamente, almeno una volta in ogni giornata di utilizzo, il PC fisso alla rete aziendale al fine di consentire l'esecuzione dei necessari aggiornamenti. Per i dispositivi portatili utilizzati in smart working il collegamento alla rete aziendale è raccomandato almeno una volta al mese;
- evitare il download e l'esecuzione di materiale che potrebbe contenere virus o altri software dannosi. Ogni eventuale download va eseguito con la supervisione dell'Ufficio Informatica o dell'Amministratore di Sistema;
- non scaricare mai file provenienti da mittenti sconosciuti o sospetti e, ove necessario, effettuare sempre un controllo tramite antivirus, prima di acquisire o aprire qualunque programma o documento acquisito via posta elettronica. In caso di dubbio contattare l'Ufficio Informatica.

L'utente è responsabile del corretto utilizzo e della diligente custodia del PC portatile e dell'eventuale smartphone o dispositivo di connettività mobile assegnatogli dall'Ente.

Alla consegna del dispositivo portatile e degli eventuali accessori forniti, l'assegnatario è tenuto, obbligatoriamente, a sottoscrivere le seguenti dichiarazioni:

- presa in consegna del dispositivo e degli eventuali accessori forniti;
- dichiarazione di conoscenza delle disposizioni previste nel presente regolamento.

L'utente è responsabile, sia durante gli spostamenti, sia durante l'utilizzo nel luogo di lavoro, che si tratti di una sede dell'Ente o di una postazione di smart working.

In particolare, la mancata o impropria custodia della attrezzatura informatica e/o di telefonia/connettività da parte dell'assegnatario può condurre ad ipotesi criminose, nel caso in cui tale attrezzatura venga sottratta, soprattutto alla luce delle disposizioni contenute in materia di trattamento dei dati personali ex D.lgs 101/2018.

Anche il danneggiamento dell'apparecchiatura, che cagiona danno all'Ente, è sottoposto alla responsabilità dell'utente e passibile di richiesta di risarcimento, ai sensi della normativa vigente.

Nel tragitto tra il domicilio dell'utente o la postazione di smartworking e la sede di servizio, il pc e/o i dispositivi mobili di servizio non devono essere mai lasciati incustoditi, devono essere

utilizzati esclusivamente dall'utente ai quali sono assegnati e devono essere riposti, quando inutilizzati, in un mobile o locale chiuso a chiave, o comunque non in vista, al fine di tutelare, anche in questo caso, sia l'integrità fisica dei dispositivi che quella dei dati, programmi, applicativi ai quali i dispositivi accedono, ovvero in essi contenuti.
In caso di furto o smarrimento del dispositivo (PC o dispositivo mobile) l'utente è tenuto a presentare immediatamente denuncia alle competenti Autorità di Pubblica Sicurezza e ad avvertire tempestivamente l'Ente.
Alla riconsegna del PC all'Ente, viene assicurata la conservazione dei dati di profilo dell'utente e di eventuali dati o documenti salvati sulle unità locali del PC per un periodo di norma di 30 (trenta) giorni dalla riconsegna stessa; dopo di che, ai sensi delle norme di tutela dei dati e di gestione dei sistemi, si procederà all'eliminazione sistematica e definitiva di tutti i dati, i documenti e gli applicativi presenti sull'unità.

CONTROLLO DEGLI ACCESSI

L'accesso alla rete aziendale ed ai sistemi aziendali è protetto da password individuale, che ha il compito di prevenire accessi da parte di soggetti non autorizzati ai sistemi. In relazione a ciò, allo scopo di cautelare l'Ente da ogni tipo di manomissione, furto o distruzione di dati e delle relative conseguenze, sia sul piano operativo che giuridico (penale e civile), vigono le seguenti disposizioni:

- è vietato connettere in rete stazioni di lavoro diverse da quelle di proprietà dell'Ente, comprese quelle personali dei dipendenti, se non dietro esplicita e formale autorizzazione dell'Ufficio Informatica;
- fa eccezione la possibilità di collegare il PC personale dei relatori alla rete dedicata della Sala Meeting in occasione di eventi, convegni o congressi. In proposito si applica il vigente regolamento per la concessione in uso temporaneo delle sale dell'Ordine per eventi;
- è vietato condividere cartelle in rete con servizi non messi a disposizione dall'Ente;
- è vietato monitorare ciò che transita in rete.

GESTIONE DELLE PASSWORD

La sicurezza dei servizi e delle procedure informatiche dell'Ente è basata sull'uso di password e, ove richiesto, di codici di sicurezza (PIN oppure OTP).
Pertanto, è necessario che ciascun utente scelga una password "robusta" e che tale password sia mantenuta rigorosamente segreta. A questo scopo è necessario scegliere la propria password seguendo i seguenti requisiti minimi, comuni a tutti i sistemi:

- non è possibile impostare password di lunghezza inferiore a 14 caratteri;
- la password deve includere, di regola, almeno tre delle seguenti caratteristiche: lettera maiuscola, lettera minuscola, cifre, caratteri speciali da selezionare fra quelli messi a disposizione dal sistema di autenticazione;
- la password non deve far riferimento ad informazioni personali o al servizio al quale si accede, riferimenti familiari o comunque dati inerenti direttamente al soggetto titolare della password stessa.

È necessario cambiare la password con regolarità e comunque secondo la periodicità stabilita dall'Amministratore di Sistema. Ad ulteriore garanzia di sicurezza, oltre che in adempimento a specifiche disposizioni legislative, le password di accesso ai sistemi sono soggette a rinnovo obbligatorio, con cadenza predefinita, con segnalazione all'utente dell'approssimarsi della scadenza. Per la gestione delle credenziali eventualmente scadute o dimenticate è necessario ricorrere ai servizi di assistenza informatica.
La password individuale deve essere riservata. L'utente, al riguardo, deve mantenere i seguenti accorgimenti:

- non trascrivere la password su pezzi di carta o post-it lasciati in vista sulla scrivania, o attaccati al monitor;
- non comunicare a nessuno la propria password;
- non condividere con nessuno la propria password;
- assicurarsi che nessuno guardi la tastiera con l'intenzione di memorizzare la password, mentre la si digita;
- non inviare la password tramite e-mail e, se proprio è necessario comunicarla, farlo a voce, per telefono o a mano in una busta chiusa o con altre modalità crittografate;
- non utilizzare la stessa password per più scopi o procedure informatiche;
- non utilizzare la funzione di memorizzazione automatica delle password inclusa nei vari browser;
- qualora sia stato affidato all'utente l'utilizzo di una procedura informatica con una password di default, ed il sistema non lo richieda automaticamente al primo accesso, è necessario che l'utente provveda a personalizzarla immediatamente al primo uso cambiandola con una password di propria scelta, impostata secondo i criteri sopra indicati.

Qualora le password vengano scritte per fini di backup su file digitali o cartacei, si raccomanda che questi documenti siano ben custoditi e ne sia inibito l'accesso agli estranei.

UTILIZZO DEI DISPOSITIVI MOBILI DI SERVIZIO

L'assegnazione e l'uso dei dispositivi di telefonia e connettività mobile (cellulari, smartphone, tablet, modem/router, etc.), come quelle dei personal computer, devono rispondere all'interesse ed alle esigenze dell'Ente, al fine di migliorare la qualità del lavoro e della produttività, in un quadro di economia, efficacia ed efficienza. I dispositivi possono essere utilizzati come strumento informatico, sia per la gestione della comunicazione, ad esempio a mezzo e-mail, che per la navigazione online, oppure per la connettività Internet.

È fondamentale, dunque:

- individuare le figure aziendali che necessitano di un dispositivo mobile per l'esercizio della propria mansione;
- razionalizzare e controllare le spese riguardanti i servizi di telefonia e connettività mobile dell'Ente;
- rispettare regole precise riguardo all'uso appropriato dei dispositivi mobili e delle relative utenze intestate all'Ente.

Di norma il dispositivo di telefonia mobile è assegnato al Presidente dell'Ordine. Il Consiglio Direttivo può individuare altri soggetti per i quali ritenga necessario tale assegnazione.

Il dispositivo mobile aziendale può essere utilizzato solo per ragioni di servizio, ed è obbligo di ogni assegnatario farne un uso appropriato ed averne una diligente cura, custodia e conservazione. L'apparecchio affidato all'utente non può essere dato in uso a colleghi o terzi.

La scheda SIM aziendale assegnata sia fisica che virtuale, così come i dispositivi, dovranno essere utilizzati solo ed esclusivamente per ragioni di servizio. Pertanto, non è consentito attivare servizi in abbonamento o traffico dati per uso personale e/o non autorizzati dall'Ente. L'utente dovrà inoltre custodire i codici PIN e PUK associati alla SIM aziendale fisica o virtuale.

Il dispositivo mobile aziendale è dato in uso all'assegnatario che, in analogia a quanto avviene per il personal computer e gli altri dispositivi informatici, ne diventa custode e responsabile del corretto utilizzo nel rispetto del presente regolamento. L'assegnazione dà luogo, in carico al titolare, delle medesime forme di responsabilità patrimoniale previste per i consegnatari di beni dell'Amministrazione, come già richiamate.

Alla consegna del dispositivo mobile aziendale, della relativa SIM card e degli eventuali accessori forniti, l'assegnatario è tenuto, obbligatoriamente, a sottoscrivere le seguenti dichiarazioni:

- presa in consegna del telefono cellulare aziendale e degli eventuali accessori forniti;
- presa in consegna della SIM card aziendale;
- dichiarazione di conoscenza delle disposizioni previste nel presente regolamento.

Analogamente a quanto già indicato con riferimento ai personal computer, il furto o smarrimento del dispositivo (telefono cellulare o smartphone, dispositivo di connessione remota o scheda SIM) deve essere immediatamente denunciato alle competenti Autorità di Pubblica Sicurezza, e tempestivamente comunicato all'Ente per le opportune segnalazioni al gestore del servizio.

USO DELLA RETE INTERNET

La navigazione su Internet, attraverso cavo di rete LAN o Wi-Fi, è un servizio che viene messo a disposizione degli utenti a supporto delle loro attività istituzionali.

L'Ente mette a disposizione:

- una rete LAN e una rete Wi-Fi ad uso esclusivo del personale dipendente, dei collaboratori continuativi e dell'Amministratore di Sistema che consente l'accesso alla rete aziendale;
- una rete Wi-Fi a disposizione degli utenti esterni (ospiti) per la sola navigazione in Internet, logicamente separata dalla rete aziendale.

Gli utenti sono tenuti a:

- navigare per il tempo strettamente necessario e solo per fini di natura lavorativa o professionale;
- non navigare su siti aventi contenuti di dubbia integrità morale, siti di hackers e siti di distribuzione di informazioni relative a software illegale;
- non fornire dati personali, numeri di carta di credito, l'indirizzo di posta elettronica, dati dell'Ente, su siti sconosciuti e la cui origine e gestione non sia certa e fidata;
- non scaricare mai nulla da siti la cui origine e gestione non sia certa e fidata ed in particolare non installare mai sul proprio computer software, giochi o screensaver non connessi con la propria attività lavorativa e scaricati da siti terzi o da fonti che non siano autorizzate o previste dalle procedure dell'Ente;
- non utilizzare servizi di scambio di informazioni disponibili su Internet (ad es. wetransfer) a meno che non siano stati autorizzati dall'Ente.

L'uso improprio della navigazione su Internet può comportare diverse conseguenze dannose, sia per l'utente che per l'Ente. Inoltre, può condurre a serie violazioni delle procedure di sicurezza dell'Ente ed in particolare a furti o distruzione di dati o più gravi danni patrimoniali, perseguibili a norma di Legge, in particolare:

- l'uso eccessivo della navigazione su Internet per fini personali o non connessi all'attività lavorativa comporta ingenti perdite di tempo, minore produttività sul lavoro e considerevole impegno delle risorse di rete messe a disposizione dall'Ente;
- l'uso inappropriato della navigazione su Internet, ad esempio la visione di siti illegali, può portare a pesanti violazioni di legge;
- il download di software non autorizzato o sconosciuto può portare instabilità e inaffidabilità del proprio PC con conseguente riduzione delle prestazioni e violazione delle procedure di sicurezza. Inoltre, può comportare la diffusione di codici malevoli (virus) all'interno della rete aziendale, con conseguenti violazioni delle norme disciplinari e di sicurezza e tutela dei dati. In particolare, può provocare l'introduzione di:
    - software spia (spyware) che tracciano l'attività dell'utente sul dispositivo, e la comunicano a all'esterno all'insaputa dell'utente stesso;
    - virus che compromettono l'integrità e la funzionalità del dispositivo, che possono essere trasmessi verso i sistemi di archiviazione dei dati aziendali, e che possono provocare la perdita e/o distruzione di dati, anche critici;

    - software installati in maniera trasparente per l'utente, che permettono il controllo remoto del nostro dispositivo e il furto di dati;
- il download di software illegalmente duplicato comporta l'assunzione, a totale carico dell'utente, di tutte le responsabilità conseguenti alla violazione della normativa sul copyright.

SOFTWARE DI FILE SHARING

Non è consentito agli utenti di fare uso di software di file sharing non preventivamente autorizzati dall'Ente.

A tal fine è necessario seguire le seguenti regole:

- non installare sui propri dispositivi software di file sharing di nessun genere a meno che non sia stato fornito dall'Ente;
- non creare librerie sui propri dispositivi di file musicali o video o che nulla hanno a che vedere con l'attività lavorativa;
- non utilizzare software di file sharing eventualmente fornito dall'Ente per condividere con utenti esterni risorse e file dei propri dispositivi;
- non utilizzare software di file sharing eventualmente fornito dall'Ente per condividere dati che nulla hanno a che vedere con l'attività lavorativa.

INSTANT MESSAGING, CHAT, PIATTAFORME DI COMUNICAZIONE E COLLABORAZIONE UNIFICATA

Non è consentito agli utenti di fare uso di software di instant messaging, chat, piattaforme di comunicazione e collaborazione unificata (Teams, Meet, Skype, Zoom, ecc.) per finalità non lavorative.

A tal fine è necessario seguire le seguenti regole:

- non installare sui propri dispositivi applicazioni di nessun genere a meno che non siano state fornite o autorizzate dall'Ente;
- non utilizzare applicazioni di instant messaging, chat, piattaforme di comunicazione e collaborazione unificata eventualmente forniti dall'Ente per fini personali o con utenti che non hanno rapporti lavorativi o professionali con esso;
- non aprire eventuali allegati ai messaggi istantanei la cui provenienza non sia certa e non installare mai sui propri dispositivi software ricevuto in allegati di messaggi istantanei.

LA POSTA ELETTRONICA STANDARD E LA PEC

La posta elettronica, sia standard che PEC (posta elettronica certificata), è uno strumento che viene messo a disposizione degli utenti per favorire lo scambio di informazioni e per migliorare la produttività del lavoro, ma non deve essere abusato e qualora utilizzato, deve essere utilizzato in modo consapevole, corretto e sicuro e nel rispetto delle procedure stabilite dall'Ente e delle leggi vigenti.

Posta elettronica ordinaria

Si raccomanda agli utenti di adottare cura e attenzione, nell'utilizzo della posta elettronica. A tal fine è necessario seguire le seguenti regole:

- non utilizzare la casella di posta elettronica fornita dall'Ente per fini personali;
- non inviare o promuovere la ricezione e la diffusione, tramite la posta elettronica, nel corpo o come allegato di un messaggio, di materiale pornografico, illegale, commerciale, spam o comunque non legato all'attività lavorativa e professionale;
- non inviare all'esterno dell'Ente, nel corpo o come allegato di un messaggio di posta elettronica, materiale e/o documenti di proprietà dell'Ente a meno che non sia previsto dai doveri di servizio;

- inviare i messaggi di posta elettronica solamente ai destinatari indispensabili, evitando di coinvolgere nella lettura delle e-mail destinatari non necessari, ed utilizzare in modo discreto e responsabile la rubrica degli indirizzi e-mail di tutti i destinatari;
- sul dispositivo fornito dall'Ente utilizzare sempre e solo la casella di posta elettronica fornita e conseguentemente non installare/configurare account di posta elettronica personali;
- qualora si ricevano messaggi che hanno provenienza ignota, dubbia o che presentano titoli ambigui regolarsi come segue:
    - non aprire messaggi la cui provenienza non sia certa;
    - non aprire mai allegati di messaggi di posta la cui natura non sia certa;
    - non aprire messaggi il cui oggetto/titolo è dubbio, anche se appaiono ricevuti da un mittente noto;
    - non fornire informazioni personali o finanziarie o password in risposte a comunicazioni di dubbia provenienza;
    - se possibile visualizzare i messaggi di posta elettronica sempre in formato "testo";
    - in caso di necessità, mantenere disattivata l'anteprima nel programma di posta elettronica. Una mail visualizzata in formato HTML potrebbe contenere del codice in grado di inviare il vostro indirizzo e-mail al mittente. Mantenere disattiva l'anteprima del messaggio permetterà di poter eliminare il messaggio senza aprirlo;
- qualora si ricevano messaggi che nulla hanno a che vedere con l'attività lavorativa e che si ritiene abbiano fini pubblicitari (SPAM):
    - non rispondere a messaggi di dubbia provenienza e che nulla hanno a che vedere con l'attività dell'Ente;
    - non fornire dati finanziari e password di un utente, con il rischio di essere vittima di phishing;
    - non cliccare su link che si trovano all'interno di mail pubblicitarie;
    - non rispondere mai alle mail degli spammer, nemmeno per rimuovere il proprio nominativo dalla loro lista;
    - spostare i messaggi nella cartella SPAM del sistema di posta, in modo che il sistema stesso possa acquisire informazioni utili a ridurre o debellare l'intrusione;
- segnalare all'Ufficio Informatica qualunque abuso del servizio di posta elettronica di cui l'utente sia venuto a conoscenza.

La PEC

La posta elettronica certificata (PEC) consente l'invio di messaggi la cui trasmissione è valida agli effetti di legge. La PEC ha lo stesso valore legale di una raccomandata tradizionale con avviso di ricevimento. Per certificare l'invio e la ricezione di un messaggio di PEC, il gestore di posta invia al mittente una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio e dell'eventuale documentazione allegata. Allo stesso modo, il gestore invia al mittente la ricevuta di avvenuta (o mancata) consegna del messaggio, con precisa indicazione temporale. L'utente che ha in uso tale tipo di posta elettronica sia che si tratti di un indirizzo individuale o legato ad un determinato settore/ufficio/funzione, deve rispettare le medesime regole soprariportate, riguardante l'uso della posta elettronica standard in dotazione.

SOCIAL NETWORK

In materia di uso dei social network da parte del personale dipendente e dei collaboratori, si fa riferimento a quanto prescritto nel vigente Codice di Comportamento dell'Ente o altri provvedimenti o disposizioni, interni o esterni, che ne disciplinano in particolare l'ambito.

Al fine di tutelare l'immagine e la reputazione dell'Ente in rete e salvaguardare i dipendenti e il loro lavoro, il soggetto incaricato di gestisce i canali social dell'Ente:

- agisce in nome e per conto dell'Ente, è strettamente tenuto al rispetto delle regole sopra riportate e comunque a tutto quanto riportato nel presente Regolamento;
- è personalmente responsabile della tenuta dell'account e della riservatezza dei codici di accesso ricevuti;
- non può utilizzare i profili social dell'Ente per scopi privati, personali, politici o commerciali;
- in caso di cessazione del rapporto di servizio con l'Ente, è tenuto a fornire all'Ente le chiavi di accesso ai social network.

ACCESSO AI DATI DEGLI UTENTI

Tutti i dati e le informazioni trattate dalle procedure informatiche sono di proprietà dell'Ente. Pertanto, qualsiasi diffusione della loro conoscenza e del loro utilizzo al di fuori dei doveri di servizio deve essere esplicitamente autorizzata.

È necessario seguire le seguenti regole:

- non utilizzare la rete dell'Ente per scambiare e/o condividere dati che nulla hanno a che vedere con l'attività lavorativa e non salvare sui server dell'Ente dati o file che nulla a che vedere con l'attività lavorativa;
- non visualizzare né copiare file o informazioni che si trovano sui PC di altri utenti o sui server dell'Ente e che non abbiano attinenza con l'attività lavorativa dell'utente;
- seguire le procedure di archiviazione standard dell'Ente per eseguire il salvataggio dei dati presenti sui dispositivi assegnati agli utenti.

Qualora per esigenze produttive o organizzazione del lavoro risulti necessario e urgente accedere a files o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un utente (quali file salvati, posta elettronica, ecc.) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato, si osservano le seguenti regole:

- il Dirigente o il Responsabile dell'Ufficio Informatica incaricano per iscritto l'Amministratore di Sistema di accedere alla risorsa con credenziali di amministratore ovvero tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'utente interessato, con avviso che al primo accesso alla risorsa l'utente dovrà inserire nuove credenziali;
- l'attività svolta dall'Amministratore di Sistema deve essere poi riepilogata per iscritto;
- l'accesso avviene nel rispetto dei principi di proporzionalità e non eccedenza rispetto alle finalità produttive e di organizzazione;
- qualora indirettamente durante l'accesso si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro.

VIRUS INFORMATICI

Al fine di minimizzare il rischio di infezione e di diffusione dei virus è necessario seguire le seguenti regole:

- non disinstallare o disabilitare il software antivirus, che deve sempre essere presente, attivo e aggiornato sul proprio PC;
- non installare sul proprio dispositivo software di nessun genere meno che non sia stato fornito o autorizzato dall'Ente;
- non collegare al proprio dispositivo apparecchi rimovibili di scambio dei dati (chiavette usb, hard disk esterni, ecc.) la cui provenienza non sia certa e sui quali possano essere contenuti virus o file infetti;
- non aprire messaggi di posta elettronica standard o certificata la cui provenienza non sia certa.

VIDEOSORVEGLIANZA

L'Ente utilizza un sistema di videosorveglianza presso la propria sede per la tutela del proprio patrimonio.

Ferme restando le disposizioni del Garante della Privacy in materia di videosorveglianza, dovranno essere rispettati i seguenti principi:

- il periodo di conservazione dei dati è di 24 ore successive alla rilevazione, salvo i giorni in cui i locali dell'Ente rimangono chiusi;
- tale termine può essere superiore nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'Autorità Giudiziaria o di Polizia Giudiziaria;
- i dati (immagini/video) non possono essere utilizzati per altre finalità ed in particolar modo è esclusa la finalità di controllo a distanza dell'attività lavorativa;
- i log di accesso ai dati registrati sono accessibili per 6 mesi;
- i dati (immagini/video) possono essere visionati solo da responsabili o incaricati del trattamento dei dati ai sensi della vigente normativa in materia di protezione dei dati personali.

ASSISTENZA TECNICA E MANUTENZIONI

L'Amministratore di Sistema può accedere ai dispositivi informatici dell'Ente sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:

- verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale;
- verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete;
- richieste di installazione/aggiornamento software e manutenzione preventiva hardware e software;
- periodico monitoraggio della funzionalità, efficienza e sicurezza dell'infrastruttura informatica dell'Ente.

Gli interventi tecnici posso avvenire previo consenso dell'utente quando l'intervento richiede l'accesso ad aree personali dell'utente stesso. Qualora l'intervento tecnico in loco o in remoto non necessiti di accedere mediante credenziali utente, l'Amministratore di Sistema è autorizzato ad effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata.

L'Amministratore di Sistema è altresì autorizzato ad effettuare interventi di tipo emergenziale senza il consenso dell'utente cui la risorsa è assegnata in caso di osservazione di potenziali pericoli per i sistemi informatici dell'Ente, come, ad esempio, il rilevamento di un virus da parte del sistema antivirus centralizzato o il rilevamento di attività di rete di tipo malevolo da parte di sistemi di intrusion detection o sulla base dell'analisi dei log del firewall. L'Amministratore di Sistema potrà in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema informativo e dei dati, sia sui PC assegnati agli utenti sia sulle unità di rete.

GLOSSARIO

Backup: duplicazione di un file o di un insieme di file su un supporto esterno al computer, per avere una copia di riserva.
Cloud: sistema configurato su server remoto che consente di disporre di risorse software e hardware (come memorie di massa per l'archiviazione di dati, o applicazioni), il cui utilizzo è erogato come servizio.
Download, scaricamento: ricevere o prelevare tramite rete telematica (ad esempio da un sito web) uno o più file, trasferendolo sul disco rigido del computer o su altra periferica.
File sharing: sistema per lo scambio di file tra utenti di Internet tramite un server comune.
Hard disk: principale unità di memorizzazione dei dati sul computer, in cui vengono memorizzati il sistema operativo, i programmi applicativi, i dati di configurazione del computer, ed eventualmente i documenti creati dall'utente.
Instant messaging: strumenti di comunicazione on-line, simultanea ed in tempo reale, tra due o più utenti.
Login: procedura di accesso a un sistema informatico, che prevede l'inserimento di un codice identificativo (UserID o nome utente) e di una parola d'ordine (Password) da parte dell'utente. Nei sistemi che richiedono particolari cautele di sicurezza può essere integrata con un codice (PIN), assegnato all'utente o rilasciato in tempo reale tramite telefono cellulare (OTP).
Logout: procedura di scollegamento da un sistema informatico a cui si era avuto accesso tramite un'operazione di login.
Password: parola d'ordine dell'utente.
Phishing: Truffa informatica effettuata inviando un'e-mail con il logo contraffatto di un istituto di credito o di una società di commercio elettronico, in cui si invita il destinatario a fornire dati riservati (numero di carta di credito, password di accesso al servizio di home banking, ecc.), motivando tale richiesta con ragioni di ordine tecnico.
PIN: codice alfanumerico breve (di solito non più di 8 caratteri) abbinato a nome utente e password, che integra la sicurezza negli accessi ai sistemi informatici.
OTP: codice numerico di sicurezza per accesso ai sistemi informatici, abbinato a nome utente e password, come il PIN, ma rilasciato tramite app o SMS sul telefono cellulare dell'utente, ed utilizzabile una sola volta per un tempo limitato.
Server: computer di elevate prestazioni, che in una rete distribuisce un servizio (un applicativo, o l'accesso a cartelle e file di dati) agli elaboratori degli utenti collegati, detti client.
Software: è l'insieme delle componenti immateriali di un sistema informatico, costituito principalmente dai programmi che vengono elaborati dal computer; è contrapposto all'hardware, cioè la parte materiale, tangibile, dello stesso sistema.
SPAM: messaggio pubblicitario non richiesto, inviato in modo massivo e ripetuto a un numero molto elevato di utenti di Internet, tramite posta elettronica.
Spyware: software scaricato, per lo più in maniera inconsapevole, durante la navigazione in Internet o l'installazione di un software gratuito, programmato per registrare e trasmettere a terzi dati personali e informazioni sull'attività online di un utente, generalmente a scopo pubblicitario.
Worm: sottoclasse di virus, software che crea diverse copie di sé stesso in uno stesso computer.