Ordine degli Ingegneri della Provincia di Savona
Ente pubblico non economico posto sotto l'alta vigilanza del Ministero della Giustizia, R.D. 2537/1925, art.57

Prot. 157/2019 Savona, 18/02/2019

Oggetto: REGOLAMENTO PER L'UTILIZZO DELLA STRUMENTAZIONE INFORMATICA DELL'ORDINE E DELLA RETE INTERNET

CAPO I – I PRINCIPI

1. SCOPO

Lo scopo del presente disciplinare interno è di definire l'ambito di applicazione, le modalità e le norme sull'utilizzo della strumentazione informatica da parte degli utenti assegnatari al fine di tutelare i beni dell'Ordine degli Ingegneri della Provincia di Savona (di seguito anche OISV) ed evitare condotte inconsapevoli e/o scorrette che potrebbero esporre OISV a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi. L'insieme delle norme comportamentali ivi incluse, pertanto, è volto a conformare OISV ai principi di diligenza, informazione e correttezza, con l'ulteriore finalità di prevenire eventuali comportamenti illeciti degli assegnatari, pur nel rispetto dei diritti ad essi attribuiti dall'ordinamento giuridico italiano. A tal fine, pertanto, si rileva che gli eventuali controlli ivi previsti escludono finalità di monitoraggio diretto ed intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa, con particolare riferimento al regolamento (UE) 2016/679, al Decreto Legislativo n. 196/2003 (c.d. Codice Privacy), al Decreto Legislativo n.101/2018, alla Legge n. 300/1970 (c.d. Statuto dei Lavoratori) alla luce delle modifiche intervenute ad opera del D. Lgv. 14 settembre 2015, n. 151 ed ai provvedimenti appositamente emanati dall'Autorità Garante (si veda in particolare Provv. 1° marzo 2007).

2. APPLICABILITÀ

La presente procedura si applica a tutti gli assegnatari. e al personale esterno incaricato da OISV che siano assegnatari di beni e risorse informatiche di OISV ovvero utilizzatori di servizi e risorse informative di pertinenza di OISV.

3. TERMINI E DEFINIZIONI

– Chat: servizio offerto da Internet, che mediante apposito software permette a più interlocutori di conversare scambiandosi messaggi scritti che appaiono in tempo reale sul monitor di ciascuno;
− Client: personal computer collegato in rete a un altro computer (server), sul quale risiedono i dati che il primo utilizza;
− Computer portatile o laptop: elaboratore elettronico dell'Ente trasportabile con facilità;
− E-mail: messaggio inviato tramite posta elettronica;
− Ente: L'OISV, l'organizzazione e/o comunque il Titolare dei beni e delle risorse informatiche ivi disciplinate, il quale opererà per mezzo dei soggetti che ne possiedono la rappresentanza.
− Estensione: set di tre lettere che segue il nome di un file di un computer e ne identifica il genere;
− Log: registrazione ufficiale di eventi;
− Password: parola o sigla di riconoscimento fornita dall'utente al computer per poter accedere a un sistema operativo a un programma o a un file;

− Peer to peer: sistema di computer collegati gli uni agli altri senza la connessione ad un server; − Personal Computer: elaboratore Elettronico destinato all'uso dell'Ente;
− Phishing: l'attività criminale di mandare e-mail o costituire un sito web al fine di ingannare qualcuno e carpire informazioni (es. numeri di carta di credito o password).
− Rete Ente: sistema di trasmissione delle informazioni costituito da linee di collegamento e da stazioni che possono essere costituite da elaboratori, terminali o unità di memoria;
− Server: computer collegato in rete ad altri computer (client), sul quale risiedono i dati che questi utilizzano;
− Smartphone: apparecchio elettronico che combina le funzioni di un telefono cellulare e di un computer palmare.
− Spamming: mandare messaggi a diverse persone tramite e-mail o internet generalmente a fini commerciali;
− Tablet: elaboratore elettronico di proprietà dell'Ente compatto con interfaccia touch;
− Utente: colui che si serve di un'attrezzatura di lavoro;

4. TITOLARITA' DEI BENI E DELLE RISORSE INFORMATICHE
I beni e le risorse informatiche, i servizi ICT e le reti informative costituiscono beni dell'Ente rientranti nel patrimonio sociale e sono da considerarsi di esclusiva proprietà dell'Ente. Il loro utilizzo, pertanto, è consentito solo per finalità di adempimento delle mansioni affidate ad ogni Utente in base al rapporto in essere (ovvero per scopi professionali afferenti l'attività svolta per l'Ente), e comunque per l'esclusivo perseguimento degli obiettivi prefissati. A tal fine si precisa sin d'ora che qualsivoglia dato e/o informazione trattato per mezzo dei beni e delle risorse informatiche di proprietà dell'Ente, sarà dalla stessa considerata come avente natura professionale dell'Ente e non personale.

5. RESPONSABILITÀ PERSONALE DELL'UTENTE
Ogni Utente è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidatigli dall'Ente nonché dei relativi dati trattati per finalità dell'Ente stesso. A tal fine ogni Utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con l'Ente, è tenuto a tutelare (per quanto di propria competenza) il patrimonio assegnatogli da utilizzi impropri e non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia. L'obiettivo è quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse dell'Ente. Ogni Utente, pertanto, è tenuto, in relazione al proprio ruolo e alle mansioni in concreto svolte, ad operare a tutela della sicurezza informatica dell'Ente, riportando al proprio responsabile e al DPO (Data Protection Officer) e senza ritardo eventuali rischi di cui è a conoscenza ovvero violazioni del presente disciplinare interno. Sono vietati comportamenti che possano creare un danno, anche di immagine, all'Ente.

6. AGGIORNAMENTO
L'aggiornamento del presente regolamento è competenza del Consiglio dell'Ordine degli Ingegneri della Provincia di Savona ed è sottoposto a parere del DPO.

CAPO II – MISURE ORGANIZZATIVE

7. AMMINISTRATORI DEL SISTEMA

L'Ente conferisce all'amministratore di sistema il compito di sovrintendere i beni e le risorse informatiche dell'Ente. I principali compiti, a titolo meramente esemplificativo e non esaustivo sono:
1) gestire l'hardware e il software di tutta la strumentazione informatica di appartenenza dell'Ente;
2) gestire la creazione, l'attivazione, la disattivazione, e tutte le relative attività amministrative degli account di rete e dei relativi privilegi di accesso alle risorse, previamente assegnati agli utenti;
3) monitorare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi affidati agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
4) creare, modificare, rimuovere o utilizzare qualunque account o privilegio purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;
5) rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli utenti, solo ove le medesime siano previste nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;
6) provvedere alla sicurezza informatica dei sistemi informatici dell'Ente, nel rispetto di quanto prescritto dal D.lgs. 196/2003 e regolamento (UE) 2016/679;
7) utilizzare le credenziali di accesso di amministratore del sistema per accedere, anche da remoto, ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un Utente in caso di prolungata assenza, irreperibilità o impedimento dello stesso. Tale ultima attività, tuttavia, deve essere disposta per mezzo di un soggetto che rivesta quantomeno la posizione di Responsabile Sicurezza e Protezione dei Dati (RSPD) all'interno dell'Ente e deve essere limitata altresì al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto, e deve essere prontamente informato l'utente prima di resettare le credenziali di accesso per effttuare accesso terzo.

8. ASSEGNAZIONE DEGLI ACCOUNT E GESTIONE DELLE PASSWORD

Creazione e gestione degli Account

Un account Utente consente l'autenticazione dell'utilizzatore e di conseguenza ne disciplina l'accesso alle risorse informatiche dell'Ordine, per singola postazione lavorativa. La gestione di tali account segue quanto sotto espressamente previsto:
- l'accesso al proprio account avviene tramite l'utilizzo delle "credenziali di autenticazione" (es. "Username" e "Password"), comunicate all'Utente dall'amministratore di sistema, che le genera, attraverso modalità che ne garantiscano la segretezza; - le credenziali di autenticazioni costituiscono dati dell' Ente da mantenere strettamente riservati e non è consentito comunicarne gli estremi a terzi; - se l'Utente ha il sospetto che le proprie credenziali di autenticazione siano state identificate da qualcuno, o il sospetto di un utilizzo non autorizzato del proprio account e delle risorse a questo associate, lo stesso è tenuto a modificare immediatamente la password e/o a segnalare la violazione all'amministratore del sistema nonché al Responsabile privacy di riferimento;
- ogni Utente è responsabile dell'utilizzo del proprio account Utente;
- in caso di assenza improvvisa o prolungata dell'assegnatario e per improrogabili necessità legate all'attività lavorativa, per le esigenze produttive dell'ente o per la sicurezza ed operatività delle risorse informatiche, l'Ente si riserva la facoltà, informando l'utente assegnatario del profilo preventivamente al reset delle credenziali di accesso, di accedere a qualsiasi dotazione e/o apparato assegnato in uso all'Utente per mezzo dell' intervento dell'Amministratore di sistema.

Gestione e utilizzo delle password

Dopo la prima comunicazione delle credenziali di autenticazione da parte dell'amministratore di sistema, l'Utente ha il compito di modificare, al suo primo utilizzo, la propria password, procedendo allo stesso modo ogni 90 giorni, quando il sistema di controllo accessi ne viene richiesto il cambio. L'Utente, nel definire il valore della password, deve rispettare le seguenti regole:

• utilizzare almeno 8 caratteri alfanumerici, inclusi i caratteri speciali (#, %, etc.);
• utilizzare almeno tre delle seguenti categorie: un carattere maiuscolo, un carattere minuscolo, un numero, un carattere non alfanumerico tipo "@#§£$%...";
• evitare di includere parti del nome, cognome e/o comunque elementi a lui agevolmente riconducibili;
• evitare l'utilizzo di password comuni e/o prevedibili;
• proteggere con la massima cura la riservatezza della password ed utilizzarla entro i limiti di autorizzazione concessi.

Si ricorda che la password non deve essere annotata su post-it o altri supporti (ivi compresa la sua memorizzazione sul telefono/smartphone lavorativo) non è conforme alla normativa e costituisce violazione del presente disciplinare interno.

Cessazione degli Account

In caso di interruzione e/o cessazione del rapporto di lavoro con l'Utente, le credenziali di autenticazione di cui sopra verranno disabilitate entro un periodo massimo di 96 ore da quella data; entro un mese, invece, si disporrà la definitiva e totale disabilitazione dell'account Utente. Qualora vi sia richiesta di reset password di un utente a qualsiasi titolo, perché, per esempio, sussiste il dubbio che terzi ne siano venuti a conoscenza o perché dimenticata, l'amministratore di sistema procederà a riassegnare una nuova password temporanea al fine di consentire all'utente l'accesso ai sistemi presso cui è accreditato, con l'impegno di modificarla al primo accesso successivo al reset.

9. POSTAZIONI DI LAVORO

Per postazione di lavoro si intende il complesso unitario di Personal Computer (di seguito, PC), notebook, accessori, periferiche e ogni altro device concesso, dall'Ente, in utilizzo all'Utente. L'assegnatario di tali beni e strumenti informatici dell'ente, pertanto, ha il compito di farne un uso compatibile con i principi di diligenza sanciti nel codice civile. Al fine di disciplinare un corretto utilizzo di tali beni, l'Ente ha adottato le regole tecniche, che di seguito si riportano:

• ogni PC, notebook (accessori e periferiche incluse), e altro device, sia esso acquistato, noleggiato, o affidato in locazione, rimane di esclusiva proprietà dell'Ente, ed è concesso all'Utente per lo svolgimento delle proprie mansioni lavorative e comunque per finalità strettamente attinenti l'attività svolta;
• è dovere di ogni Utente usare i computer e gli altri dispositivi a lui affidati responsabilmente e professionalmente;
• il PC e gli altri dispositivi di cui sopra devono essere utilizzati con hardware e software autorizzati dall'Ente. Per utilizzare software o applicativi non presenti nella dotazione standard fornita, si necessita di espressa autorizzazione dell'Ente;
• le postazioni di lavoro non devono essere lasciate incustodite con le sessioni utenti attive;
• quando un Utente si allontana dalla propria postazione di lavoro, deve bloccare tastiera e schermo con un programma salvaschermo (screensaver) protetto da password o effettuare il log-out dalla sessione;

• l'Utente deve segnalare con la massima tempestività all'amministratore del sistema ovvero al proprio Responsabile di riferimento eventuali guasti tecnici, problematiche tecniche o il cattivo funzionamento delle apparecchiature;
• è fatto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici dell'Ente a soggetti terzi.
• l'Ente si riserva la facoltà di rimuovere qualsiasi elemento hardware o software la cui installazione non sia stata appositamente e preventivamente prevista o autorizzata.
• in caso di attività di manutenzione ovvero di fine assegnazione, gli strumenti informatici verranno consegnati all'Ente. Gli apparecchi di proprietà personale dell'Utente quali computer portatili, telefoni cellulari, agende palmari (PDA), hard disk esterni, penne USB, lettori musicali o di altro tipo, fotocamere digitali, ecc. non potranno essere collegati ai computer o alle reti informatiche dell'ente, salvo preventiva autorizzazione scritta dell'Ente.

CAPO III – CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI
10 – PERSONAL COMPUTER, COMPUTER PORTATILI

Il personal computer, il computer portatile presente sul proprio posto di lavoro o assegnato sono considerati quali strumenti di lavoro di proprietà dell'Ente, e devono essere utilizzati per compiere mansioni lavorative. Ne consegue che gli utenti sono tenuti al rispetto delle seguenti regole:
- non è consentito modificare la configurazione hardware e software del proprio PC, se non previa esplicita autorizzazione dell'Ente;
- non è consentito rimuovere, danneggiare o asportare componenti hardware;
- non è consentito installare autonomamente programmi informatici, software ed ogni altro applicativo non autorizzato espressamente dall'Ente;
- non è consentito connettere al personal computer o al computer portatile apparecchi elettronici (telefoni cellulari personali o dell'Ente, agende elettroniche, PC portatili, chiavi USB, ecc.)
- è onere dell'Utente, in relazione alle sue competenze, eseguire richieste di aggiornamento sulla propria postazione di lavoro derivanti da software antivirus nonché sospendere ogni attività in caso di minacce virus o altri malfunzionamenti, segnalando prontamente l'accaduto all'amministratore del sistema;
- per quanto concerne, invece, la gestione dei computer portatili, l'Utente ha l'obbligo di custodirli con diligenza e in luogo protetto durante gli spostamenti. Non è consentito all'Utente caricare o inserire all'interno del portatile qualsiasi dato personale non attinente con l'attività lavorativa svolta. In ogni caso, al fine di evitare e/o ridurre al minimo la possibile circolazione di dati personali sull'apparecchio, si ricorda agli utenti di cancellare tutti i dati eventualmente presenti prima di consegnare il portatile agli uffici competenti per la restituzione o la riparazione. Sul server centrale l'Ente può creare uno spazio riservato all'Utente per la conservazione dei dati, al fine di permettere all'utente di conservarvi file di lavoro. L'assegnatario è tenuto ad utilizzare detto spazio per conservare esclusivamente dati appartenenti all' Ente in quanto i file in esso contenuti possono essere aperti, spostati e ulteriormente sottoposti a lettura e/o modifica. Nel caso in cui l'Utente vi conservi, contrariamente alle direttive impartitegli, dati di natura personale, l'Ente in nessun caso potrà essere ritenuto responsabile della salvaguardia o della perdita di tali dati. Il personale IT ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente e in sua presenza. E' obbligo dell'Utente mantenere attivo l'aggiornamento automatico del sistema operativo nonché dell'antivirus.

11. SOFTWARE

Premesso che l'installazione di software privi di regolare licenza non è consentita in nessun caso, gli utenti dovranno ottenere espressa autorizzazione dell'Ente (cfr. art. 21) per installare o comunque utilizzare qualsiasi programma o software dotato di licenza non proprietaria ("freeware" o "AGPL"). L'Ente richiama l'attenzione del proprio personale su alcuni aspetti fondamentali che l'Utente è tenuto ad osservare per un corretto utilizzo del software all'interno dell'ente:

• l'Ente acquista le licenze d'uso dei software da vari fornitori esterni. L'Utente, pertanto, è soggetto a limitazioni nell'utilizzo di tali programmi e della relativa documentazione e non ha il diritto di riprodurlo in deroga ai diritti concessigli. Tutti gli utenti sono quindi tenuti a utilizzare il software entro i limiti specificati nei contratti di licenza;

• non è consentito fare né il download né l'upload tramite internet di software non autorizzato;

• l'Ente, sulla scorta di quanto disposto dalle normative a tutela della proprietà intellettuale e del diritto d'autore, ricorda che le persone coinvolte nella riproduzione illegale del software sono responsabili sia civilmente che penalmente e quindi possono essere condannate al pagamento dei danni e anche alla reclusione;

• in nessun caso l'Ente utilizza software o altri strumenti di tipo Key Log per la registrazione delle operazioni eseguite da tastiera;

• l'Ente non tollererà la duplicazione illegale del software.

12. DISPOSITIVI MOBILI DI CONNESSIONE (INTERNET KEY)

Agli assegnatari di computer portatili, può essere data in dotazione anche una chiavetta per la connessione alla rete dell'ente, volta a facilitare lo svolgimento delle mansioni lavorative anche da remoto. I suddetti dispositivi devono essere utilizzati esclusivamente sui computer forniti in dotazione dall'Ente e non è consentito concederne l'utilizzo a soggetti terzi, né utilizzarli su computer privati. Specifiche relative ai limiti entro cui l'Utente potrà utilizzare il servizio offerto tramite la chiavetta, sono riportate nella scheda tecnica consegnata all'Utente unitamente al dispositivo di cui sopra. L'Utente dovrà attenersi ai suddetti limiti, potendo in caso contrario l'Ente richiedere il rimborso dei costi sostenuti per il superamento degli stessi.

13. DISPOSITIVI DI MEMORIA PORTATILI

Per dispositivi di memoria portatili si intendono tutti quei dispositivi che consentono di copiare o archiviare dati, file o documenti esternamente al computer. Sono considerati tali CD-ROM, DVD, penne o chiavi di memoria USB, fotocamere digitali, dischi rigidi esterni, etc. L'utilizzo di tali supporti risponde alle direttive che di seguito si riportano:

- non è consentito utilizzare supporti rimovibili personali per lo scambio dati, se non preventivamente autorizzati per iscritto dalla Ente;
- è onere dell'Utente custodire i supporti magnetici contenenti dati sensibili e giudiziari in armadi chiusi a chiave, onde evitare che il loro contenuto possa essere trafugato e/o alterato e/o distrutto. In caso di utilizzo di supporti di memoria esterno o di scambio di di dati sensiobili o giudiziari in formato elettornico, è necessario crittografare i dati per evitare peridata di dati in caso di smarrimento o furto dei supporti.
- Si precisa che, ove autorizzati in base a quanto sopra disposto, una volta connessi all'infrastruttura informatica dell'ente, i dispositivi saranno soggetti (ove compatibili) al presente disciplinare interno.

14. STAMPANTI, FOTOCOPIATRICI E FAX

L'utilizzo dei suddetti strumenti deve avvenire sempre per scopi professionali. Non è consentito un utilizzo per fini diversi o privati, salvo una specifica autorizzazione da parte dell'Ente. E' richiesta una particolare attenzione quando si invia su una stampante condivisa documenti aventi ad oggetto dati personali o informazioni riservate; ciò al fine di evitare che persone non autorizzate possano venirne a conoscenza. Si richiede quindi di evitare di lasciare le stampe incustodite e ritirarne immediatamente le copie non appena uscite dalla stampa. L'utilizzo dei fax per l'invio di documenti che hanno natura strettamente confidenziale, è generalmente da evitare. Nei casi in cui questo sia necessario, si deve preventivamente avvisare il destinatario, in modo da ridurre il rischio che persone non autorizzate possano venirne a conoscenza, e successivamente chiedere la conferma telefonica di avvenuta ricezione.

15. STRUMENTI DI FONIA MOBILE E/O DI CONNETTIVITA' IN MOBILITA'

L'Ente mette a disposizione, a seconda del ruolo o della funzione del singolo Utente, impianti di telefonia fissa e mobile, nonché dispositivi - quali smartphone e tablet - che consentono di usufruire della navigazione in internet tramite rete dati e/o del servizio di telefonia tramite rete cellulare. Specifiche relative ai limiti entro cui l'Utente potrà utilizzare tali strumenti sono riportate nella scheda tecnica consegnata all'Utente unitamente ai dispositivi di cui sopra. L'Utente dovrà attenersi ai suddetti limiti, potendo in caso contrario l'Ente richiedere il rimborso dei costi sostenuti per il superamento degli stessi. Come per qualsiasi altra dotazione, il dispositivo mobile rappresenta un bene dell'Ente che è dato in uso per scopi esclusivamente lavorativi. E' tuttavia concesso un utilizzo personale sporadico e moderato dei telefoni dell' OISV utilizzando la c.d. "diligenza del buon padre di famiglia" e comunque tale da non ledere il rapporto fiduciario instaurato con il cessionario (Ente). A tal fine si informano gli utilizzatori dei servizi di fonia dell'ordine, che l'Ente eserciterà i diritti di cui all'art. 124 D.lgs. 196/2003 e successive modifiche (cd. fatturazione dettagliata), richiedendo ai provider di telefonia i dettagli necessari ad effettuare controlli sull'utilizzo ed i relativi costi di traffico effettuato nel tempo. I controlli saranno eseguiti secondo le modalità descritte all'art. 18 del presente disciplinare interno. L'Ente si riserva la facoltà, qualora dall'esame del traffico di una singola utenza rilevi uno scostamento significativo rispetto alla media del consumo, di richiedere un tabulato analitico delle chiamate effettuate dalla SIM in incarico all'Utente per il periodo interessato. L'utilizzo dei dispositivi ivi disciplinati risponde alle regole che di seguito si riportano: - ogni Utente assegnatario del dispositivo è responsabile dell'uso appropriato dello stesso, e, conseguentemente, anche della sua diligente conservazione, ivi compresa l'eventuale codice IMEI dei dispositivi di fonia e di connessione mobile. I dispositivi devono essere dotati di password di sicurezza (cd. codice pin del dispositivo) che ne impedisca l'utilizzo da parte di soggetti non autorizzati. A tal fine si precisa che:

• il CODICE PIN dovrà essere composto di n. 4 cifre numeriche;
• il CODICE PIN dovrà essere modificato dall'assegnatario con cadenza al massimo semestrale;
• ogni Utente deve adottare le necessarie e dovute cautele per assicurare la segretezza della password e, qualora ritenga che un soggetto non autorizzato possa esserne venuto a conoscenza, dovrà provvedere immediatamente a cambiarla dandone comunque comunicazione all'Ente; - in caso di danneggiamento l'Utente assegnatario dovrà darne immediato avviso all'Ente; in caso di furto o smarrimento del dispositivo mobile in oggetto, l'Utente assegnatario dovrà denunciare il fatto alle competenti autorità pubbliche e darne successivo avviso all'Ente; ove detti eventi siano riconducibili ad un comportamento negligente, imprudente dell'Utente e/o comunque a sua colpa nella custodia del bene, lo stesso sarà ritenuto unico responsabile dei danni derivanti;

- in caso di furto o smarrimento l'Ente si riserva la facoltà di attuare la procedura di remote-wipe (cancellazione da remoto di tutti i dati sul dispositivo), rendendo il dispositivo inutilizzabile e i dati in esso contenuti irrecuperabili; - non è consentito all'Utente caricare o inserire all'interno del dispositivo o SIM qualsiasi dato personale non attinente con l'attività lavorativa svolta, salvo quanto previsto dal successivo paragrafo. In ogni caso, al fine di evitare e/o ridurre al minimo la possibile circolazione di dati personali sull'apparecchio, si ricorda agli assegnatari di cancellare tutti i dati eventualmente presenti prima di consegnare il cellulare agli uffici competenti per la restituzione o la riparazione.
-.
- non è consentito all'Utente effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi;
- non è consentito all'Utente effettuare procedure di jailbreak, modifiche del firmware o procedure di sblocco a vario titolo, tali da permettere l'illegittima installazione di software e/o applicazioni coperte da copyright;
- è onere dell'Utente mantenere installato il software antivirus sullo smartphone dell'ente, così come fornito dall'amministratore di sistema; in caso di problemi l'Utente potrà rivolgersi al Personale IT competente;
- l'eventuale installazione di applicazioni, sia gratuite che a pagamento, sugli smartphone e tablet deve essere espressamente autorizzata, rimanendo, diversamente, a carico dell'Utente le spese che l'Ente dovrà sostenere, nonché le responsabilità derivanti dall'installazione non autorizzata;
- per motivi di sicurezza sul lavoro i dipendenti devono limitare l'uso dei telefoni privati a casi eccezionali e devono sempre subordinare l'uso di suddette apparecchiature alla sicurezza. In particolare, nel caso in cui dovessero avere necessità di utilizzare le apparecchiature telefoniche (anche dell'ente) durante la guida di mezzi, è consentito l'uso di apparecchi a viva voce o dotati di auricolare purché non richiedano per il loro funzionamento l'uso delle mani e il conducente abbia adeguate capacità uditive. L'Ente proibisce espressamente di collegare i dispositivi mobili personali alla rete internet riservata ai dispositivi dell'ente.

CAPO IV – GESTIONE DELLE COMUNICAZIONI TELEMATICHE

16. GESTIONE UTILIZZO DELLA RETE INTERNET

Ogni Utente potrà essere abilitato, dall'Ente, alla navigazione Internet. Col presente disciplinare interno si richiama gli utenti ad una particolare attenzione nell'utilizzo di Internet e dei servizi relativi, in quanto ogni operazione posta in essere è associata all'"Indirizzo Internet Pubblico" assegnato all'Ente stesso. Internet è uno strumento messo a disposizione degli utenti per uso professionale. Ciascun lavoratore, pertanto, deve quindi usare la rete Internet in maniera appropriata, tenendo presente che ogni sito web può essere governato da leggi diverse da quelle vigenti in Italia; l'Utente deve quindi prendere ogni precauzione a tale riguardo. Le norme di comportamento da osservare nell'utilizzo delle connessioni ad Internet sono le seguenti:
a. l'utilizzo è consentito esclusivamente per scopi professionali e, pertanto, non è consentito navigare in siti non attinenti allo svolgimento delle proprie mansioni lavorative;
b. non è consentita l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, ad esclusione delle operazioni / casi espressamente autorizzati dall'Ente e rientranti nell'attività lavorativa dell'Utente;
c. è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;

d. non sono permesse, se non per motivi professionali, la partecipazione a forum, l'utilizzo di chat-line o di bacheche elettroniche e le registrazioni in guest-book, anche utilizzando pseudonimi (o nickname);
e. non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica, pedopornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
f. è consentito l'utilizzo di soluzioni di Instant Messaging e/o chat esclusivamente per scopi professionali ed attraverso gli strumenti ed i software messi a disposizione dall'Ente;
g. non è consentito l'utilizzo di sistemi di social networking sul luogo di lavoro o durante l'orario lavorativo;
h. non è consentito lo scambio e/o la condivisione (es. i c.d. sistemi di Peer-to-Peer) a qualsiasi titolo, anche se non a scopo di lucro, di materiale audiovisivo, cinematografico, fotografico, informatico, etc., protetto da copyright;
i. non è consentito sfruttare i marchi registrati, i segni distintivi e ogni altro bene immateriale di proprietà dell'Ente in una qualsiasi pagina web o pubblicandoli su Internet, a meno che tale azione non sia stata approvata espressamente. L'Ente proibisce altresì di utilizzare i social network per lo scambio di qualsiasi informazione avente carattere lavorativo. È altresì proibito rigorosamente qualsiasi uso del Web che non trasmetta un'immagine positiva o che possa essere nocivo all'immagine dell'Ente. Per facilitare il rispetto delle predette regole, l'Ente si riserva, per mezzo dell'amministratore di sistema, la facoltà di configurare specifici filtri che inibiscono l'accesso ai contenuti ivi non consentiti (con esclusione dei siti istituzionali) e che prevengono operazioni non correlate all'attività lavorativa (es. upload, restrizione nella navigazione, download di file o software). L'eventuale conservazione di dati è effettuata per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza. I sistemi software sono programmati e configurati in modo da cancellare periodicamente e automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la cd. rotazione dei log file) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

17. GESTIONE E UTILIZZO DELLA POSTA ELETTRONICA DELL'ENTE

Principi guida

Ad ogni Utente titolare di un account, l'Ente provvede ad assegnare una casella di posta elettronica individuale per tutta la durata del rapporto. I servizi di posta elettronica devono essere utilizzati a scopo professionale: si ricorda a tutti gli utenti che l'account email è uno strumento di proprietà dell'Ente ed è conferito in uso per l'esclusivo svolgimento delle mansioni lavorative affidate. Ad uno stesso Utente possono essere assegnate più caselle di posta elettronica che possono essere condivise con altri utenti dello stesso gruppo/dipartimento. Tali caselle devono essere utilizzate per la ricezione dei messaggi, mentre per le risposte o gli invii, è consigliabile utilizzare la casella di posta individuale assegnata. L'Ente valuterà caso per caso e previa richiesta dell'Utente, la possibilità di attribuire allo stesso un diverso indirizzo destinato ad uso privato. Attraverso l'e-mail dell'Ente, gli utenti rappresentano pubblicamente la società e per questo motivo viene richiesto di utilizzare tale sistema in modo lecito, professionale e comunque tale da riflettere l'immagine dell'Ente. Gli utenti sono responsabili del corretto utilizzo delle caselle di posta elettronica dell'Ente e sono tenuti ad utilizzarla in modo conforme alle presenti regole. Gli stessi, pertanto, devono:
- conservare la password nella massima riservatezza e con la massima diligenza, nel rispetto di quanto previsto dal suindicato capitolo 8 (Gestione e Utilizzo delle password);

- mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti. Il limite della dimensione della casella postale è fissato in 50Gb per Utente;
- prestare attenzione alla dimensione degli allegati per la trasmissione di file all'interno della struttura nonché alla posta ricevuta. Gli allegati provenienti da mittenti sconosciuti non devono essere aperti in quanto possono essere utilizzati come veicolo per introdurre programmi dannosi (es. virus).
- accertarsi dell'identità del mittente e controllare a mezzo di software antivirus i file attachment di posta elettronica prima del loro utilizzo;
- rispondere ad e-mail pervenute solo da emittenti conosciuti e cancellare preventivamente le altre;
- collegarsi a siti internet contenuti all'interno di messaggi solo quando vi sia comprovata sicurezza sul contenuto degli stessi. L'utente che riceve una e-mail a carattere, violento, razzista o pornografico, o che rappresenti forme di spamming o phishing ha il dovere di avvertire rapidamente l'Ente affinché siano prese le misure necessarie per fermare il ricevimento di questi messaggi non sollecitati. E' vietato trasmettere e-mail di tipo professionale al proprio indirizzo privato. Non è consentito agli utenti:
- diffondere intenzionalmente e senza autorizzazione il proprio indirizzo e-mail dell' OSIV attraverso la rete internet;
- utilizzare la casella di posta elettronica dell'ente per inviare, ricevere o scaricare allegati contenenti video, brani musicali, etc., salvo che questo non sia funzionale all'attività prestata in favore dell'Ente (es: presentazioni o materiali video). Si ricorda che, salvo l'utilizzo di appositi strumenti di cifratura, i sistemi di posta elettronica non possono garantire la riservatezza delle informazioni trasmesse. Pertanto, si richiede agli utenti di valutare con attenzione l'invio di informazioni classificabili quali "riservate" o aventi comunque carattere "strettamente confidenziale". In caso sia strettamente necessario inviare informazioni riservate è cura dell'utente crittografare le stesse per garantirne maggiore riservatezza. L'Ente proibisce espressamente l'utilizzo dell'account di posta elettronica dell' Ordine per la registrazione a servizi di uso personale e comunque non attinenti all'attività lavorativa (a titolo esemplificativo e non esaustivo operazioni di remote banking, acquisti on-line, ecc). Occorre inoltre che i messaggi di posta elettronica contengano un avvertimento ai destinatari, nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi e precisato che le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente. In ogni caso è fatto divieto all'Utente di collegarsi, anche attraverso servizi webmail, al proprio account di posta elettronica dell'ordine mediante telefono cellulare/smartphone personali.

NB: Nei casi in cui l'Ente si doti di posta elettronica certificata si applicheranno, ove compatibili, le presenti disposizioni.

Accesso alla casella di posta elettronica del lavoratore assente

Saranno messe a disposizione di ciascun Utente, con modalità di agevole esecuzione, apposite funzionalità del sistema di posta elettronica che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le coordinate di altro soggetto cui trasmettere le comunicazioni e-mail di contenuto lavorativo o altre utili modalità di contatto in caso di assenza del lavoratore. In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi webmail), l'Ente, perdurando l'assenza oltre un determinato limite temporale pari a 60 giorni, disporrà lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l'amministratore di sistema oppure, se presente, un incaricato dell'Ente per la protezione dei dati DPO), l'attivazione di un analogo accorgimento (risposta automatica o re-indirizzamento),

avvertendo l'assente. Nel caso, invece, l'Ente necessiti conoscere il contenuto dei messaggi di posta elettronica dell'Utente resosi assente per cause improvvise o per improrogabili necessità legate all'attività lavorativa, si procederà come segue:
- la verifica del contenuto dei messaggi sarà effettuata per il tramite di idoneo "fiduciario", da intendersi quale lavoratore previamente nominato e/o incaricato (per iscritto) dall'Utente assente;
- di tale attività sarà redatto apposito verbale e informato l'Utente interessato prima di effettuarne accesso.
- sarà preventivamente richiesto all'utente di farlo lui stesso, se possibile, tramite web mail.

Cessazione dell'indirizzo di posta elettronica dell'Ente

In caso di interruzione del rapporto con l'Utente, l'indirizzo di posta elettronica verrà disabilitato a partire dal giorno successivo di cessazione previa comunicazione da parte dell'Ente; entro 1 mese, invece, si disporrà la definitiva e totale cancellazione dello stesso. In ogni caso, l'Ente si riserva il diritto di conservare i messaggi di posta elettronica che riterrà rilevanti. I Sistemi informatici dell'Ente registrano la posta inviata e ricevuta dagli utenti su supporto digitale per l'archiviazione . Al fine di conservare le proprie e-mail, preservandole dalla cancellazione, l'Utente potrà gestire un archivio sul proprio computer in locale sotto la responsabilità del proprietario delle e-mail stesse. Tale registrazione è conservata in osservanza delle norme civilistiche e fiscali ex art. 2220 cod. civ. e dell'art. 22 del D.P.R. n. 600 del 29/9/73 e comunque fino al termine di eventuali accertamenti fiscali o di accertamenti comunque disposti dall'autorità giudiziaria.

CAPO V – DISPOSIZIONI FINALI

18. I CONTROLLI

I principi

L'Ente, in linea con quanto prescritto dall'ordinamento giuridico italiano (art. 4, Statuto dei Lavoratori), esclude la configurabilità di forme di controllo da parte dell'Ente aventi direttamente ad oggetto l'attività lavorativa dell'Utente. Ciononostante, non si esclude che, per ragioni organizzative e produttive, di tutela del patrimonio dell'Ordine ovvero per esigenze dettate dalla sicurezza del lavoro, si utilizzino sistemi informatici, impianti, apparecchiature o dispositivi dai quali derivi la possibilità di controllo a distanza dell'attività degli utenti. In tal caso tali strumenti verranno valutati e subordinati rispetto alla normativa di settore, ed i dati acquisiti con lo strumento verranno trattati secondo l'informativa privacy allegata al presente disciplinare. Fermo restando il diritto dell'Ente di effettuare controlli sull'effettivo adempimento della prestazione lavorativa nonché sul corretto utilizzo dei beni e servizi informatici dell'Ente (artt. 2086, 2087 e 2104 c.c.), i controlli posti in essere, saranno sempre tali da evitare ingiustificate interferenze con i diritti e le libertà fondamentali degli utenti e non saranno costanti, prolungati e indiscriminati, nel rispetto del principio di pertinenza e non eccedenza. L'Ente, nel riservarsi il diritto di procedere a tali controlli, informa che le modalità di effettuazione degli stessi sono ispirate al principio della "gradualità" così come di seguito più precisamente specificato. Modalità di effettuazione dei controlli I controlli consentono all'Ente di intervenire con verifiche qualora si riscontrino anomalie d'area o di unità, senza arrivare al dettaglio del soggetto singolo, almeno in una prima fase. Secondo il principio della gradualità: - i controlli saranno effettuati inizialmente solo su dati aggregati riferiti all'intera struttura organizzativa ovvero a singole aree lavorative, aventi caratteristiche tali da precludere l'immediata identificazione dell'utente. - nel caso in cui si dovessero riscontrare violazioni del presente disciplinare interno, indizi di commissione di gravi abusi o illeciti o attività contrarie ai doveri di fedeltà e diligenza, verrà diffuso un avviso generalizzato, o circoscritto all'area o struttura lavorativa interessata, relativo all'uso anomalo degli strumenti informatici dell'Ente, con

conseguente invito ad attenersi scrupolosamente alle istruzioni ivi impartite. - in caso siano rilevate ulteriori violazioni, si potrà procedere con verifiche più specifiche e puntuali, anche su base individuale. In ogni caso l'Ente non può in alcun caso utilizzare sistemi da cui derivino forme di controllo a distanza dell'attività lavorativa che permettano di ricostruire l'attività del lavoratore. Per tali s'intendono, a titolo meramente esemplificativo e non esaustivo:
- la lettura e la registrazione sistematica dei messaggi di posta elettronica, al di là di quanto necessario per fornire e gestire il servizio di posta elettronica stesso;
- la riproduzione e la memorizzazione sistematica delle pagine internet visualizzate da ciascun Utente, dei contenuti ivi presenti, e del tempo di permanenza sulle stesse;
- la lettura e la registrazione dei caratteri inseriti dal lavoratore tramite tastiera o dispositivi analoghi;
- l'analisi occulta di computer portatili affidati in uso.