# Comunità Alta Valsugana e Bersntol

## Tolgamoa'schòft Hoa Valzegu' ont Bersntol

(Provincia di Trento)

## DECRETO DEL PRESIDENTE N. 75

**OGGETTO:** **Approvazione disciplinare delle misure di sicurezza tecniche e organizzative e di utilizzo dei dispositivi informatici, internet e posta elettronica.**

L'anno **DUEMILAVENTITRE**, addì **QUINDICI** del mese di **MAGGIO**, il Presidente sig. Fontanari Andrea

**EMANA**

il decreto in oggetto.

Assiste il Segretario Generale, dott.ssa MARIUCCIA CEMIN.

OGGETTO: Approvazione disciplinare delle misure di sicurezza tecniche e organizzative e di utilizzo dei dispositivi informatici, internet e posta elettronica.

**IL PRESIDENTE**

L'art. 32 del Regolamento Europeo 679/2016 (GDPR), prevede che il titolare del trattamento, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio, deve adottare le misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Il titolare del trattamento, in virtù del principio di accountability di cui all'art. 5 par. 2 del soprarichiamato GDPR, è quindi tenuto ad adottare tutte le misure e gli strumenti che siano adeguati per il contesto di riferimento e che garantiscano altresì un livello di sicurezza adeguato, considerando che le misure devono essere personalizzate in ragione del proprio specifico contesto.

Con nota assunta al ns. prot. arr. n. 4369 dd. 09.03.2023 il Servizio privacy RPD del Consorzio dei Comuni Trentini, nella sua qualità di Responsabile Protezione Dati (RPD), al fine di fornire uno strumento di riferimento, ha elaborato ed inviato un modello di *"Disciplinare delle misure di sicurezza tecniche e organizzative e di utilizzo dei dispositivi informatici, internet e posta elettronica"*, da integrare/modificare/adattare in ragione della specificità dell'Ente, suggerendo di coinvolgere l'amministratore di sistema nella sua implementazione per verificare che le misure inserite nel disciplinare siano coerenti con il sistema organizzativo e informatico dell'Ente stesso.

Preso atto che tale disciplinare ha l'obbiettivo di fornire ad amministratori, dipendenti, collaboratori e a tutti coloro che, a vario titolo, utilizzano il sistema informatico dell'Ente e/o che si avvalgono degli strumenti e spazi di lavoro, le indicazioni per una corretta e adeguata gestione dei dati personali.

Verificato, in particolare, che il disciplinare ha ad oggetto l'uso di sistemi, applicazioni e strumenti informatici dell'Ente (PC, tablet, notebook ed altri strumenti con relativi software e applicativi, smartphone, … ), e che regolamenta l'utilizzo della posta elettronica e di internet.

Constatato che il disciplinare costituisce altresì strumento per la corretta regolazione del rapporto di lavoro, atteso che tale disciplina costituisce adeguata informazione delle modalità d'uso degli strumenti di lavoro e di effettuazione dei controlli nel rispetto di quanto disposto dal Regolamento Europeo 679/2016 sulla protezione dei dati personali e dal Codice Privacy (d. lgs. 196/2003).

Visto nello specifico il disciplinare allegato al presente provvedimento, predisposto dal Consorzio dei Comuni Trentini nell'ambito del servizio privacy fornito alle amministrazioni comunali ed alle comunità di valle come integrato/modificato/adattato, in ragione della specificità dell'Ente, dall'amministratore di sistema.

Esaminato dunque il disciplinare di cui all'oggetto, nella versione *"implementata"* dall'amministratore di sistema dell'ente.

Preso atto di tutto quanto sopra e ritenuto quindi ora opportuno, sulla scorta di tali premesse normative approvare tale documento, nella qualità di Presidente pro tempore Responsabile del Trattamento dati dell'ente.

Visto il Bilancio di Previsione finanziario 2023-2025, approvato dal Consiglio dei Sindaci con deliberazione n. 10 dd. 27 dicembre 2022.

Vista la Legge Provinciale 16 giugno 2006 n. 3 e ss.mm.

Visto lo Statuto della Comunità Alta Valsugana e Bersntol ed in particolare l'art. 77 in base al quale gli atti regolamentari e di organizzazione del Comprensorio Alta Valsugana si applicano, in quanto compatibili, fino all'entrata in vigore della corrispondente disciplina adottata dalla Comunità.

Visto il Codice degli Enti locali della Regione Autonoma Trentino – Alto Adige approvato con Legge Regionale 3 maggio 2018 n. 2.

Visto il Regolamento di attuazione dell'ordinamento finanziario e contabile degli enti locali, approvato con D.P.G.R. 27 ottobre 1999, n. 8/L.

Visto il Regolamento di Contabilità approvato con deliberazione assembleare n. 40 dd. 16 dicembre 2019.

Visto il Decreto Legislativo 23 giugno 2011, n. 118 e la Legge provinciale 9 dicembre 2015, n. 18.

Ritenuto di dover dichiarare il presente provvedimento immediatamente eseguibile, ai sensi dell'articolo 183 comma 4 del Codice degli enti locali della Regione autonoma Trentino-Alto Adige, approvato con L.R. 3 maggio 2018 n. 2, per consentire la sollecita adozione degli atti/misure gestionali ed organizzativi di competenza conseguenti;

Visto il parere favorevole di regolarità tecnica espresso sul presente provvedimento ai sensi dell'articolo 185 del Codice degli enti locali della Regione autonoma Trentino-Alto Adige, approvato con L.R. 3 maggio 2018, n. 2 e dato atto che non è necessario acquisire il parere di regolarità contabile e l'attestazione della copertura finanziaria, ai sensi dell'articolo 191 del D.Lgs. 18 agosto 2000, n. 267, in quanto il presente decreto non comporta aspetti di natura finanziaria.

Tutto ciò premesso,

**DECRETA**

1. di approvare, per le motivazioni espresse in premessa, il *"Disciplinare delle misure di sicurezza tecniche e organizzative e di utilizzo dei dispositivi informatici, internet e posta elettronica"*, nel testo risultante dall'allegato A) parte integrante e sostanziale del presente provvedimento;

2. di di dare atto che il disciplinare di cui al punto 1. entra in vigore a decorrere dalla data di esecutività del presente decreto di approvazione;

3. di incaricare il Segretario generale, in qualità di designato al trattamento dei dati del Servizio Segreteria Generale, Affari Generali e Organizzazione, il Responsabile del Servizio Programmazione e Diritto allo Studio, in qualità di referente privacy dell'ente ed il Tecnico informatico, in qualità di amministratore di sistema, ad adottare gli atti/misure gestionali ed organizzativi di competenza conseguenti;

4. di inviare copia del disciplinare al personale dipendente dell'ente;

5. di dichiarare il presente decreto immediatamente eseguibile, ai sensi dell'articolo 183 comma 4 del Codice degli enti locali della Regione autonoma Trentino-Alto Adige, approvato con L.R. 3 maggio 2018, n. 2, per le motivazioni espresse in premessa;

6. di disporre, ai sensi dell'art.7, comma 1 della L.R. n. 8/2012, la pubblicazione del presente provvedimento sul sito della Comunità, sezione *"Amministrazione trasparente"* – sottosezione *"Altri contenuti – dati ulteriori"*;

7. di dare evidenza, ai sensi dell'articolo 4 della L.P. 30.11.1992, n. 23, che avverso il presente provvedimento sono ammessi i seguenti ricorsi:
   - opposizione al Presidente della Comunità, entro il periodo di pubblicazione, da parte di ogni cittadino ai sensi dell'articolo 183, comma 5, del Codice degli enti locali della Regione autonoma Trentino-Alto Adige, approvato con L.R. 03.05.2018, n. 2;
   - ricorso giurisdizionale avanti al Tribunale Regionale Giustizia Amministrativa di Trento, entro 60 giorni, ai sensi degli articoli 13 e 29 del D.Lgs. 2 luglio 2010, n. 104;

- ricorso straordinario al Presidente della Repubblica entro 120 giorni ai sensi dell'articolo 8 del D.P.R. 24.11.1971, n. 1199;

richiamando per gli atti delle procedure di affidamento relativi a pubblici lavori, servizi o forniture, ivi comprese le procedure di affidamento di incarichi di progettazione e di attività tecnico-amministrative ad esse connesse, la tutela processuale di cui agli articoli 119 e 120 del D.Lgs. 2 luglio 2010, n. 104, per effetto della quale il ricorso al Tribunale Regionale Giustizia Amministrativa di Trento va proposto entro 30 giorni e non è ammesso il ricorso straordinario al Presidente della Repubblica.

Data lettura del presente decreto, lo stesso viene approvato e sottoscritto.

| IL PRESIDENTE | IL SEGRETARIO GENERALE |
| --- | --- |
| Andrea Fontanari | dott.ssa Mariuccia Cemin |

*Documento prodotto in originale informatico e firmato digitalmente ai sensi degli art. 20 e 21 del "Codice dell'amministrazione digitale" (D.Leg.vo 82/2005).*

# DISCIPLINARE

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

# DELLA

# COMUNITA' ALTA VALSUGANA E BERSNTOL

# Sommario

PREMESSA ..... 3
1. Misure di sicurezza fisiche ..... 3
2. Misure per il trattamento con ausilio di supporti cartacei ..... 4
3. Misure di sicurezza - strumenti informatici ..... 4
3.1 Postazioni informatiche ..... 4
3.2 Credenziali e password ..... 5
3.3 Banche dati, software, applicazioni e cartelle del server ..... 5
3.4 Sistema di backup ..... 6
3.5 Sistema antivirus e antispam ..... 6
3.6 Sistema firewall ..... 6
3.7 Server ..... 6
3.8 Personal Computer ..... 7
3.9 Supporti di memorizzazione ..... 7
3.10 Fotocopiatrici e scanner ..... 7
3.11 Misure di sicurezza per altri strumenti elettronici ..... 7
4. Misure di sicurezza - posta elettronica, internet e videoconferenza ..... 8
4.1 Posta Elettronica ..... 8
4.2 Internet ..... 9
4.3 Sistemi di telefonia ..... 9
4.4 Videoconferenza ..... 9
5. Strumentazione informatica in Smart Working/Lavoro Agile ..... 9
6. Fine vita (documenti cartacei e dispositivi elettronici) ..... 10
6.1 Smaltimento dei documenti cartacei ..... 10
6.2 Smaltimento di rifiuti elettrici ed elettronici ..... 10
7. Interventi di assistenza e manutenzione ..... 11
8. Monitoraggio e controlli ..... 11
9. Responsabilità e sanzioni ..... 12
ALLEGATO 1 - GLOSSARIO ..... 13
ALLEGATO 2 - INVENTARIO DELLA STRUMENTAZIONE INFORMATICA, DEI SOFTWARE E DELLE APPLICAZIONI IN DOTAZIONE ALL'ENTE ..... 15

# PREMESSA

Il presente disciplinare ha l'obbiettivo 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 dal Regolamento Europeo 679/2016 sulla protezione dei dati personali, e dal Codice Privacy (d. lgs. 196/2003), come adeguato dal d. lgs. n. 101/2018 e ss.mm..

In via preliminare, occorre precisare che compete al datore di lavoro assicurare la funzionalità e il corretto impiego della rete di internet e della posta elettronica da parte dei lavoratori. Il datore di lavoro deve definire le modalità d'uso di tali strumenti nell'organizzazione dell'attività lavorativa, e deve adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità dei sistemi informativi e dei dati, anche al fine di prevenire utilizzi indebiti che possono essere fonte di responsabilità per i dipendenti e per l'amministrazione. Quindi le disposizioni sono in primo luogo adottate a garanzia degli interessati, e debbono altresì contemperare le esigenze degli utenti del sistema informativo con quelle dell'amministrazione.

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;
- rendere noti gli strumenti messi a disposizione dell'azienda e i software disponibili indicati nell'allegato 2 "inventario della strumentazione informatica";
- 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 nell'allegato 1 "Glossario".

## 1. Misure di sicurezza fisiche

**Accesso alla sede**: per l'accesso fisico ai locali e la disattivazione dell'allarme dell'Ente, quest'ultimo individua i soggetti autorizzati e li dota di una chiave (ad es. trasponder, chiavi semplici, codice, …), la quale deve essere personale, univoca e non utilizzabile da altri e conservata con l'opportuna diligenza a cura dell'assegnatario.
**Accesso alle sale adibite ad uso comune (riunioni o aule corso)**, per minimizzare i rischi relativi ad accesso fisico non autorizzato e furto, gli utenti devono seguire le seguenti regole:

- le sale riunioni e le aule corsi, quando non utilizzate, sono chiuse a chiave. Le chiavi sono custodite da personale dell'Ente incaricato per la gestione della sala o dell'aula;
- qualora le chiavi siano assegnate a personale esterno all'ente, va debitamente autorizzata e documentata la consegna e la restituzione e devono esser fornite le misure di sicurezza da osservare nell'utilizzo della sala.

# 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 presenti devono essere riposti in modo tale da tutelare la riservatezza dei dati in essi contenuta.

Gli **archivi dei documenti cartacei** sono **custoditi in locali** o in elementi di arredo muniti di serratura e chiusi a chiave.
Le chiavi sono custodite dal personale autorizzato.
L'accesso alle banche dati cartacee da parte degli utenti è autorizzato dall'Ente (dal Segretario generale o dai Responsabili di Servizio) in ragione delle mansioni e dei compiti loro assegnati.
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. A fronte di modifiche organizzative dell'Ente i profili di autorizzazione dei singoli autorizzati devono essere rivisti.
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

Ciascuna postazione di lavoro è assegnata nominalmente ad un utente. In caso di necessità operativa è sempre possibile, da parte di ciascun utente, accedere alla rete tramite un'altra postazione utilizzando le proprie credenziali.
Per accedere ai servizi informatici da una postazione di lavoro, l'utente deve utilizzare 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 U:, T:, S:, N: ed il sistema in cloud denominato Google Drive, 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 Transito; 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 files 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 le chat interne (ad es. Google Meet, Google Chat) per farne uso non consono alla 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 previa richiesta del segretario/responsabile del servizio dell'utente interessato. La stessa procedura deve essere seguita per la disattivazione delle utenze per coloro che cessano la propria attività nell'Ente.
L'utente deve essere consapevole del fatto che "cedere" le proprie credenziali ossia comunicarle a terzi significa autorizzare terzi a proprio nome al trattamento dei dati dell'Ente, con effetti potenzialmente dannosi, e che possono esporre a responsabilità disciplinare, civile e penale.

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

- non si possono utilizzare credenziali di altri utenti, anche se conosciute casualmente o fornite volontariamente da altri colleghi;
- le credenziali di autenticazione devono essere modificate o disattivate se cambia la posizione dell'utente all'interno dell'Ente (promozione, spostamento organizzativo, sospensione dell'attività o dimissioni);
- la **password** deve essere composta da almeno 8 caratteri nei quali devono essere presenti almeno un carattere speciale, un numero e un carattere maiuscolo;
- 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 tre 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).

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 (ad esempio nelle pause pranzo) 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 15 minuti.

## 3.3 Banche dati, software, applicazioni e cartelle del server

Il segretario/il responsabile del servizio autorizza l'accesso alle banche dati informatiche dell'Ente, ai software, alle applicazioni e alle cartelle del server ed in particolare:

- decide a quali cartelle del server l'utente può avere accesso (l'abilitazione all'accesso non può essere generica a tutte le cartelle del server);
- decide a quali banche dati informatiche, software e/o applicazioni l'utente può avere accesso;
- provvede alla revisione dei profili di autorizzazione dei singoli autorizzati a fronte di modifiche organizzative, 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.

## 3.4 Sistema di backup

L'Ente dota il proprio sistema informatico 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, disco C:).

## 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:

- non aprire allegati che contengano un'estensione doppia;
- 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 (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 (Internet e Telpat). Il sistema firewall, controllando il traffico in entrata ed in uscita dalla rete riesce a minimizzare i rischi di intrusione e accesso non autorizzato alla rete informatica dell'Ente e quindi agli strumenti informatici e ai dati in essi contenuti.

## 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 (avvalendosi di un gruppo di continuità adeguatamente dimensionato).
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 in cui sono ospitati i server/armadi, 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 da utenti autorizzati che le custodisce in sicurezza;
- l'accesso ai locali in cui sono ospitati i server/armadi è consentito solo ad utenti autorizzati;
- è attivo un sistema che monitora costantemente il funzionamento dei dispositivi e degli applicativi collegati al server. Il sistema si basa su un apposito dispositivo software che consente il tempestivo rilevamento di malfunzionamenti o guasti dei dispositivi e degli applicativi monitorati che in automatico invia 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;
- nei locali/armadi in cui sono ospitati i server è installato un sensore di temperatura 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 ad un gruppo di continuità.

## 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.

## 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 sconsigliato l'uso di chiavette USB per il trasferimento di file in assenza di antivirus e antimalware.

## 3.10 Fotocopiatrici e scanner

Gli utenti nello svolgimento delle attività a loro assegnate se 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 loro contenuti, si devono rispettare le seguenti regole:

- gli strumenti, se contengono dati dell'Ente, devono essere conservati in modo sicuro (contenitori chiusi a chiave);
- se lo strumento è predisposto, inserire un PIN per proteggere i dati memorizzati. Tale PIN può essere condiviso solo con altre persone autorizzate al trattamento dei dati memorizzati o consegnato al responsabile incaricato della gestione degli strumenti;
- se gli strumenti sono adoperati 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 incaricato della gestione degli strumenti che valuta la sua 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 il sistema operativo e 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 videoconferenza

## 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. L'utente, utilizzando le apposite funzioni di delega fornite dal sistema di posta elettronica può comunque concedere, in caso di necessità e per ragioni di servizio, l'accesso e l'utilizzo della propria casella ad altri colleghi;
- 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 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, etc…;
- 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…), dev'essere bloccato l'accesso e il contenuto dev'essere cancellato entro un congruo termine 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, oltre ad una policy informativa di avviso della scadenza a tempo della casella per l'utilizzatore.
Nel caso invece di caselle e-mail condivise per servizio/ufficio e non riconducibili ad un unico soggetto (ad es. segreteria, anagrafe, info…) non è prevista la chiusura e la cancellazione della casella e dei dati in essa contenuti.

### 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, adottando una apposita policy di black list.
Nell'utilizzo di internet è vietato:

- lo scarico (upload e/o download) di files 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 guestbooks anche utilizzando pseudonimi (o nicknames) 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
- accertarsi dell'identità dell'interlocutore prima di fornire informazioni o dati personali relativi ad una persona fisica.

### 4.4 Videoconferenza

Nell'utilizzo del sistema di videoconferenza reso disponibile dall'Ente, è necessario ricordare:

- che i sistemi di videoconferenza sono strumenti di lavoro da utilizzare in alternativa a riunioni in presenza o come alternativa alla chiamata telefonica, di dotarsi di cuffie con microfono (per esempio anche quelle del telefono cellulare); questo migliora sensibilmente la qualità del segnale audio;
- di spegnere il proprio microfono quando non utilizzato per evitare di introdurre rumori, brusii o interferenze;
- che nel caso ci si connetta dalla propria abitazione e non si disponga di una zona riservata è possibile utilizzare sfondi virtuali, o, se si preferisce, disattivare la videocamera testando preventivamente l'illuminazione;
- che nel caso in cui non si disponga di banda sufficiente a garantire un adeguato segnale audio-video è conveniente disattivare la videocamera;
- di scollegarsi sempre al termine della videoconferenza.

## 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, da utilizzarsi nel totale rispetto delle regole determinate dalla regolamentazione e in conformità con le indicazioni che gli saranno fornite.
Gli strumenti di lavoro affidati al dipendente devono essere usati esclusivamente per lo svolgimento dell'attività lavorativa, nel rispetto di quanto previsto dai regolamenti 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, all'assistenza informatica e dovrà consegnare lo strumento guasto 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 viene 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.

Il dipendente potrà utilizzare, nel caso in cui non possa disporre di strumentazione fornita dall'Ente, apparecchiature di proprietà per svolgere attività lavorativa previa specifica autorizzazione dell'Ente.
Nel caso di utilizzo di sistemi di proprietà verrà fornita assistenza solo sulle componenti software che saranno fornite dall'Ente.
In particolare, si richiama la necessità di verificare che l'antivirus installato sul computer sia attivo, aggiornato e connesso.
Nel caso in cui ci sia necessità di connettersi a rete wireless diverse da quella della propria abitazione si raccomanda, al fine di prevenire l'esposizione a cyber attacchi, di evitare il collegamento a reti non sicure o sulle quali non siano presenti adeguati sistemi di protezione e sicurezza.

# 6. Fine vita (documenti cartacei e dispositivi elettronici)

## 6.1 Smaltimento dei documenti cartacei

I documenti cartacei per cui non è più obbligatorio provvedere alla loro conservazione (cfr. manuale di scarto dell'Ente), possono essere di due tipi:

- documenti cha 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 e 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. Per ottenere ciò l'Ente si è dotato di macchine distruggi-documenti di livello DIN P-4, è un livello medio che è in grado di produrre frammenti della dimensione di 4 x 38 mm. Praticamente, da un foglio di dimensioni A4, vengono generati ben 421 frammenti. Il livello P-4 è indicato per documenti confidenziali il cui trattamento renderà impossibile riuscire ad assemblare e a leggere anche la più piccola parte del documento originario.
Tali misure e accorgimenti possono essere attuate anche con l'ausilio o conferendo incarico a terzi tecnicamente qualificati, quali centri di assistenza, produttori e distributori di apparecchiature che attestino l'esecuzione delle operazioni effettuate o che si impegnino ad effettuarle.

## 6.2 Smaltimento di rifiuti elettrici ed elettronici

In caso di smaltimento di rifiuti elettrici ed elettronici (ad es. pc, smartphone, tablet), l'effettiva cancellazione dei dati personali dai supporti contenuti nelle apparecchiature elettriche ed elettroniche è obbligatoria in modo da impedire l'acquisizione indebita di dati personali.
La distruzione dei supporti prevede il ricorso a metodologie diverse a seconda del loro tipo, quali:

- sistemi software per la cancellazione completa dei dischi rigidi;

- sistemi di punzonatura[1] o deformazione meccanica;
- distruzione fisica o di disintegrazione (usata per i supporti ottici come i CD-ROM e i dvd);
- demagnetizzazione ad alta intensità.

Tali misure e accorgimenti possono essere attuate anche con l'ausilio o conferendo incarico a terzi tecnicamente qualificati, quali centri di assistenza, produttori e distributori di apparecchiature che attestino l'esecuzione delle operazioni effettuate o che si impegnino ad effettuarle.

## 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 di norma effettuati dagli amministratori di sistema tramite il servizio di assistenza e amministrazione remota. Il sistema di assistenza in remoto consente, previa autorizzazione del dipendente, 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 servizio o struttura, 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 o 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, verrà preventivamente inviato un avviso a tutti i lavoratori per preallertare rispetto al controllo attivato nei giorni ed ore specificati. 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;

[1] Ad esempio, utilizzando un perno d'acciaio temprato, che tramite una leva, perfora l'hard disk in una o più zone distruggendolo definitivamente.

- 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 essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità esplicitati.

## 9. Responsabilità e sanzioni

L’utente che abbia violato il presente disciplinare o la normativa ivi richiamata, potrà essere soggetto ad azione disciplinare in conformità a quanto stabilito dal Codice etico e di comportamento, dai contratti collettivi di lavori e dalla normativa in materia di pubblico impiego, fatta salva la possibilità per l’Ente di esercitare le opportune azioni giudiziarie nelle sedi competenti, a tutela dei propri diritti giuridicamente tutelati.
In caso di danno, la violazione espone altresì l’utente responsabile ad azioni legali di carattere civile o penale da parte dei danneggiati e a richieste di risarcimento anche da parte dell’Ente.

# ALLEGATO 1 - GLOSSARIO

**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.
**Comunicazione di dati personali**
Il dare conoscenza di dati personali ad uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione o mediante interconnessione.
**Diffusione di dati personali**
Il dare conoscenza di dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione. Vi è diffusione, ad esempio, in caso di pubblicazione in internet di dati personali (es. sito web, albo pretorio).
**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…)
**Pseudonimizzazione**
Il trattamento dei dati personali in modo tale che i dati personal i non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive si ano conservate separata mente e soggette a misure tecniche e organizzative intese a garantire che tal i dati personali non siano attribuiti a una persona fisica identificata o identificabile.
**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.

**Ondemand (in differita)**

Modalità di accesso in rete a file audiovisivi che vengono resi disponibili su richiesta di un utente.

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

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

**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 freeware**

Programmi software distribuiti in modo gratuito.

**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.

**Stand – alone**

Si riferisce ad un'apparecchiatura capace di funzionare da sola, indipendentemente dalla presenza di altre apparecchiature con cui potrebbe comunque interagire.

**Streaming (in diretta)**

Modalità di accesso in rete a file audiovisivi di cui si può fruire in tempo reale.

**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.

**Webcast/Web casting**

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.

# ALLEGATO 2 - INVENTARIO DELLA STRUMENTAZIONE INFORMATICA, DEI SOFTWARE E DELLE APPLICAZIONI IN DOTAZIONE ALL'ENTE

## STRUMENTAZIONE INFORMATICA

- Server VmWare e macchine virtuali con sistema operativo Windows Server
- Backup su disco NAS
- Computer desktop e portatili con sistema operativo Microsoft Windows
- Smartphone Android
- Router wifi con SIM dati integrata (cd. saponette)
- Fotocopiatrici multifunzione, scanner e stampanti fino al formato A3 a colori e bianco/nero
- Stampanti laser personali in formato A4 bianco/nero
- Scanner da scrivania in formato A4
- Scanner per grandi formati fino ad A0
- Plotter
- Firma digitale con smartcard o token usb

## SOFTWARE E APPLICAZIONI

- Microsoft Windows (sistema operativo)
- Microsoft Office (Word, Excel, Powerpoint, Publisher, suite per ufficio, strumento di produttività aziendale utilizzato per creare contenuti quali documenti di testo, grafici o presentazioni)
- Google Workspace (suite di software e strumenti di produttività per il cloud computing e per la collaborazione, include Gmail, Meet, Calendar per la comunicazione; Drive per l'archiviazione; Documenti, Moduli la produttività e la collaborazione)
- Protocollo Informatico Trentino PITRE
- Autocad (programma di disegno tecnico assistito dal computer)
- QGis (software per visualizzare, organizzare, analizzare e rappresentare dati spaziali)
- Gisco Atti.Net (gestione degli atti amministrativi)
- Videoconferenza LifeSize cloud e Google Meet

N.B.: Tutti i marchi e nomi sopra riportati sono di proprietà dei rispettivi detentori dei copyright; marchi di terzi, nomi di prodotti, nomi commerciali, nomi corporativi e società citati possono essere marchi di proprietà dei rispettivi titolari o marchi registrati da altre società e appartengono ai loro legittimi proprietari e sono stati utilizzati a puro scopo esplicativo, senza alcun fine di violazione dei diritti di copyright vigenti.

Firmato da: ANDREA FONTANARI