Camera di Commercio
Vicenza

Istruzioni operative per l'utilizzo delle attrezzature informatiche e sistemi di comunicazione

PRINCIPI

1. Oggetto

Le presenti istruzioni hanno per oggetto la definizione di criteri e modalità operative di utilizzo della strumentazione da parte degli utenti assegnatari (dipendenti, lavoratori somministrati, collaboratori, tirocinanti, stagisti ecc.) al fine di tutelare i beni aziendali ed evitare condotte inconsapevoli o scorrette che potrebbero esporre la Camera di commercio di Vicenza a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi.

2. Definizione

Nel presente documento si intende per:
UTENTE: a titolo esemplificativo e non esaustivo, ogni dipendente, collaboratore, consulente, fornitore o altro che in modo continuativo non occasionale operi all'interno della struttura aziendale utilizzandone beni e servizi informatici;
ENTE: La Camera di commercio di Vicenza titolare dei beni e delle risorse informatiche qui disciplinate;

3. Titolarità dei beni e delle risorse informatiche

I beni e le risorse informatiche, i servizi ICT e le reti informative costituiscono beni aziendali rientranti nel patrimonio dell'ente e sono da considerarsi di sua esclusiva proprietà.

Ciò considerato, il loro utilizzo è consentito solo per finalità di adempimento delle mansioni lavorative affidate a ciascun utente in base al rapporto in essere, ovvero per gli scopi professionali afferenti l'attività svolta per l'ente, e comunque per l'esclusivo perseguimento degli obiettivi aziendali.

A tal fine si precisa sin d'ora che qualsivoglia dato o informazione trattato per mezzo dei beni e delle risorse informatiche di proprietà dell'ente sarà dallo stesso considerato come avente natura aziendale e non riservata.

Qualora per lo svolgimento delle attività aziendali si utilizzino dispositivi personali questi una volta connessi alla rete informatica aziendale sono comunque soggetti (ove ciò sia compatibile) alle presenti istruzioni operative.

4. Assegnazione e Custodia delle attrezzature informatiche

Ogni utente è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidatigli dall'ente nonché dei relativi dati aziendali trattati per le finalità dello stesso.
A tal fine ogni utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con l'ente e per quanto di propria competenza, è tenuto a tutelare il patrimonio aziendale da utilizzi impropri o non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia. L'obiettivo è e rimane sempre quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse aziendali.
Ogni utente è tenuto a operare a tutela della sicurezza informatica aziendale, in relazione al al proprio ruolo e alle mansioni in concreto svolte, riportando al proprio responsabile organizzativo diretto, all'Automazione e senza ritardo eventuali rischi di cui è a conoscenza ovvero violazioni delle presenti istruzioni.

In caso di furto o smarrimento dei beni dell'ente affidati individualmente all'utente è obbligatorio che questi effettui tempestivamente denuncia presso l'ufficio di pubblica sicurezza locale, comunicando l'accaduto alla Direzione e consegnando copia della denuncia in Azienda.

Qualora tali eventi siano riconducibili a un comportamento negligente o imprudente dell'utente stesso o comunque a sua colpa nella custodia del bene, lo stesso potrà essere ritenuto unico responsabile dei danni derivanti dall'evento.

5. Monitoraggio e controlli

Il Segretario Generale dispone l'esecuzione di controlli anonimi sull'utilizzo degli strumenti informatici aziendali quando sono rilevate anomalie nel loro funzionamento. Esaurito il controllo, il Segretario Generale ne comunica il risultato a tutti i dipendenti e raccomanda loro di osservare scrupolosamente le disposizioni contenute nelle presenti istruzioni.
Le attività relative all'uso del servizio di accesso a Internet sono automaticamente registrate in forma elettronica attraverso i LOG di sistema nel rispetto delle disposizioni di legge in materia di tutela della privacy e perciò prive di elementi informativi che consentono di tracciare la navigazione degli utenti; fa eccezione l'archiviazione del **Log integrale** di navigazione, fatta dall'Internet Provider, all'unico scopo di rispondere a richieste dell'autorità giudiziaria.
I dati contenuti nei LOG di sistema sono trattati esclusivamente in forma anonima, in modo tale da precludere l'identificazione degli utenti e/o delle loro attività. I dati anonimi aggregati, riferibili all'intera struttura o a sue aree, sono a disposizione del Segretario Generale per le valutazioni di competenza e riguardano, per ciascun sito/dominio visitato: il numero di utenti che lo visitano, il numero delle relative pagine richieste e della quantità di dati scaricati.
I dati personali contenuti nei LOG di navigazione sono trattati in via eccezionale e tassativamente dall'Internet Provider per rispondere a eventuali richieste dell'autorità giudiziaria.

ORGANIZZAZIONE

6. Amministratori di sistema

L'ente conferisce all'amministratore di sistema, appartenente alla UO. Provveditorato e gestione sedi, sezione Automazione, il compito di sovrintendere ai beni e alle risorse informatiche aziendali.
È compito dell'amministratore di sistema:

- Gestire i rapporti con i fornitori esterni, anche in house, di servizi informatici;
- Gestire l'hardware e il software di tutta la strumentazione informatica di appartenenza dell'ente;
- 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;
- Monitorare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi affidati agli utenti, purché rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
- Creare, modificare, rimuovere account;
- Rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
- 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 a un utente in caso di prolungata assenza, non rintracciabilità o impedimento dello stesso (in esempio documenti contenuti nelle cartelle di rete ovvero nei profili personali dei PC fisici o di memorie fisiche).

Tale ultima attività, tuttavia, deve essere disposta per mezzo di un soggetto che rivesta quantomeno la posizione di soggetto autorizzato al trattamento dei dati personali (o designato) all'interno dell'ente e deve essere limitata altresì al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.

7. Assegnazione degli account e gestione delle password

7.1 Creazione e Gestione degli Account

Un account utente consente l'autenticazione dell'utilizzatore e di conseguenza ne disciplina l'accesso alle risorse informatiche aziendali nonché ai dati trattati per finalità aziendali.

Gli account utenti vengono creati dagli amministratori di sistema e sono personali, cioè associati univocamente alla persona assegnataria.

Ogni utente è responsabile dell'utilizzo del proprio account utente.

L'accesso al proprio account avviene tramite l'utilizzo delle "credenziali di autenticazione", solitamente username e password, comunicate all'utente dall'amministratore di sistema che le genera con modalità tali da garantire la segretezza.

Le credenziali di autenticazione costituiscono dati aziendali da mantenere strettamente riservati e non è consentito comunicarne gli estremi a terzi, anche a soggetti in posizione apicale all'interno dell'ente.
Parimenti non possono essere utilizzate le credenziali appartenenti ad altri utenti, nemmeno se sono state comunicate da questi ultimi.
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, è tenuto a modificare immediatamente la password e a segnalare la violazione all'amministratore del sistema nonché al responsabile privacy di riferimento.

In caso di assenza improvvisa o prolungata del lavoratore e per improrogabili necessità legate all'attività lavorativa, per le esigenze produttive aziendali o per la sicurezza e operatività delle risorse informatiche, l'ente ha facoltà di accedere a qualsiasi dotazione o apparato assegnato in uso all'utente per mezzo dell'intervento dell'amministratore di sistema.

L'utente è consapevole che la conoscenza delle credenziali da parte di terzi consente loro l'accesso alla rete aziendale, la fruizione dei relativi servizi in nome dell'utente titolare e l'accesso ai dati cui il medesimo è abilitato (con eventuali conseguenze quali, per esempio, la visualizzazione di informazioni riservate, la distruzione o la modifica dei dati, la lettura della posta elettronica e dei file in cloud, l'uso di servizi, ecc.), pertanto l'utente è impegnato a rispettare quanto qui previsto.

L'utente risponde civilmente, oltre che per i propri fatti illeciti, anche di quelli commessi da chiunque imputi il suo codice identificativo e/o password, con riferimento all'immissione in rete di contenuti critici o idonei a offendere l'ordine pubblico o il buon costume.

La violazione delle disposizioni contenute nel presente documento comporta l'applicazione delle sanzioni disciplinari stabilite dal vigente contratto collettivo nazionale di lavoro, ferma restando ogni altra responsabilità, civile e penale.

7.2 Gestione e Utilizzo delle Password

A seguito della prima comunicazione delle credenziali di autenticazione da parte dell'amministratore di sistema, l'utente ha il compito di modificare al primo utilizzo la propria password procedendo allo stesso modo ogni 6 mesi.

Le regole standard nella definizione del valore delle password sono:

- Lunghezza minima della stringa di 8 caratteri, ricordando che più è lunga la stringa e maggiore è la sicurezza della password;
- Presenza di lettere minuscole (a-z);

- Presenza di lettere maiuscole (A-Z);
- Presenza di numeri arabi (0-9);
- presenza Caratteri non alfanumerici (ad esempio !, ?, #, *);
- Evitare di includere parti del nome, cognome o comunque elementi a lui agevolmente riconducibili;
- Evitare l'utilizzo di password comuni o prevedibili;
- Proteggere con la massima cura la riservatezza della password ed utilizzarla entro i limiti di autorizzazione concessi;
- non annotare password su post it o altri supporti.

Scrivere la password su post-it o altri supporti non è conforme alla normativa, compromette in maniera pressoché totale le misure di sicurezza previste, costituisce violazione delle presenti istruzioni operative e comporta l'applicazione di sanzioni.

7.3 Cessazione degli Account

In caso di interruzione del rapporto di lavoro con l'utente, fine servizio o per gravi violazioni degli obblighi contenuti nel presente documento, le credenziali di autenticazione verranno disabilitate e l'account utente cancellato.

8. Postazioni di lavoro

Per postazione di lavoro si intende il complesso unitario di personal computer (di seguito pc), notebook, tablet, smartphone, PC virtuale (VDI), accessori, periferiche e ogni altro dispositivo informatico (device) concesso in utilizzo all'utente. L'assegnatario di tali beni e strumenti informatici aziendali ha il compito di farne un uso compatibile con i principi di diligenza sanciti nel codice civile.

Al fine di indicare un corretto utilizzo di tali beni l'ente ha adottato le seguenti regole tecniche:

• Ogni pc, fisico e virtuale, notebook (accessori e periferiche incluse), tablet, smartphone o altro dispositivo (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 esclusivamente con hardware e software autorizzati dall'ente. Per utilizzare software o applicativi non presenti nella dotazione standard fornita è necessario presentare espressa richiesta scritta.

• 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 effettuare il log-out dalla sessione o bloccare tastiera e schermo con un programma salvaschermo (screensaver) protetto da password, in modo da non consentire l'uso della propria stazione a persone non autorizzate.

• L'utente deve segnalare con la massima tempestività all'amministratore di sistema o al proprio responsabile di riferimento eventuali guasti e problematiche tecniche rilevati o il cattivo funzionamento delle apparecchiature.
• È fatto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici aziendali a soggetti terzi, salvo i casi previsti per l'erogazione di servizi agli sportelli.
• L'ente si riserva la facoltà di rimuovere d'ufficio e senza alcun preavviso qualsiasi elemento hardware o software la cui installazione non sia stata appositamente e preventivamente prevista o autorizzata.

Gli apparecchi di proprietà personale dell'utente quali computer portatili, telefoni cellulari, smartphone, agende palmari, hard disk esterni, penne USB, lettori musicali o di altro tipo, fotocamere digitali e qualsiasi altro dispositivo non potranno essere collegati ai computer o alle reti informatiche aziendali salvo preventiva autorizzazione scritta dell'ente.

MODALITÀ DI UTILIZZO DELLA STRUMENTAZIONE

9. Dispositivi informatici di proprietà dell'ente (devices): Desktop, Laptop, Tablet, Smartphone, PC virtuali etc.

Per l'espletamento delle proprie mansioni gli utenti utilizzano dispositivi (devices) di proprietà dell'ente e sono tenuti al rispetto delle seguenti regole:

• Non è consentito modificare la configurazione hardware e software del dispositivo assegnato (device), se non previa esplicita autorizzazione dell'ente che la esegue per mezzo dell'amministratore del sistema;
• Non è consentito rimuovere, danneggiare o asportare componenti hardware;
• Non è consentito installare autonomamente programmi informatici, applicativi e ogni altro software non autorizzato espressamente dall'ente;
• È onere dell'utente, in relazione alle sue competenze lavorative, 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;
• È onere dell'utente spegnere il PC utilizzato al termine del lavoro. Per quanto concerne la gestione dei computer e degli altri dispositivi portatili, l'utente ha l'obbligo di custodirli con diligenza e in luogo protetto durante gli spostamenti;
• non è consentito salvare file audio, video e file non istituzionali di qualsiasi tipo nella memoria locale del computer o di altri dispositivi portatili, nel cloud e nelle cartelle di rete su cui è eseguito giornalmente il back-up.

10. Utilizzo di pc di proprietà dell'utente per l'attività lavorativa

Se l'utente, previo accordo con l'ente o da questi autorizzato, utilizza un pc di proprietà per l'attività lavorativa, questo dispositivo dovrà rispettare tutte le regole di sicurezza dei pc camerali.

In particolare l'utente per tale specifico dispositivo dovrà attenersi scrupolosamente anche a quanto segue:

- Utilizzare unicamente terminali dotati di **sistema operativo** e di **antivirus costantemente aggiornati.**
- Verificare che il terminale contenga unicamente **software licenziato e aggiornato**, in caso contrario procedere con la rimozione di tutto il software privo di licenza o obsoleto prima di accedere alle risorse camerali.
- Per l'esecuzione delle attività lavorative **non utilizzare profili utente condivisi con terzi**. **L'utenza lavorativa dovrà essere separata da quella ad uso domestico** e dovrà prevedere un accesso separato con username e password a conoscenza esclusiva dell'utente.

11. Indicazioni operative e sicurezza dati

L'accesso ai pc fisici camerali e ai pc virtuali avviene mediante le credenziali di dominio fornite al dipendente secondo la procedura prevista di Assegnazione degli account (parag. 7).

L'attività lavorativa del dipendente di regola è svolta, garantendo la migliore sicurezza nella gestione dei dati aziendali, su PC virtuale attivabile su qualunque PC fisico installato negli uffici camerali.

Il PC fisico è utilizzato limitatamente nei casi previsti dall'Automazione (in esempio: webinar, video riunioni, utilizzo del Voip Virtuale, scansioni) o per comprovate esigenze operative (rallentamento o malfunzionamento della VDI, utilizzo di software non presenti nel pc virtuale).
Qualora si utilizzi il PC fisico nessun documento deve essere memorizzato su esso (in caso si procede alla sua cancellazione al termine della sessione lavorativa). L'Automazione non esegue backup e/o ripristino di dati da partizioni fisiche di memoria del pc fisico.

Parimenti nessun documento deve essere memorizzato nello spazio locale del PC virtuale (desktop, file system) onde evitare l'appesantimento della macchina virtuale con conseguente rallentamento della esecuzione delle attività e potenziale perdita di dati.

I dati vanno salvati sempre nel cloud (drive e cartelle di rete).

Per accedere alle applicazioni camerali da una postazione di lavoro (fisica o virtuale) l'utente imputa le proprie credenziali di accesso. Superato il sistema di autenticazione, l'utente è collegato alla rete camerale e a Internet, anche allorquando presta l'attività lavorativa a distanza (lavoro agile/telelavoro domiciliare).

12. 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 per installare o comunque utilizzare qualsiasi programma o software dotato di licenza non proprietaria, ad esempio freeware o shareware.

Il personale deve prestare attenzione ad alcuni aspetti fondamentali che ciascun utente è tenuto a osservare per un corretto utilizzo del software in azienda:
• Le licenze d'uso del software sono acquistate da vari fornitori esterni. L'utente è pertanto soggetto a limitazioni nell'utilizzo di tali programmi e della relativa documentazione; non ha il diritto di riprodurre programmi e documentazione in deroga ai diritti concessigli. Tutti gli utenti sono quindi tenuti a utilizzare il software entro i limiti specificati nei rispettivi contratti di licenza.
• Non è consentito eseguire il download o l'upload di software non autorizzato.
• Considerato quanto disposto dalle normative a tutela della proprietà intellettuale e del diritto d'autore, le persone coinvolte nella riproduzione illegale del software sono responsabili sia civilmente che penalmente e quindi soggette alle sanzioni previste dalla legge che comprendono il risarcimento del danno, il pagamento di multe e anche la reclusione.

13. Dispositivi di memoria portatili

Per dispositivi di memoria portatili si intendono tutti quei dispositivi che consentono di copiare o archiviare dati, files, o documenti esternamente al computer: cd-rom, dvd, pen-drive USB, riproduttori musicali mp3, fotocamere digitali, dischi rigidi esterni, ecc.
L'utilizzo di tali supporti risponde alle regole di seguito riportate:
• non è consentito utilizzare supporti rimovibili personali, se non preventivamente autorizzati per iscritto dall'ente;
• è onere dell'utente custodire i supporti contenenti dati (art. 9-10 GDPR) in armadi chiusi a chiave, onde evitare che il loro contenuto possa essere trafugato o alterato o distrutto.

14. Strumenti di fonia mobile o di connettività in mobilità

A seconda del ruolo o della funzione del singolo utente, l'ente rende disponibili e dispositivi quali smartphone e tablet che consentono di usufruire sia della navigazione in internet tramite rete dati che del servizio di telefonia tramite rete mobile.
Le specifiche relative ai limiti entro cui l'utente potrà utilizzare tali strumenti sono riportate nella scheda tecnica di assegnazione consegnata unitamente al dispositivo. L'utente dovrà

attenersi ai limiti previsti in detta scheda e in caso contrario potrà essere richiesto il rimborso dei costi sostenuti per il loro superamento.
Come per qualsiasi altra dotazione aziendale, il dispositivo mobile rappresenta un bene aziendale concesso in uso per scopi esclusivamente lavorativi e pertanto è soggetto alle medesime regole di sicurezza dei dati e degli strumenti informatici in dotazione.
È permesso un utilizzo personale dello strumento qualora è attivo un profilo proprio di traffico dati e telefonia (dual billing).
Al fine di controllo del corretto utilizzo dei servizi di fonia aziendale l'ente può esercitare i diritti di cui all'art. 124 D. Lgs. 196/2003 (fatturazione dettagliata) richiedendo ai provider di telefonia i dettagli necessari agli accertamenti sull'uso e relativo costo del traffico effettuato nel tempo.

Se l'utente utilizza un dispositivo mobile personale deve attenersi alle medesime regole per i dispositivi aziendali.

L'utilizzo dei dispositivi mobili risponde alle seguenti regole:
• l'utente assegnatario del dispositivo aziendale è responsabile dell'uso appropriato dello stesso, e conseguentemente, anche della sua diligente conservazione;
• I dispositivi, sia di proprietà dell'Ente e sia personali, devono essere protetti adeguatamente con **sistemi di sicurezza (esempio: codice PIN) che ne impediscano sia l'accensione che l'utilizzo da parte di altri soggetti**.

In caso di furto o smarrimento dei dispositivi mobili, l'utente **dovrà tempestivamente disattivare da remoto il collegamento degli account camerali** (ad esempio account Google) e **provvedere al cambio password degli stessi**.

Dovrà altresì effettuare tempestivamente denuncia presso l'ufficio di pubblica sicurezza locale, comunicare l'accaduto alla Direzione e consegnare copia della denuncia in Azienda.

MODALITÀ DI UTILIZZO DEI SERVIZI TELEMATICI

15. Utilizzo della rete internet aziendale

Ciascun utente è chiamato ad un uso attento e consapevole della navigazione internet e dei servizi collegati, in quanto ogni operazione posta in essere è associata all'"Indirizzo Internet Pubblico" assegnato all'ente.

La connessione Internet, in quanto bene aziendale a disposizione degli utenti per uso professionale, deve essere utilizzata in maniera appropriata, tenendo presente che ogni sito web può essere governato da leggi diverse da quelle vigenti in Italia; ciò deve essere tenuto in considerazione in modo da prendere ogni precauzione conseguente.

La navigazione internet è pertanto utilizzabile esclusivamente per lo svolgimento delle attività dell'ente.

E’ proibita la navigazione in internet per motivi diversi da quelli strettamenti legati all’attività lavorativa ed in tal senso, a titolo puramente esemplificativo, l’utente non può utilizzare internet per:

- navigare in siti non attinenti allo svolgimento delle proprie mansioni lavorative;
- registrarsi a siti i cui contenuti non siano legati all’attività lavorativa;
- partecipare se non per motivi professionali a forum, chat line, bacheche elettroniche e le registrazioni in guest-book, anche utilizzando pseudonimi (o nicknames);
- utilizzare per scopi personali sistemi Peer to Peer (P2P), di file sharing, podcasting, webcasting o similari per lo scambio o la condivisione di materiale audiovisivo, cinematografico, fotografico, informatico o altro anche se non protetto da copyright;
- scaricare software dalla rete senza l'autorizzazione dell'Ufficio Automazione;
- 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 preventivamente ed espressamente approvata;

Al fine di evitare la navigazione in siti non pertinenti all’attività lavorativa l’ente per il tramite del proprio internet provider adotta sistemi di blocco o filtro automatico che prevengano determinate operazioni di upload o l’accesso a determinati siti inserite a monte in una black list.

E' tuttavia consentito ai dipendenti di poter accedere, attraverso la rete internet aziendale, per finalità personali a siti di informazione (Giornali e quotidiani) e/o di altro genere (es. siti prenotazione treni/aerei/home banking) purché fuori dall’orario di servizio (pausa pranzo) o, previamente autorizzati dal superiore gerarchico, per un periodo di tempo assai limitato e solo per eventuali necessità ed urgenze. Tale navigazione per finalità personali deve essere comunque improntata a criteri di buona fede e correttezza e non può in alcun caso pregiudicare il disbrigo assiduo e diligente delle mansioni assegnate.

16. Regole operative all’esterno dell’ambiente camerale

Di seguito sono riportate le regole per operare in modo efficiente e sicuro quando ci si trova all’esterno dell’ambiente camerale. Queste indicazioni sono da considerare aggiuntive a tutto quello riportato ai punti precedenti del presente documento.

Per la **connettività internet** fuori dalla rete camerale, l’utente è impegnato a:
a) Utilizzare unicamente connettività fornita dal proprio fornitore di servizi contrattualizzati (ISP);
b) verificare che la propria rete domestica sia adeguatamente protetta con cifratura, in caso di wi-fi, almeno wpa2 e password di almeno 8 caratteri alfanumerici, applicando le regole standard di valorizzazione delle password (vedi art. 7.2) ;
c) in caso di utilizzo di una rete LAN, verificare che i cavi siano direttamente collegati al proprio modem/switch;
d) per le connessioni internet esterne alla rete domestica, **non utilizzare wi-fi pubblici e, soprattutto, “reti aperte” e/o sconosciute**.

17. Gestione e Utilizzo della posta elettronica aziendale

17.1 Principi guida

Per ciascun utente titolare di un account, l'ente provvede ad assegnare una casella di posta elettronica individuale.
I servizi di posta elettronica devono essere utilizzati a scopo professionale: **l'account e-mail** è uno strumento di proprietà dell'ente ed **è conferito in uso per l'esclusivo svolgimento delle mansioni lavorative affidate**.
Attraverso le caselle e-mail aziendali gli utenti rappresentano pubblicamente l'ente e per questo motivo viene richiesto di utilizzare tale sistema in modo lecito, professionale e comunque tale da riflettere positivamente l'immagine aziendale.
Gli utenti sono responsabili del corretto utilizzo delle caselle di posta elettronica aziendale conformemente alle presenti regole.
Gli stessi devono:
• conservare la password nella massima riservatezza e con la massima diligenza;
• mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti;
• prestare attenzione agli allegati provenienti da mittenti sconosciuti, in quanto possono essere utilizzati come veicolo per introdurre programmi dannosi (agenti di alterazione, ad esempio virus, trojan ecc). Accertarsi sempre dell'identità del mittente;
• inviare preferibilmente files in formato PDF;
• rispondere alle e-mail pervenute solo da emittenti conosciuti e cancellare preventivamente le altre;
• collegarsi a siti internet contenuti all'interno di messaggi solo per motivate ragioni e quando vi sia comprovata sicurezza sul contenuto degli stessi.
Inoltre, non è consentito agli utenti:
• diffondere il proprio indirizzo e-mail aziendale attraverso la rete internet;
• utilizzare la casella di posta elettronica aziendale per inviare, ricevere o scaricare allegati contenenti video, brani musicali, ecc., salvo che questo non sia funzionale all'attività prestata in favore dell'ente, per esempio presentazioni o materiali video aziendali;
• utilizzare tecniche di «mail spamming», cioè l'invio massiccio di comunicazioni a liste di distribuzione extra-aziendali o di attivare procedimenti equivalenti;
• allegare al testo delle comunicazioni materiale potenzialmente insicuro (ad es. programmi, scripts, macro), o file di dimensioni eccessive.

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".

Occorre infine 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 da altri nell'organizzazione di appartenenza del mittente.

Nei casi in cui all'utente è assegnata una PEC si applicheranno, ove compatibili, le medesime disposizioni.

17.2 Gestione casella dell'utente assente

In caso di assenze programmate del lavoratore quest'ultimo attiva l'impostazione di avviso di assenza per i corrispondenti con messaggio risposta automatico di non reperibilità, indicando anche utili modalità di contatto degli uffici.

Diverso è il caso di assenze non programmate - ad esempio per malattia - nelle quali il lavoratore non possa attivare la procedura descritta anche avvalendosi di un collegamento remoto.
Perdurando l'assenza oltre il limite temporale di 7 (sette) giorni l'ente disporrà, l'inserimento di una risposta automatica-per il tramite dell'amministratore del sistema di posta elettronica.

17.3 Cessazione dell'indirizzo di posta elettronica

In caso di interruzione del rapporto di lavoro con l'utente, l'indirizzo di posta elettronica verrà disabilitato entro un periodo massimo di 30 (trenta) giorni da quella data ed entro 90 (novanta) giorni si disporrà la definitiva e totale cancellazione dello stesso.
Prima della cessazione del rapporto di lavoro l'utente consegna al proprio responsabile eventuali messaggi di posta inerenti le attività di ufficio.

In ogni caso, l'ente si riserva il diritto di conservare i messaggi di posta elettronica ritenuti rilevanti per le proprie attività.

Il servizio di posta elettronica cessa altresì quando sono accertate gravi violazioni degli obblighi contenuti nel presente documento.

17.4 Pubblicazione di contenuti e realizzazione di siti personali

All'utente camerale non è consentita la produzione e la pubblicazione di siti Internet che non siano autorizzate per ragioni di servizio dal Segretario Generale.

17.5 Interruzione e cessazione d'ufficio del servizio

Il servizio di Internet e di posta elettronica è interrotto dall'Ufficio Automazione per le manutenzioni ordinarie e straordinarie; salvo casi di forza maggiore, le interruzioni sono preventivamente comunicate agli utenti.

SANZIONI E COMUNICAZIONI

18. Sanzioni

La violazione di quanto previsto dal presente documento, rilevante anche ai sensi degli artt. 2104 e 2105 c.c., potrà comportare l'applicazione di sanzioni disciplinari in base a quanto previsto dall'art. 7 (sanzioni disciplinari) della Legge 20 maggio 1970 n.300 (Statuto dei Lavoratori).
Nel caso venga commesso un reato o la cui commissione sia ritenuta probabile o solo sospettata l'ente avrà cura di informare senza ritardo, e senza necessità di preventive contestazioni o addebiti formali, le autorità competenti dell'utilizzo illecito o non conforme dei beni e degli strumenti informatici aziendali.
In caso di violazione accertata delle regole e degli obblighi esposti in questo documento da parte degli utenti l'ente si riserva la facoltà di sospendere, bloccare o limitare gli accessi di un account, quando appare ragionevolmente necessario per proteggere l'integrità, la sicurezza o la funzionalità dei propri beni e strumenti informatici e inoltre per impedire il reitero di tale violazione.

19. Informativa agli utenti ex art. 13 disciplinare (UE) 2016/679

Le presenti istruzioni operative, nella parte in cui contengono le regole per l'utilizzo dei beni e degli strumenti informatici aziendali e relativamente al trattamento di dati personali svolti dall'ente finalizzato all'effettuazione di controlli leciti, così come definiti nel paragrafo 5, valgono quale informativa ex art. 13 del disciplinare (UE) 2016/679.

20. Comunicazioni

Contestualmente all'assegnazione di un account le presenti istruzioni operative sono messe a disposizione degli utenti per la consultazione.
La versione più aggiornata delle stesse è pubblicata in formato digitale sulla intranet digitale e consegnata a mezzo posta elettronica.
Per ogni aggiornamento del presente documento sarà data comunicazione anche tramite l'invio di specifico messaggio e-mail e tutti gli utenti sono tenuti a conformarsi alla versione più aggiornata.
Le richieste di autorizzazione o concessione previste dalle presenti istruzioni possono essere inoltrate all'ente per mezzo di qualsiasi strumento che ne garantisca la tracciabilità, ad esempio tramite e-mail, a cui è riconosciuto il valore di forma scritta in modo del tutto analogo rispetto a quella cartacea