COMUNE DI LEDRO

Provincia di Trento

VERBALE DI DELIBERAZIONE N. 43
della GIUNTA COMUNALE

OGGETTO: Misure minime di sicurezza tecniche ed organizzative e di utilizzo dei dispositivi informatici, internet e posta elettronica. Approvazione disciplinare.

L'anno duemilaventitré, il giorno ventiquattro del mese agosto alle ore 16:40, si è riunita la Giunta comunale.

Sono presenti:

Cognome e Nome	Qualifica	Presente/Assente
Girardi Renato	Sindaco	Assente
Oliari Claudio	ViceSindaco	Presente
Molinari Vania	Assessore	Presente
Sartori Roberto	Assessore	Presente
Trentini Dario	Assessore	Presente
Zendri Luca	Assessore	Presente

Assiste il Segretario generale dottoressa *Lorena Giovanelli*.

Riconosciuto legale il numero degli intervenuti, il signor *Claudio Oliari*, nella sua qualità di vice sindaco, assume la presidenza e invita la Giunta comunale a deliberare in merito all'oggetto suindicato.

LA GIUNTA COMUNALE

Premesso che i dati personali presenti all'interno degli strumenti informatici in dotazione ad amministratori, dipendenti, collaboratori ed a tutti coloro che, a vario titolo, utilizzano il sistema informatico dell'ente (utenti), sono utilizzati per finalità istituzionali, per esigenze organizzative e produttive, per la sicurezza sul lavoro e per la tutela del patrimonio dell'ente;

Ritenuto necessario fornire agli utenti del sistema informatico dell'ente le indicazioni per una corretta e adeguata gestione dei dati personali, trattati in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici dell'ente (pc, tablet, notebook, e-mail ed altri strumenti con relativi software e applicativi, smartphone, eccetera), posta elettronica ed internet che sono messi loro a disposizione per lo svolgimento dell'attività inerente la propria funzione e/o mansione;

Dato atto, in particolare, che le indicazioni per una corretta ed adeguata gestione dei dati personali trattati con strumenti informatici hanno lo scopo di:
- assicurare la funzionalità ed il corretto impiego delle strumentazioni informatiche e telematiche da parte degli utenti, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa;
- prevenire rischi alla sicurezza del sistema;
- responsabilizzare gli utilizzatori sulle conseguenze di un uso improprio delle strumentazioni;
- definire in maniera trasparente le modalità di effettuazione dei controlli e le conseguenze, anche disciplinari, di un utilizzo indebito;
- porre in essere adeguate misure organizzative e tecnologiche volte a prevenire il rischio di utilizzi impropri degli strumenti informatici, della rete informatica e del sistema di telefonia fissa e mobile, nel rispetto dei diritti dei lavoratori e del diritto alla riservatezza;

Esaminato il testo del disciplinare recante "*Misure minime di sicurezza tecniche ed organizzative e di utilizzo dei dispositivi informatici, internet e posta elettronica",* il quale disciplina:

1. Misure di sicurezza fisiche
2. Misure per il trattamento con ausilio di supporti cartacei
3. Misure di sicurezza - strumenti informatici
   - 3.1. Postazioni informatiche
   - 3.2. Credenziali e password
   - 3.3. Banche dati, software, applicazioni e cartelle del server
   - 3.4. Sistema di backup
   - 3.5. Sistema antivirus e antispam
   - 3.6. Sistema firewall
   - 3.7. Server
   - 3.8. Personal computer
   - 3.9. Supporti di memorizzazione
   - 3.10. Fotocopiatrici e scanner
   - 3.11. Misure di sicurezza per altri strumenti elettronici
4. Misure di sicurezza - posta elettronica, internet e sistemi di telefonia
   - 4.1. Posta elettronica
   - 4.2. Internet
   - 4.3. Sistemi di telefonia
5. Strumentazione informatica in smart working/lavoro agile
6. Smaltimento documenti cartacei e dispositivi elettronici
   - 6.1. Smaltimento dei documenti cartacei
   - 6.2. Smaltimento di rifiuti elettrici ed elettronici
7. Interventi di assistenza e manutenzione
8. Monitoraggio e controlli
9. Attuazione del disciplinare e tenuta dell'inventario della strumentazione informatica, dei software e delle applicazioni in dotazione all'ente
   - 9.1. Responsabilità nell'attuazione del presente disciplinare
   - 9.2. Inventario;

Visto il Codice degli enti locali della Regione autonoma Trentino-Alto Adige, approvato con L.R. 03.05.2018 n. 2;

Preso atto dei pareri favorevoli senza osservazioni resi in forma scritta ed inseriti nella presente deliberazione, espressi dai responsabili dei servizi interessati, in ordine alla regolarità tecnico amministrativa e contabile ex articolo 185 del Codice degli enti locali della Regione Trentino-Alto Adige, approvato con L.R. 03/05/2018, n. 2;

Ad unanimità di voti favorevoli espressi in forma palese

DELIBERA

1. Di approvare il disciplinare recante le "Misure minime di sicurezza tecniche ed organizzative e di utilizzo dei dispositivi informatici, internet e posta elettronica", nel testo allegato alla presente deliberazione quale parte integrante e sostanziale.
2. Di abrogare il "Disciplinare interno per l'utilizzo di internet e della posta elettronica da parte dei dipendenti" approvato con determinazione n. 594 dd. 09/11/2011".
3. Di disporre la pubblicazione del disciplinare di cui al precedente punto 1. in Amministrazione-Trasparente/Disposizioni-generali/Atti-generali/Atti-amministrativi-generali.
4. Di dare evidenza, ai sensi dell'articolo 4 della L.P. 30.11.1992 n. 23, che avverso il presente provvedimento è ammessa opposizione alla Giunta Comunale, durante il periodo di pubblicazione, da parte di ogni cittadino ex articolo 183 del Codice degli enti locali della Regione autonoma Trentino-Alto Adige, approvato con L.R. 03.05.2018 n. 2, nonché ricorso straordinario al Presidente della Repubblica entro 120 giorni ex articolo 8 del D.P.R. 24.11.1971 n. 1199 o, in alternativa, ricorso giurisdizionale avanti al T.R.G.A. di Trento entro 60 giorni ex articoli 13 e 29 del D.Lgs. 02.07.2010 n. 104, da parte di chi abbia un interesse concreto ed attuale.

IL VICE SINDACO	IL SEGRETARIO GENERALE
Claudio Oliari	*dottoressa Lorena Giovanelli*
documento firmato digitalmente	*documento firmato digitalmente*

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, predisposto e disponibile presso questa Amministrazione in conformità alle regole tecniche (artt. 3bis e 71 D.Lgs. 82/2005). La firma autografa è sostituita dall'indicazione a stampa del nominativo del responsabile (art. 3 D.Lgs. 39/1993).

Alla presente deliberazione sono uniti:
- pareri rilasciati ai sensi dell'articolo 185 della L.R. 03.05.2018 n. 2 e del Regolamento comunale per la disciplina dei controlli interni;
- certificazione pubblicazione.

COMUNE DI LEDRO

Provincia di Trento

DISCIPLINARE

MISURE MINIME DI SICUREZZA TECNICHE ED ORGANIZZATIVE E DI UTILIZZO DEI DISPOSITIVI INFORMATICI, INTERNET E POSTA ELETTRONICA

Sommario

Premessa

Il presente disciplinare ha l'obiettivo di fornire ad amministratori, dipendenti, collaboratori e a tutti coloro che, a vario titolo, utilizzano il sistema informatico dell'Ente (di seguito "utenti"), le indicazioni per una corretta e adeguata gestione dei dati personali, trattati in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici dell'Ente (PC, tablet, notebook, e-mail ed altri strumenti con relativi software e applicativi, smartphone, …..), posta elettronica ed internet che sono messi a disposizione per le attività lavorative.

I dati personali e le altre informazioni dell'utente presenti all'interno dei suddetti strumenti, o che si possono eventualmente raccogliere tramite il loro uso, sono utilizzati per finalità istituzionali, per esigenze organizzative e produttive, per la sicurezza sul lavoro e per la tutela del patrimonio dell'Ente. Per tutela del patrimonio dell'Ente, si intende la sicurezza fisica, informatica e la tutela del sistema informatico e fisico-organizzativo dell'Ente. Tali informazioni sono utilizzabili anche a fini connessi al rapporto di lavoro, visto che il presente manuale costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dalla normativa europea sulla protezione dei dati personali e dal Codice per la tutela dei dati personali.

Il presente disciplinare ha lo scopo di:
- assicurare la funzionalità ed il corretto impiego delle strumentazioni informatiche e telematiche da parte degli utenti, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa;
- prevenire rischi alla sicurezza del sistema;
- responsabilizzare gli utilizzatori sulle conseguenze di un uso improprio delle strumentazioni;
- definire in maniera trasparente le modalità di effettuazione dei controlli e le conseguenze, anche disciplinari, di un utilizzo indebito;
- porre in essere adeguate misure organizzative e tecnologiche volte a prevenire il rischio di utilizzi impropri degli strumenti informatici, della rete informatica e del sistema di telefonia fissa e mobile, nel rispetto dei diritti dei lavoratori e del diritto alla riservatezza.

Per chiarezza le definizioni di interesse per il presente disciplinare sono contenute nel "Glossario".

1. Misure di sicurezza fisiche

Per l'accesso fisico ai locali i soggetti autorizzati sono dotati di chiave non duplicabile e codice personale di disattivazione dell'allarme. E' vietato l'utilizzo, anche momentaneo, della chiave e del codice da parte di soggetti diversi dall'assegnatario.

2. Misure per il trattamento con ausilio di supporti cartacei

Per tutelare la riservatezza e prevenire furti, copie e/o la distruzione dei dati contenuti nei documenti cartacei, l'Ente applica le seguenti regole:
- i documenti cartacei possono essere consultati esclusivamente dagli utenti autorizzati;
- la consultazione è consentita esclusivamente nei limiti in cui è necessaria per lo svolgimento delle mansioni e dei compiti assegnati;
- la consultazione dei documenti cartacei è consentita per il tempo strettamente necessario allo svolgimento delle mansioni e dei compiti assegnati. Una volta espletati tali mansioni e tali compiti, i documenti devono essere riposti nella posizione dalla quale erano stati prelevati;
- i documenti cartacei non devono essere lasciati incustoditi;
- se l'utente si allontana dalla propria postazione di lavoro, i documenti che riportano dati personali devono essere riposti in modo tale da tutelare la riservatezza dei dati in essi contenuta.

Gli archivi contenenti banche dati cartacei sono custoditi in locali o in elementi di arredo muniti di serratura e chiusi a chiave. Le chiavi sono custodite dal personale autorizzato al trattamento dei dati.
L'accesso alle banche dati cartacee è consentito agli utenti incaricati del trattamento dei dati, individuati in ragione delle mansioni e dei compiti loro assegnati nel Piano Integrato di Amministrazione e Organizzazione, negli atti di nomina dei Responsabili dei Settori e Servizi, nonché negli atti di nomina dei Responsabili dei procedimenti.
L'utente deve attenersi ai profili di autorizzazione assegnati in modo da garantire che il trattamento dei dati personali sia svolto esclusivamente con riferimento ai dati necessari.
Per proteggere gli archivi di documenti cartacei dal rischio di accesso fisico non autorizzato, furto e distruzione, l'accesso da parte di soggetti esterni all'Ente è consentito esclusivamente in presenza di personale dell'Ente.

3. Misure di sicurezza - strumenti informatici

3.1 Postazioni informatiche

Per accedere ai servizi informatici da una postazione di lavoro, l'utente deve utilizzare le proprie credenziali composte da un codice identificativo (id utente) e una parola chiave segreta (password). Superato il sistema di autenticazione, l'utente è collegato alla rete dell'Ente e ad internet.

Le attività di gestione e manutenzione dei personal computer dell'Ente fanno capo all'amministratore di sistema e non è permesso agli utenti di intervenire personalmente sulle apparecchiature informatiche. In particolare:

- l'Ente mette a disposizione degli utenti differenti sistemi di memorizzazione su cui effettuare il salvataggio e la condivisione dei documenti e dei files di lavoro: i dischi di rete, identificati sulle postazioni di lavoro da lettere Z, U, S, P ed il sistema in cloud (drive su Zimbra associato al servizio di posta elettronica), utilizzabile attraverso un browser web. Su queste unità vengono svolte attività di amministrazione e salvataggio periodico (backup). Per il trasferimento dei file interni l'Ente mette a disposizione la cartella di scambio denominata Z:\Scambio; i file dovranno essere tagliati e incollati nella cartella di destinazione in modo da svuotare la cartella di transito;
- tutti i documenti relativi all'attività lavorativa devono essere salvati sui sistemi di memorizzazione in rete definiti al punto precedente, in aree private o condivise. I file salvati su differenti unità di memorizzazione (dischi interni alle postazioni di lavoro, chiavette USB, etc..) non sono recuperabili in caso di guasto dell'unità di memorizzazione e non saranno salvati e/o ricopiati in caso di sostituzione delle postazioni di lavoro;
- nell'utilizzo di programmi, materiali audiovisivi, documenti ed ogni altra informazione protetta a norma di legge, gli utenti devono rispettare diritti d'autore, copyright e licenze d'uso di software;
- non è permesso l'utilizzo e/o la connessione alla propria postazione di lavoro o in rete di sistemi o periferiche hardware private non autorizzate;
- è vietato pubblicare o diffondere, anche tramite social network, notizie e informazioni di cui l'utente sia venuto a conoscenza per ragione di ufficio, fatti salvi i casi in cui lo stesso sia autorizzato dall'Amministrazione;
- non è consentito utilizzare chat interne per farne uso non consono all'attività lavorativa.

3.2 Credenziali e password

Il sistema di autenticazione serve a regolamentare l'accesso agli strumenti informatici utilizzati dagli utenti ed a proteggere gli strumenti ed i dati in essi contenuti da accessi non autorizzati. Le credenziali di autenticazione permettono agli utenti di gestire solo trattamenti di dati a cui sono autorizzati.

Gli utenti autorizzati possono accedere tramite le proprie credenziali di autenticazione, costituite da un nome utente e una password e, in casi specifici, da un ulteriore codice OTP (one time password) rilasciato via SMS, App o e-mail.

Le credenziali di autenticazione sono rilasciate dall'amministratore di sistema o dal fornitore dei servizi informatici. L'amministratore di sistema cura altresì la disattivazione delle utenze per coloro che cessano la propria attività nell'Ente.

Le credenziali di autenticazione sono strettamente personali, non devono essere condivise con altri utenti e ne deve essere garantita la segretezza:

- è vietato l'utilizzo di credenziali di altri utenti, anche se conosciute casualmente o fornite volontariamente da altri colleghi;
- le credenziali di autenticazione sono modificate o disattivate qualora all'utente vengano modificate le competenze e i compiti d'ufficio;
- la password deve essere composta da almeno 8 caratteri che soddisfino almeno tre dei seguenti criteri: almeno un carattere speciale, almeno un numero, almeno un carattere maiuscolo e almeno un carattere minuscolo;
- la password non deve contenere parte/i del ID utente, del nome e/o del cognome;
- la password non deve contenere riferimenti agevolmente riconducibili all'utente;
- la password deve essere modificata dall'utente al primo utilizzo e, successivamente, con cadenza almeno trimestrale. Il sistema di autenticazione (server) deve prevedere che ogni nuova password sia diversa almeno dalle dieci precedenti;
- la password deve essere mantenuta riservata, non deve essere lasciata incustodita o in vista sulla propria postazione di lavoro, non deve essere trascritta su supporti facilmente accessibili a terzi (es. post-it);
- se la password viene salvata in un file dedicato, è importante proteggere il file con password (ad es. file ZIP o RAR protetto da password) o utilizzare un password manager.

Al fine di accrescere ulteriormente la sicurezza, l'utente:

- non deve permettere che, in propria assenza, terzi non autorizzati utilizzino gli strumenti informatici a lui assegnati;
- se si assenta temporaneamente dalla propria postazione deve spegnere o rendere non possibile l'utilizzo dello strumento informatico a lui assegnato (chiudere a chiave la porta dell'ufficio, bloccare il pc o far partire lo screen saver sbloccabile solo con l'introduzione della password);

- sul proprio pc deve impostare l'avvio dello screen saver in automatico dopo l'inutilizzo per breve tempo, ad esempio 10 minuti.

3.3 Banche dati, software, applicazioni e cartelle del server

In applicazione del principio di necessità del trattamento ossia che gli autorizzati sono legittimati ad accedere ai soli dati personali pertinenti e non eccedenti per le mansioni e attività agli stessi affidate, i Settori/Servizi di cui si compone la struttura amministrativa sono autorizzati all'accesso alle banche dati informatiche dell'Ente, ai software, alle applicazioni e alle cartelle del server per le materie di competenza del Settore/Servizio definite nella sezione Organizzazione e capitale umano del Piano Integrato di Amministrazione e Organizzazione. All'interno dei Settori, il responsabile del Servizio Informatica/Amministratore di sistema in collaborazione con il responsabile di Settore, definisce i profili di accesso dei responsabili dei procedimenti alle cartelle del server e alle banche dati informatiche, software e/o applicazioni relative alle materie oggetto dei procedimenti assegnati.

3.4 Sistema di backup

Il sistema informatico dell'Ente è dotato di un sistema automatico di salvataggio dei dati. Il salvataggio viene eseguito a cadenza stabilita e comunque non superiore ad un giorno. Pertanto, gli utenti devono salvare tutti i dati sul server, evitando di mantenerli in locale sui singoli PC (ad es. desktop).

3.5 Sistema antivirus e antispam

Il sistema antivirus previene l'azione di programmi (malware, virus) che hanno l'obbiettivo di rubare un sistema informatico, i dati o i programmi in esso contenuti, nonché danneggiare file o software, anche al fine di interrompere in modo totale o parziale il funzionamento del sistema.

Il sistema antispam serve a prevenire la ricezione di messaggi di posta elettronica indesiderati (messaggi spam). L'Ente provvede a far installare programmi antivirus e antispam che sono mantenuti automaticamente aggiornati dall'amministratore di sistema o da altri fornitori di servizi informatici.

La maggior parte dei virus sono diffusi tramite la posta elettronica e internet, ad esempio tramite tecniche di phishing, malvertising, domain squatting, ecc.

Al fine di minimizzare il rischio di introdurre virus nel sistema informatico dell'Ente gli utenti devono:
- prima di aprire una e-mail, in particolare se non richiesta o nel caso in cui si ritenga quantomeno insolita, verificare il mittente ed eventualmente non aprire allegati o collegarsi a siti internet contenuti nel testo della e-mail;
- anche se l'e-mail proviene da indirizzo istituzionale o noto (ad es. INPS, Agenzia Entrate, Poste, banche …) imitandone l'interfaccia, verificare comunque la veridicità dell'indirizzo e l'autenticità del mittente oltre al contenuto;
- prima di utilizzare supporti esterni, se pur autorizzati (chiavette Usb, Hard disk esterni o CD), di qualsiasi provenienza, procedere con un controllo da parte dell'antivirus.

3.6 Sistema firewall

Il sistema firewall permette di separare la rete informatica dell'Ente e le reti informatiche esterne. Il sistema firewall, controllando il traffico in entrata ed in uscita dalla rete riesce a minimizzare i rischi intrusione e accesso non autorizzato alla rete informatica dell'Ente e quindi agli strumenti informatici e ai dati in essi contenuti. Il firewall è gestito e mantenuto aggiornato da Trentino Digitale. Ogni postazione informatica e server ha il proprio firewall attivo gestito e mantenuto aggiornato centralmente dall'amministratore di sistema.

3.7 Server

I server sono protetti dai rischi di accesso fisico non autorizzato, distruzione o perdita di dati dovuta ad eventi fisici e all'interruzione della fornitura elettrica.

L'Ente assicura le seguenti misure di sicurezza:
- i server sono ospitati in appositi locali/armadi, destinati a contenere unicamente i server stessi ed eventualmente le apparecchiature di rete;
- i locali/armadi in cui sono ospitati i server, se situati in posizioni tali da rendere possibili intrusioni, sono muniti di adeguate protezioni (chiusure sicure, sistemi antintrusione, …);
- gli accessi ai locali/armadi in cui sono ospitati server sono chiusi a chiave. Le chiavi sono custodite dall'amministratore di sistema che le custodisce in sicurezza;
- l'accesso ai locali/armadi in cui sono ospitati i server è consentito solo ad utenti autorizzati;
- è attivo un sistema che monitora costantemente il funzionamento dei dispositivi e degli applicativi collegati alla rete informatica. Il sistema si basa su un apposito dispositivo hardware/software che consente il tempestivo

rilevamento di malfunzionamenti o guasti dei dispositivi e degli applicativi monitorati che in automatico arriva all'amministratore di sistema inviandone appositi log di alert.

Gli utenti che hanno accesso ai locali/armadi in cui sono ospitati i server devono informare l'Ente nel caso in cui riscontrino il mancato rispetto delle misure di sicurezza.

Per prevenire i rischi di incendio, surriscaldamento e anomalia dell'alimentazione elettrica delle apparecchiature elettroniche, sono stabilite le seguenti misure di sicurezza:
- in prossimità dei locali/armadi in cui sono ospitati i server è installato un estintore a CO2 o a polvere o dispositivo antincendio munito di allarme;
- i server sono collocati in locale climatizzato in cui la temperatura è mantenuta tra 17° e i 22° gradi e nell'armadio è installato un sensore che segnala se la temperatura dell'aria supera i 30° celsius;
- le copie di backup sono custodite in luoghi sicuri e diversi da dove sono presenti i server;
- la rete elettrica di alimentazione dei server è collegata a due gruppi di continuità a doppia conversione.

3.8 Personal computer

Per proteggere i dati contenuti nei pc:
- gli utenti devono mantenere la corretta configurazione del pc; è vietato alterarne le componenti hardware e software e installare software non autorizzati;
- è vietato scaricare sul pc file audio, video o di altro tipo non necessari per lo svolgimento delle mansioni e dei compiti assegnati;
- il pc portatile, quando non utilizzato, deve essere custodito in locali o in elementi di arredo muniti di serratura e chiusi a chiave;
- è vietato scaricare sul pc portatile file audio, video o di altro tipo non necessari per lo svolgimento delle mansioni e dei compiti assegnati;
- è vietato connettere il pc portatile a reti diverse dalla rete informatica dell'Ente, se non strettamente necessario per svolgimento delle mansioni e dei compiti assegnati;
- sono attivate le seguenti ulteriori misure di sicurezza: i dischi dei pc portatili sono criptati, il bios è protetto da password, il firewall blocca qualsiasi connessione in ingresso per le reti identificate non attendibili.

3.9 Supporti di memorizzazione

Gli utenti nello svolgimento delle attività a loro assegnate, se autorizzati, possono utilizzare supporti rimovibili (chiavetta Usb - Pendrive Memoria Flash, CD, cassette, ecc….). In tal caso devono rispettare le seguenti regole:
- prima di utilizzare qualsiasi tipo di memoria esterna dev'essere eseguita una scansione manuale dell'antivirus;
- se i supporti rimovibili sono adoperati anche da altri autorizzati, prima della consegna ad altro autorizzato, deve essere eseguita la formattazione del supporto al fine di cancellare tutti i dati presenti e nel caso in cui, per motivi tecnici, non possa essere eseguita la formattazione, il supporto deve essere distrutto;
- i supporti rimovibili, se contengono dati dell'Ente, devono essere conservati in modo sicuro (contenitori chiusi a chiave);
- è inibito dall'amministratore di sistema utilizzare chiavette USB autopartenti/avviabili/bootables;
- per il trasferimento di file è vietato l'uso di chiavette USB non autorizzate e prive di crittografia.

3.10 Fotocopiatrici e scanner

Gli utenti che nello svolgimento delle attività a loro assegnate utilizzano una fotocopiatrice devono seguire le seguenti regole:
- non dimenticare sotto il coperchio della fotocopiatrice o dello scanner il documento da duplicare;
- nel caso di uso di fotocopiatrici centralizzate o multifunzioni di rete dotate di disco rigido autonomo, è necessaria l'autenticazione di manutenzione da parte dell'amministratore di sistema;
- verificare la correttezza dell'esecuzione, la leggibilità del documento od eventuali errori di acquisizione del testo.

3.11 Misure di sicurezza per altri strumenti elettronici

Agli utenti nello svolgimento delle attività possono essere assegnati o utilizzare, se autorizzati, strumenti elettronici quali cellulari, smartphone, fotocamere, videocamere, ecc…..

In tal caso, al fine di minimizzare il rischio furto o perdita di detti strumenti e degli eventuali dati in essi contenuti, devono essere rispettate le seguenti regole:
- gli strumenti devono essere conservati in modo sicuro;
- se lo strumento è predisposto, deve essere inserito il PIN per proteggere i dati memorizzati. Tale PIN può essere condiviso solo con altre persone autorizzate al trattamento dei dati memorizzati o consegnato a responsabile incaricato della gestione degli strumenti;

- se gli strumenti sono utilizzati anche da altri utenti non autorizzati al trattamento dei dati memorizzati, prima della consegna, deve essere eseguita la cancellazione di tutti i dati presenti e nel caso in cui, per motivi tecnici, non possa essere eseguita, il supporto deve essere consegnato al responsabile del Servizio Informatica che valuta l'eventuale distruzione;
- se sono effettuate foto o riprese, le stesse dovranno essere scaricate e memorizzate nel sistema informatico dell'Ente e dovranno essere cancellate dalla memoria dello strumento.

Vale quanto indicato precedentemente sia per il caso di un telefono fornito dall'Ente sia di un dispositivo proprio dell'utente per cui l'Ente fornisce la SIM card.

Nel caso in cui sia utilizzato un dispositivo personale (smartphone/portatile/tablet, ...) per accedere a informazioni lavorative, ad es. utilizzo della posta elettronica, tramite app o direttamente via web, l'utente è tenuto ad aggiornare costantemente sistema operativo ed applicazioni e ad adottare idonee misure di protezione all'accesso (biometria, password, PIN), antivirus con scansioni periodiche.

4. Misure di sicurezza - posta elettronica, internet e sistemi di telefonia

4.1 Posta elettronica

Il servizio di posta elettronica è disponibile per ogni utente in forma centralizzata: l'indirizzo di posta elettronica può essere nominale, individuale o condiviso fra più utenti.

Nell'utilizzo della posta elettronica devono essere adottate le seguenti misure:
- l'assegnazione della casella di posta avviene unicamente per ragioni di servizio;
- le caselle nominali sono da ritenersi personali e accessibili esclusivamente da parte dell'utente proprietario attraverso l'inserimento di una password; la password deve essere mantenuta riservata e non deve essere comunicata;
- è a disposizione di ciascun utente una apposita funzionalità di sistema che consente di inviare automaticamente, in caso di assenze programmate, messaggi di risposta personalizzabili segnalando eventualmente l'indirizzo della persona da contattare;
- è doveroso informare tempestivamente il Referente privacy data breach e l'amministratore di sistema su potenziali rischi o problemi inerenti alla sicurezza informatica della posta elettronica;
- verificare il destinatario del messaggio prima dell'invio e non utilizzare la modalità 'rispondi a tutti' se non realmente e strettamente necessaria;
- nel caso di ricezione e-mail da destinatari sospetti è necessario procedere alla loro immediata eliminazione;
- inserire l'informativa breve per il trattamento dei dati personali e nota di riservatezza in calce all'e-mail;
- per il caso di invio tramite e-mail di dati particolari (ad es. salute, orientamenti politici, razziali, sessuali, religiosi, ecc., dati biometrici, dati giudiziari, ...):
- verificare che l'indirizzo del destinatario sia correttamente digitato;
- l'oggetto del messaggio non deve contenere direttamente categorie particolari di dati.

In ogni caso è tassativamente vietato:
- utilizzare tecniche di "e-mail spamming" cioè di invio massiccio di comunicazioni a liste di distribuzione esterne o di azioni equivalenti;
- utilizzare il servizio di posta elettronica per inoltrare 'catene di S. Antonio', appelli e petizioni (anche se possono sembrare veritieri e socialmente utili), giochi, scherzi, barzellette, messaggi inerenti a virus, ecc.…;
- utilizzare la casella personale per l'iscrizione a dibattiti, forum o mailing-list se non inerenti alla propria attività lavorativa;
- utilizzare il servizio di posta elettronica per trasmettere pubblicità personale o commerciale.

Nel caso di cessazione dell'attività lavorativa dell'utente della casella di posta elettronica, sia nel caso di indirizzo nominale che di funzione (ad es. presidente, sindaco, segretario…), deve esserne bloccato l'accesso dal giorno successivo e il contenuto dev'essere cancellato entro tre mesi dando previamente la possibilità di recuperare le informazioni strettamente personali. Tempi maggiori di conservazione possono essere autorizzati dal Segretario generale per motivi di necessità opportunamente giustificati. Contestualmente, devono essere implementati sistemi automatici volti ad informare i terzi e a fornire indirizzi alternativi.

4.2 Internet

Tutti gli utenti in possesso di credenziali per accedere alla rete interna dell'Ente possono collegarsi alla rete internet il cui utilizzo è consentito unicamente per ragioni di servizio.

L'utente è direttamente responsabile dell'uso di internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.

L'utilizzo imprudente di alcuni servizi della rete internet può essere fonte di particolari minacce alla sicurezza del sistema (ad es. virus informatici) e all'immagine dell'Ente.

L'Ente ha provveduto ad inibire i siti ritenuti non pertinenti all'attività lavorativa o malevoli, adottando una apposita policy di black list.

Nell'utilizzo di internet è vietato:
- lo scarico (upload e/o download) di file e/o programmi software, se non esplicitamente autorizzati;
- la partecipazione a forum non autorizzati, l'utilizzo di chat line, di bacheche elettroniche e la registrazione in guestbook anche utilizzando pseudonimi (o nickname) e, più in generale, qualunque utilizzo di questi servizi internet se non strettamente connessi all'attività lavorativa;
- l'utilizzo del collegamento ad internet per attività in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
- l'utilizzo di sistemi peer to peer (P2P), di file sharing, podcasting, webcasting o similari non pertinenti all'attività lavorativa.

4.3 Sistemi di telefonia

Tutti gli utenti dotati di un telefono fisso connesso alla postazione di lavoro sono collegati alla rete internet tramite VoIP. L'utente è direttamente responsabile dell'uso del telefono, dei soggetti che contatta, delle informazioni che fornisce all'interlocutore. Nell'utilizzo del telefono è necessario qualificarsi all'interlocutore.

5. Strumentazione informatica in smart working/lavoro agile

Al fine di rendere possibile lo svolgimento della prestazione lavorativa il dipendente potrà essere dotato dall'Ente di un personal computer.

Gli strumenti di lavoro affidati al dipendente devono essere usati esclusivamente per lo svolgimento dell'attività lavorativa, nel rispetto di quanto previsto dalle direttive dell'Ente e non per scopi personali o non connessi all'attività lavorativa.

Il dipendente ha l'obbligo di utilizzare e custodire gli strumenti di lavoro affidatigli con la massima cura e diligenza e di scegliere sempre un luogo che garantisca la riservatezza, ovvero che sia impedita la visualizzazione delle informazioni sullo schermo o l'ascolto delle conversazioni da parte di persone non autorizzate.

In caso di guasto delle attrezzature in dotazione il lavoratore dovrà dare immediato avviso al proprio responsabile, al responsabile del Servizio Informatica e dovrà consegnare lo strumento guastato non appena possibile.

Il dipendente che effettua attività di smart-working/lavoro agile può collegare il pc messo a disposizione dall'Ente alla propria rete WI-FI.

Per l'accesso alla rete dell'Ente è utilizzato un programma installato sul pc (VPN), che garantendo un accesso sicuro ai sistemi informatici dell'Ente, permette al dipendente di svolgere l'attività lavorativa in modalità analoga a quella dell'ufficio.

Nell'accordo individuale di lavoro agile è specificata la possibilità per il dipendente di utilizzare, nel caso in cui non possa disporre di strumentazione fornita dall'Ente, di apparecchiature di proprietà per svolgere attività lavorativa. Nel caso di utilizzo di sistemi di proprietà verrà fornita assistenza solo sulle componenti software che saranno fornite dall'Ente.

L'utilizzo del personal computer di proprietà dell'utente è subordinato alla presenza sul pc di un antivirus attivo aggiornato e di un sistema operativo che riceva i periodici aggiornamenti di sicurezza.

Le disposizioni del presente disciplinare integrano e non sostituiscono la disciplina del lavoro agile contenuta nel Piano Integrato di Organizzazione e Amministrazione, nell'accordo individuale e negli accordi sindacali provinciali sul lavoro agile.

6. Smaltimento documenti cartacei e dispositivi elettronici

6.1 Smaltimento dei documenti cartacei

I documenti cartacei per cui non è più obbligatorio provvedere alla loro conservazione (in base al manuale di scarto dell'Ente), possono essere di due tipi:
- documenti che hanno esaurito la propria utilità giuridico-amministrativa;
- documenti che non possiedono più apprezzabile interesse come fonte storica.

I documenti non più utili, contenenti dati, devono essere distrutti in tutta sicurezza mediante idonea attrezzatura distruggi documenti. La distruzione deve avvenire in modo tempestivo, senza lasciare traccia dei dati in essi contenuti ed eliminando, perciò, il rischio che tali dati possano essere utilizzati in seguito in modo fraudolento.

6.2 Smaltimento di rifiuti elettrici ed elettronici

In caso di smaltimento di rifiuti elettrici ed elettronici, al fine di impedire l'acquisizione indebita di dati personali, deve essere assicurata l'effettiva cancellazione dei dati personali dai supporti contenuti nelle apparecchiature elettriche ed elettroniche

La distruzione dei supporti prevede il ricorso a metodologie diverse a seconda del loro tipo, quali:
- sistemi di punzonatura (ad esempio, utilizzando un perno d'acciaio temprato, che tramite una leva, perfora l'hard disk in una o più zone distruggendolo definitivamente) o deformazione meccanica;
- distruzione fisica o di disintegrazione (usata per i supporti ottici come i CD-ROM e i dvd);
- demagnetizzazione ad alta intensità.

7. Interventi di assistenza e manutenzione

Gli interventi di assistenza, installazione e aggiornamento dei software e, in generale, quelli volti a fronteggiare guasti nel funzionamento delle postazioni di lavoro, qualora possibile, sono effettuati dal responsabile del Servizio Informatica o da tecnici esterni incaricati tramite il servizio di assistenza e amministrazione remota. Il sistema di assistenza in remoto consente, previa autorizzazione del dipendente/utente, di condividere a distanza con l'operatore del supporto tecnico l'utilizzo di tastiera, mouse e schermo, senza che l'utente stesso perda il controllo di quanto avviene al proprio strumento in dotazione e ai dati eventualmente accessibili attraverso lo stesso.

Se invece sono necessari interventi di manutenzione sulla macchina o di assistenza, adeguamento, ecc., presso la postazione di lavoro, è necessario che l'utente o, in sua assenza, altro dipendente del Settore/Servizio o il responsabile del Servizio Informatica, assista alle operazioni di manutenzione.

8. Monitoraggio e controlli

L'Ente ha predisposto il proprio sistema informativo ed internet per esclusive esigenze organizzative e di servizio. A tal fine si avvale legittimamente di sistemi che consentono un monitoraggio continuo di eventi potenzialmente pericolosi sulla rete.

Non saranno utilizzati sistemi hardware e/o software idonei ad effettuare un controllo a distanza dei lavoratori, in particolare mediante:
- la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- la lettura o la registrazione dei caratteri inseriti tramite la tastiera e analogo dispositivo.

Il trattamento dei dati contenuti nei log può avvenire esclusivamente in forma anonima in modo tale da precludere l'identificazione dei lavoratori e/o delle loro attività.

Potrà essere attivato un controllo dei log, non in forma anonima, in via eccezionale e tassativamente, nelle seguenti ipotesi:
1. per corrispondere ad eventuali richieste della polizia postale e/o dell'autorità giudiziaria;
2. su richiesta del datore di lavoro, quando si verifichi un evento dannoso o una situazione di pericolo che richieda un immediato intervento;
3. su richiesta del datore di lavoro, limitatamente al caso di riscontrate anomalie di traffico web, la cui entità sia tale da compromettere la sicurezza e l'integrità dei sistemi informativi.

Nei casi 2 e 3 sopra descritti, i lavoratori sono preventivamente avvisati con indicazione del giorno e dell'orario in cui si svolgerà il controllo. I dati contenuti nei log sono conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, di servizio e di sicurezza, comunque non superiore a 30 giorni, e sono periodicamente cancellati automaticamente dal sistema. Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e avverrà solo in relazione:
- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria e della polizia giudiziaria.

L'Ente, inoltre, per ragioni di necessità e urgenza legate in ogni caso all'espletamento delle funzioni istituzionali, potrà

accedere agli strumenti lavorativi del dipendente, previa opportuna e motivata notifica a quest'ultimo.

In tutti questi casi, il trattamento dei dati personali sarà limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità esplicitati.

9. Attuazione del disciplinare e tenuta dell'inventario della strumentazione informatica, dei software e delle applicazioni in dotazione all'ente

9.1 Responsabilità nell'attuazione del presente disciplinare

Ferma restando la personale responsabilità civile, penale, amministrativa e disciplinare dell'utente che contravviene alle disposizioni contenute nel presente disciplinare, nel codice di comportamento e nei contratti ed accordi individuali di lavoro, al responsabile del Servizio Informatica è assegnato il compito e la responsabilità dell'attuazione delle misure di sicurezza informatica, la vigilanza sul corretto funzionamento del sistema e la vigilanza sul rispetto delle disposizioni destinate agli utenti del sistema informatico dell'Ente.

9. 2 Inventario

Il responsabile del Servizio Informatica è responsabile dell'inventario della strumentazione informatica e dei software autorizzati come descritto nella griglia delle misure minime di sicurezza ai punti ABSC_1 e ABSC_2.

Glossario

Utenti
Amministratori, dipendenti, collaboratori e tutti coloro che, a vario titolo, utilizzano il sistema informatico dell'Ente.
Dato personale
Qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Dati particolari
Dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale della persona, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
Dati giudiziari
Dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.
Trattamento di dati personali
Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Violazione di dati personali (data breach)
Violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
Autorizzato al trattamento
La persona fisica che tratta i dati personali sotto la diretta autorità del titolare e sulla base delle istruzioni dagli stessi impartite. Gli autorizzati si possono suddividere in designati ed incaricati, in base al ruolo rivestito all'interno dell'Ente.
Amministratore di sistema
In ambito informatico, è la figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti.
Strumenti informatici
Strumenti tecnologici utilizzati per la gestione di informazioni e dati, forniti e/o inventariati dall'Ente (es. computer, tablet, supporti di memoria esterni rimovibili, firma digitale remota e token, smartphone, bodycam, dashcam, droni ed altri strumenti con relativi software e applicativi…)
Backup
il termine, che significa copia di sicurezza, indica l'operazione di duplicare su differenti supporti di memoria le informazioni (dati o programmi) presenti sui dischi di una stazione di lavoro o di un server. Normalmente viene svolta con una periodicità stabilita.
Chat
(letteralmente, "chiacchierata") è un servizio informatico che permette attraverso internet, di attivare e gestire un dialogo in tempo reale fra due o più utenti utilizzando principalmente messaggi testuali.
File sharing
condivisione di file all'interno di una rete comune.
Forum
Generalmente si riferisce ad un archivio informatico contenente discussioni e messaggi scritti dagli utenti oppure al software utilizzato per fornire questo archivio. Ci si riferisce comunemente ai forum anche come board, message board, bulletin board, gruppi di discussione, bacheche e simili.
ID utente
Codice identificativo personale per l'accesso ai sistemi informatici. Normalmente è formato dal cognome o dal cognome e parte del nome.
Log
Il termine, che significa giornale di bordo o semplicemente giornale, viene utilizzato nell'informatica per indicare la registrazione cronologica delle operazioni man mano che vengono eseguite ed il file su cui tali registrazioni sono memorizzate.
Mailing-list
(letteralmente, lista per corrispondenza traducibile in italiano con lista di diffusione) è un sistema organizzato per la partecipazione di più persone in una discussione tramite posta elettronica.
Mail spamming
è l'invio di grandi quantità di messaggi indesiderati. Può essere messo in atto attraverso qualunque media, ma il più

usato è internet attraverso l'e-mail.

Password ("parola chiave", "parola d'ordine", o anche "parola d'accesso")

È una sequenza di caratteri utilizzata per accedere ad una risorsa informatica.

Password manager

Programma che archivia in modo sicuro e crittografato le credenziali di accesso a dati o servizi in una sorta di cassaforte virtuale, rendendola disponibile all'utente quando ne avrà bisogno con un'unica password (master password).

Podcasting

Sistema che permette di scaricare in modo automatico documenti (generalmente audio o video) chiamati podcast, utilizzando un programma generalmente gratuito chiamato aggregatore o feeder. Con podcast si intende un file (generalmente audio o video), messo a disposizione su Internet e scaricabile automaticamente.

Software peer to peer

Programmi utilizzati per la condivisione e lo scambio di files fra elaboratori. Questi programmi vengono utilizzati principalmente per scambiarsi file di tipo mp3, (file musicali) e DivX (contenenti i film) spesso in violazione dei diritti d'autore.

Virtual Private Network (VPN)

VPN (Virtual Private Network), Terminal Server o applicativi Web sono tecnologie che permettono di accedere alle risorse della rete locale del Consiglio provinciale attraverso la rete internet.

Voice over IP (VoIP)

Si può parlare di tecnologia VoIP, ovvero voce tramite protocollo internet, quando si effettua una telefonata utilizzando la stessa connessione sia per dati che per voce.

Webcasting

Descrive la trasmissione di segnale audio o video, in tempo reale o ritardato, mediante tecnologie web. Il suono o il video sono catturati con sistemi audio-video convenzionali, quindi digitalizzati e inviati in streaming su un web server. Un client webcast consente agli utenti di connettersi ad un server che sta distribuendo (operazione detta di web casting) e di ascoltare o visualizzare il contenuto audio/video.