PROVINCIA
DI TERAMO
Medaglia d'Oro al Merito Civile

Regolamento per l'utilizzo delle risorse informatiche e il trattamento dati della Provincia di Teramo

Approvato con Delibera del Presidente n. 241 del 30/11/2023

Sommario

ART. 1 - OGGETTO DEL REGOLAMENTO E AMBITO DI APPLICAZIONE

1. La Provincia di Teramo (di seguito anche detta Titolare) adotta il presente Regolamento per definire le condizioni di utilizzo degli strumenti di lavoro informatici e digitali, al fine di:
   a. evitare comportamenti inconsapevoli che possano innescare problemi o minacce alla sicurezza nel trattamento dei dati;
   b. informare i soggetti che trattano dati con risorse informatiche delle misure di tipo organizzativo e tecnologico adottate all'interno dell'Ente per la sicurezza dei dati;
   c. illustrare le modalità di utilizzo consapevole e diligente delle risorse informatiche messe a disposizione;
   d. comunicare agli utenti le finalità e le modalità dei controlli che l'Ente potrebbe effettuare sulle risorse messe a disposizione; non sono in nessun caso installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo l'utilizzo come strumenti per il controllo a distanza dell'attività dei lavoratori;
   e. fornire agli utenti una serie di indicazioni operative sulle corrette modalità di trattamento dei dati personali, delle informazioni e degli strumenti che permettono di gestirli, al fine di garantire l'adeguata riservatezza, integrità e disponibilità dei dati gestiti dall'Ente.
2. Le prescrizioni contenute nel presente Regolamento si applicano a tutto l'insieme delle risorse informative, elettroniche, di comunicazione, di archiviazione, audiovisive, cartacee e a qualsiasi altra tipologia di risorsa utilizzata, quali strumenti di lavoro, per perseguire le finalità istituzionali, siano esse di proprietà della Provincia di Teramo, che di soggetti che operano in nome e per conto di essa.
3. Gli strumenti tecnologici considerati nel presente Regolamento costituiscono tutti strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, anche ai sensi e per gli effetti dell'art. 4, comma secondo, della Legge n. 300/1970 ("Statuto dei Lavoratori").
4. Il presente Regolamento si applica a tutto il personale dipendente, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori e consulenti della Provincia di Teramo, indipendentemente dalla natura del rapporto contrattuale, autorizzati a far uso di strumenti tecnologici dell'Ente o ad accedere alla rete informatica e ad eventuali dati ed informazioni ivi conservati e trattati.
5. Nel caso di soggetti esterni designati dalla Provincia di Teramo responsabili o sub-responsabili del trattamento ai sensi dell'art. 28 del Regolamento UE 2016/679, questi devono impegnarsi a rispettare e far rispettare gli stessi principi di sicurezza e di modalità di gestione delle informazioni presenti nel Regolamento a tutti i propri dipendenti e ad eventuali altri soggetti.

ART. 2 - DEFINIZIONI E CONTESTO NORMATIVO DI RIFERIMENTO

Ai fini dell'applicazione del presente Regolamento deve intendersi per:

TITOLARE DEL TRATTAMENTO DEI DATI: la figura individuata dall'art. 4 GDPR, definita come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri soggetti, determina le finalità e i mezzi del trattamento di dati personali. Vigila sulla puntuale osservanza di tutte le disposizioni in materia di trattamento dei dati. Designa e/o autorizza tutte le altre figure coinvolte nel trattamento dei dati. In questo specifico contesto è rappresentato dalla Provincia di Teramo che adotta il presente Regolamento, a eccezione di specifiche e definite circostanze in cui la Provincia di Teramo agisce come responsabile del trattamento dei dati.

SISTEMI INFORMATIVI: è l'abbreviazione della struttura preposta alla gestione, alla configurazione, al coordinamento e al rilascio delle risorse informatiche della Provincia di Teramo, a cui fanno riferimento gli Amministratori di Sistema competenti per tale contesto. Quando tale struttura è esterna all'Ente, essa svolge le proprie attività in nome e per conto di essa, agendo in qualità di responsabile del trattamento dei dati ai sensi dell'art. 28 GDPR.

AMMINISTRATORI DI SISTEMA: sono le figure, designate dal titolare o dai responsabili, che provvedono operativamente alla gestione e manutenzione del sistema informatico sulla base delle misure organizzative fissate dal responsabile dei servizi informativi, in linea con quanto indicato dal Garante della Privacy nel suo provvedimento del 27 Novembre 2008 e aggiornamenti successivi. Il provvedimento prevede la possibilità di nominare Amministratori di Sistema sia soggetti interni che esterni alla Provincia di Teramo: per le finalità del presente Regolamento si intendono gli Amministratori di Sistema preposti alla gestione delle risorse informatiche del titolare, siano essi interni o esterni.

AUTORIZZATI AL TRATTAMENTO DEI DATI: sono le persone fisiche designate dal titolare del trattamento, a cui sono assegnati specifici compiti e funzioni connessi al trattamento dei dati; trattano i dati sia attraverso strumenti informatici che cartacei; operano attenendosi alle istruzioni impartite.

RESPONSABILE DEL SISTEMA INFORMATICO: il soggetto responsabile del Servizio Informatico della Provincia di Teramo;

AMMINISTRATORI DEL SISTEMA: le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, nonché alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi;

AMMINISTRATORI: il Presidente della Provincia, i Consiglieri provinciali e i consiglieri delegati;

OPERATORI DEL SISTEMA INFORMATICO DELLA PROVINCIA DI TERAMO (OPERATORI): gli amministratori, i dipendenti ed i collaboratori espressamente autorizzati dalla Provincia di Teramo ad accedere ed utilizzare i sistemi informatici e telematici;

UTENTI: sono i soggetti destinatari del presente Regolamento, a cui sono assegnate le risorse informatiche del titolare. Per "utente" deve intendersi ogni dipendente, collaboratore e/o consulente o altro soggetto in possesso di specifiche credenziali di autenticazione e a cui sono state assegnate le risorse per lo svolgimento di attività correlate alle finalità perseguite dal Titolare.
Ogni utente potrà essere designato quale "autorizzato al trattamento" o "referente privacy" ovvero "amministratore di sistema", ai sensi di quanto previsto dal GDPR, dal Codice Privacy e dagli specifici provvedimenti in materia del Garante Privacy, in ragione delle specifiche attività e funzioni che ciascun utente ricopre all'interno dell'Ente come da organigramma e da contratto.

CASELLA DI POSTA ELETTRONICA PERSONALE: la casella di posta elettronica affidata ai dipendenti ed ai collaboratori della Provincia di Teramo, il formato dell'indirizzo di posta è di norma il seguente: <iniziale_del_nome>.<cognome>@provincia.teramo.it.

CASELLA DI POSTA ELETTRONICA DI SERVIZIO: la casella di posta elettronica affidata

ai settori, ai servizi ed agli uffici, il formato dell'indirizzo di posta è di norma il seguente: <Settore/Servizio/Ufficio>@provincia.teramo.it.

FIRMA DIGITALE: un particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

DATO PERSONALE: qualsiasi informazione che possa ricondurre, in forma diretta o indiretta, ad una persona fisica identificata o identificabile. Se non diversamente espresso, il dato personale è sempre quello trattato dagli utenti esclusivamente per attività correlate alle proprie funzioni all'interno della Provincia di Teramo.

DATO PRIVATO: qualsiasi informazione afferente ad utenti, non correlata alle funzioni da essi svolte nella Provincia di Teramo; tale contesto di riferimento non è pertinente o strumentale alle attività istituzionali del titolare.

DATO PROFESSIONALE: qualsiasi informazione trattata dagli utenti nello svolgimento delle proprie attività e funzioni esercitate nella Provincia di Teramo.

TRACCIAMENTO: memorizzazione di eventi e operazioni effettuata automaticamente da un qualsivoglia dispositivo informatico, per finalità manutentive e di funzionamento dello stesso.

RILEVAZIONE: complesso di operazioni di raccolta, analisi, verifica, conservazione dei tracciamenti effettuati dai dispositivi e di qualsiasi altra forma di intervento di carattere professionale riferibile al funzionamento e all'utilizzo delle risorse informatiche, svolto a fronte di comprovate necessità definite nei capitoli seguenti del presente Regolamento.

DISPOSITIVO: qualsiasi strumento di elaborazione elettronica utilizzato per lo svolgimento delle attività che fanno capo alla Provincia di Teramo, il cui utilizzo rientra nel perimetro di competenza del presente Regolamento. Rientrano in tale definizione, a titolo esemplificativo e non esaustivo, desktop computer, notebook, tablet, ecc.

SUPPORTO DI ARCHIVIAZIONE: qualsiasi supporto elettronico destinato all'archiviazione e la custodia dei dati, come ad esempio chiavette USB, hard disk esterni, CD e DVD, ecc.

GDPR (Regolamento Generale sulla Protezione dei Dati): viene così definito il Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Il presente Regolamento è redatto sulla base dei seguenti e principali riferimenti normativi:

- Codice penale, con particolare riferimento ai reati informatici;
- L. 300/1970 (Statuto dei lavoratori) - artt. 4, 7 e 8 e ss. mm ed ii.;
- D. Lgs. 196/2003 e s.m.i. (Codice in materia di protezione dei dati personali) e ss. mm ed ii. (d'ora in poi "Codice della Privacy");
- D. Lgs. 82/2005 e s.m.i. (Codice dell'amministrazione digitale) e ss. mm ed ii.;

- Provvedimenti del Garante per la protezione dei dati personali applicabili al contesto oggetto del presente documento, fra cui le "Linee guida per posta elettronica e Internet" di cui alla deliberazione 13/2007;
- D. Lgs. 81/2008 e s.m.i (Testo Unico sulla sicurezza) e ss. mm ed ii.;
- D.P.R 62/2013 (Codice di comportamento dei dipendenti della pubblica amministrazione) e Codice di comportamento della Provincia di Teramo e ss. mm ed ii.;
- Regolamento (UE) 2016/679 (General Data Protection Regulation, di seguito detto GDPR)

ART. 3 - PRINCIPI GENERALI

1. I dati raccolti durante l'utilizzo degli strumenti informatici e l'accesso alla rete internet devono rispettare le garanzie in materia di protezione dei dati e, in particolare, devono essere:
   a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
   b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
   c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
   d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
   e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
   f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

ART. 4 - COMPETENZE E RESPONSABILITÀ

1. La struttura delegata alla gestione e all'erogazione dei servizi informatici e telematici, nonché all'attuazione del presente regolamento, è il "Servizio Informatico" della Provincia di Teramo.

2. Il Responsabile del sistema informatico è il Responsabile del "Servizio Informatico" della Provincia di Teramo.

3. Il Responsabile del sistema informatico è, altresì, il Responsabile della sicurezza informatica, ed è tenuto a:
   a) informare i Dirigenti di Area e Responsabili dei Settori non incardinati in Area sulle disposizioni in merito all'uso consentito delle risorse del sistema informatico dell'Ente;
   b) assicurare che il personale a lui assegnato uniformi le proprie attività alle regole ed alle procedure descritte nel presente Regolamento;

c) assicurare che i fornitori e/o eventuale personale incaricato esterno si uniformi alle regole ed alle procedure descritte nel presente Regolamento.

4. I Dirigenti delle aree e i Responsabili dei Settori non incardinati in Area sono tenuti a:
   a) informare il personale a loro assegnato sulle disposizioni in merito all'uso consentito delle risorse del sistema informatico dell'Ente;
   b) assicurare che il personale a loro assegnato si uniformi alle regole ed alle procedure descritte nel presente Regolamento;
   c) adempiere a tutti gli obblighi inerenti ai trattamenti di dati personali di cui la Provincia di Teramo è Titolare.

5. Il Responsabile della sicurezza informatica è tenuto a svolgere le seguenti attività:
   a) monitorare i sistemi per individuare eventuali rischi per la sicurezza informatica, nel rispetto della privacy degli Operatori e delle norme a tutela del lavoratore;
   b) elaborare delle regole per un utilizzo ragionevolmente sicuro del sistema informatico;
   c) implementare e controllare delle policy di sicurezza;
   d) predisporre materiale informativo e divulgativo in materia di sicurezza informatica.

6. Ogni utente è responsabile per ciò che concerne:
   a) il rispetto delle regole dettate dall'Amministrazione per l'uso del sistema informatico;
   b) la segnalazione senza ritardo di ogni eventuale attività contraria al presente regolamento di cui venga a conoscenza;
   c) l'uso e la conservazione delle proprie credenziali di autenticazione (username e password).

7. Ogni utente in servizio, se dotato delle necessarie dotazioni informatiche, è tenuto ad accedere alla casella di posta elettronica e al protocollo, almeno per n. 2 volte durante la giornata lavorativa, preferibilmente all'inizio e alla fine della giornata lavorativa.

8. Il Settore Risorse Umane è tenuto a comunicare ai Sistemi Informativi della Provincia di Teramo ogni variazione di carattere amministrativo (assunzione, comando, cessazione etc.) relativa al personale della Provincia di Teramo, al fine di consentire agli Amministratori di Sistema la creazione/modifica/cancellazione dei permessi di accesso alle risorse informatiche, affinché siano coerenti con le mansioni affidate agli utenti e il relativo trattamento dei dati, fatta salva diversa indicazione dei Dirigenti di riferimento per necessità istituzionali. A seguito delle predette comunicazioni, i Sistemi Informativi coordineranno la consegna e il ritiro delle risorse informatiche.

ART. 5 - DATI TRATTATI ATTRAVERSO LE RISORSE INFORMATICHE CONCESSE IN DOTAZIONE

1. Le risorse informatiche sono messe a disposizione dalla Provincia di Teramo per l'esercizio delle attività correlate alle finalità istituzionali, pertanto l'utilizzo degli strumenti in dotazione deve avere prevalente carattere professionale.
2. È consentito l'utilizzo delle risorse informatiche messe a disposizione per *assolvere alle incombenze personali senza doversi allontanare dalla sede di servizio,* a condizione che:
   a) l'utilizzo sia contenuto in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali;
   b) l'utilizzo non sia contrario alle regole di condotta indicate nei successivi articoli e non possa in alcun modo ledere l'immagine della Provincia di Teramo;

c) ci si attenga esclusivamente alle prescrizioni indicate nei successivi articoli, nei quali sono definiti specifici limiti definiti per ogni tipologia di risorsa;

d) l'utilizzo non danneggi in alcun modo, diretto o indiretto, le proprietà della Provincia di Teramo;

e) l'utilizzo non comporti alcuna violazione di leggi;

f) sia esplicito verso terzi che la responsabilità di qualsiasi operazione svolta per finalità personali sia imputabile esclusivamente all'utente;

g) l'utilizzo non comprometta le misure di sicurezza e di protezione dei dati attuate e definite dal presente Regolamento o dalle politiche di sicurezza della Provincia di Teramo.

3. Non è in nessun caso consentito:
   a) l'utilizzo privato delle informazioni trattate per conto della Provincia di Teramo;
   b) trattare dati di cui la Provincia di Teramo è Titolare o Responsabile esterno del Trattamento, se non per attività strumentali al perseguimento delle finalità istituzionali dell'Ente.
4. È ammessa la custodia di dati privati sugli strumenti forniti in dotazione a condizione che:
   a) siano riposti in cartelle delle quali sia esplicitamente indicata la natura privata del dato (es. cartelle con dicitura "personale");
   b) siano esplicitamente differenziabili dai dati trattati per attività strumentali al perseguimento delle finalità istituzionali;
   c) vengano rimossi prima del rilascio o della riconsegna delle risorse fornite;
   d) non siano in alcun modo riposti su sistemi server e/o altre risorse di archiviazione fruibili attraverso condivisioni di rete.
5. Alla riconsegna delle risorse da parte degli utenti, la Provincia di Teramo potrà liberamente disporre dei dati ivi presenti. Eventuali dati di carattere privato ancora residenti al momento della riconsegna della postazione verranno trattati secondo i principi di pertinenza e non eccedenza previsti dalla normativa sulla protezione dei dati personali. La risorsa potrà essere ripristinata con valori predefiniti (o ripulita) ed assegnata ad altri soggetti.
2. La Provincia di Teramo si riserva la facoltà di rimuovere tutti i dati presenti sulle risorse riconsegnate qualora si ritenga necessario per la riassegnazione della stessa.

ART. 6 - GESTIONE DELLE PASSWORD E DEGLI ACCESSI

1. L'utente deve utilizzare sempre una password ogni qualvolta ciò sia richiesto.
2. L'utente è tenuto ad assicurare la non divulgazione a terzi, la custodia e segretezza delle password utilizzate per attività lavorative, al fine di garantire la sicurezza dei dati e dei servizi utilizzati.
3. La password di ingresso al dominio della Provincia di Teramo viene attribuita dal Servizio Sistemi Informativi dell'Ente al nuovo utente per il primo accesso dopo la creazione dell'utenza. Dopo il primo accesso il sistema chiederà all'utente di modificare la password, la quale sarà conosciuta solo dall'utente stesso. Qualora si renda necessario (per manutenzione, aggiornamenti, assenza prolungata imprevista che renda indisponibili risorse gestite dall'utente) che un Amministratore di sistema debba accedere al sistema utilizzando il profilo dell'utente, la password di accesso dell'utente stesso verrà modificata. Al successivo accesso da parte dell'utente l'Amministratore di

sistema gli rilascerà una nuova password di cortesia che dovrà essere immediatamente modificata dall'utente stesso.

4. L'accesso agli applicativi e ai sistemi può a sua volta essere regolato da un'ulteriore password: le modalità di gestione e di scadenza di dette password sono specifiche per ogni ambiente. All'utente sarà fornito un profilo personale e verranno attivate procedure per garantire all'utente stesso la conoscenza esclusiva della propria password. Nel caso il sistema non lo consenta o sia necessario l'intervento dell'Amministratore di Sistema per garantire la disponibilità dei dati, verranno concordate procedure specifiche per la gestione degli accessi.
5. Se le credenziali sono comunicate agli utenti tramite comunicazioni elettroniche, la user-id e la password non devono essere comunicate tramite lo stesso canale di comunicazione. Qualora i canali di comunicazione utilizzati siano entrambi consultabili tramite un dispositivo (es smartphone, notebook, tablet, etc), tale dispositivo deve essere a sua volta protetto dall'accesso di soggetti terzi.
6. Le password del dominio e degli applicativi, salvo impossibilità dovute all'obsolescenza del software, devono essere modificate ogni 6 mesi e soddisfare i seguenti requisiti:
   a) lunghezza minima 8/10 caratteri;
   b) contenere almeno un carattere maiuscolo;
   c) contenere almeno un carattere minuscolo;
   d) contenere almeno un carattere numerico;
   e) contenere almeno un carattere simbolo ($,*,%,@,#, ecc.);
   f) non deve contenere nome proprio, cognome e matricola;
   g) non deve contenere una sequenza di caratteri identici o gruppi di caratteri ripetuti.
7. Nel caso in cui si sospetti che una password abbia perso la segretezza, l'utente provvederà ove possibile a modificarla personalmente oppure con il supporto di uno degli Amministratori di Sistema.
8. Non è consentito utilizzare il profilo personale di altri soggetti per accedere ai sistemi. Qualora l'utente venga a conoscenza delle password di un altro utente, è tenuto a darne immediata notizia all'utente stesso o a un Amministratore di sistema.

ART. 7 - UTILIZZO DELLE POSTAZIONI DI LAVORO

1. La postazione informatica affidata agli utenti è uno strumento di lavoro. Ogni utilizzo non pertinente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza per cui va assolutamente evitato l'utilizzo improprio della stessa postazione.
2. Il Servizio Sistemi Informativi dell'Ente provvede a dotare tutti i personal computer assegnati agli utenti di sistema operativo e sue estensioni: antivirus, programmi di office automation (programmi per la redazione di documenti, di fogli elettronici, di gestori di database) e di eventuale software specifico correlato alle necessità delle attività lavorative. Provvede altresì a mantenere aggiornato il sistema operativo ed i software principali (antivirus, software per la navigazione in Internet, etc.), al fine di garantire la sicurezza complessiva del pc e del Sistema Informatico della Provincia di Teramo. L'accesso all'elaboratore è protetto con credenziali di autenticazione e autorizzazione (username e password), attribuite dal Servizio Sistemi Informativi dell'Ente secondo le modalità di cui al precedente articolo del presente Regolamento: le dette credenziali consentono anche l'autenticazione e l'autorizzazione informatica alla rete locale (LAN) della Provincia ed alla rete

Internet. All'atto del primo accesso al personal computer (login), l'utente deve modificare la password comunicatagli dal Responsabile del sistema informatico con una password personale scelta autonomamente, in base alle direttive contenute nell'apposita sezione del presente Regolamento. La username attribuita dal Responsabile del sistema informatico è immodificabile.

3. Non è consentito l'uso di programmi diversi da quelli messi a disposizione o autorizzati dalla Provincia di Teramo, in quanto l'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Ente a gravi responsabilità civili e penali in caso di violazione della normativa sulla tutela del diritto d'autore (Legge 633 del 22 aprile 1941 sulla tutela della proprietà intellettuale, D.Lgs. 518 del 29 dicembre 1992 sulla tutela giuridica del software e aggiornamenti successivi), che impone la presenza nel sistema di software provvisto di regolare licenza d'uso.
4. Non è consentito agli utenti installare programmi provenienti dall'esterno salvo preventiva autorizzazione degli Amministratori di Sistema debitamente incaricati, i quali, in rispondenza alle politiche di sicurezza della Provincia di Teramo ed alla normativa vigente, verificheranno l'opportunità (in termini di sicurezza dei sistemi) dell'installazione, onde evitare il grave pericolo di introdurre vulnerabilità, virus, nonché di alterare la stabilità delle applicazioni dell'elaboratore.
5. Gli utenti che sono in possesso di privilegi amministrativi attraverso i quali hanno la possibilità di effettuare installazioni sulla postazione di lavoro, devono comunque richiedere l'autorizzazione ai Sistemi Informativi della Provincia di Teramo prima di procedere all'installazione. Solamente in casi eccezionali di motivata urgenza possono procedere all'installazione, formalizzando l'autorizzazione successivamente. In questo caso le verifiche di sicurezza (virus, vulnerabilità, compatibilità con il sistema, etc…) che normalmente vengono effettuate dai Sistemi Informativi prima dell'inserimento di un software del sistema informatico, dovranno essere effettuate da chi effettua l'installazione.
6. Le attrezzature vengono consegnate agli utenti con una configurazione coerente con le misure organizzative e di sicurezza impostate dalla Provincia di Teramo: non è loro consentito modificare le caratteristiche impostate, salvo preventiva autorizzazione degli Amministratori di Sistema incaricati.
7. La postazione di lavoro deve essere, di norma e fatte salve specifiche disposizioni dell'Amministratore di Sistema o espresse e specifiche contingenze che rendano necessario, in via del tutto eccezionale, derogare a tale prescrizione, spenta prima di lasciare la sede di lavoro o in caso di assenze prolungate dalla sede. In ogni caso, poiché lasciare un sistema di elaborazione incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'uso indebito, l'utente che lascia incustodita la postazione accesa deve bloccarne l'uso tramite la combinazione dei tasti *CTRL + ALT + CANC* e successivo *INVIO* dopo la scelta dell'opzione che dispone il blocco del computer.
8. Il blocco dello schermo deve essere attivato con la richiesta di password per lo sblocco e deve partire automaticamente non oltre il tempo di 10 minuti di non utilizzo.
9. Ogni utente deve prestare la massima cautela nell'utilizzo dei supporti rimovibili di origine esterna. Prima dell'accesso alle risorse contenute nel supporto deve provvedere alla sua scansione tramite il software antivirus. L'utente deve avvertire immediatamente l'Amministratore di Sistema nel caso in cui vengano rilevate minacce dal sistema antivirus.
10. Non è consentito l'utilizzo di giochi o altre applicazioni di tipo ludico, anche se comprese nel sistema operativo installato.
11. Non sono permesse le seguenti attività:

a) caricare, memorizzare, pubblicare, diffondere, distribuire, tramite risorse della Provincia di Teramo, documenti, informazioni, immagini, filmati etc. in generale, ed in particolare:
   i. a carattere violento, pornografico o contrario alla pubblica decenza, o suscettibile di mancare di rispetto agli esseri umani o alla loro dignità, con contenuto discriminatorio razziale ed etnico, contrario al buon costume, oltraggioso nei confronti dei minori, contrario all'ordine pubblico, diffamatorio o che contenga contenuti illeciti penalmente o civilmente riconducibili a categorie qui non espressamente indicate;
   ii. illeciti in base alla normativa sul diritto d'autore;
   iii. pregiudizievoli per le risorse della Provincia di Teramo e per l'integrità e la conservazione dei dati della Provincia di Teramo stessa;
   iv. pregiudizievoli per l'immagine e il buon nome della Provincia di Teramo anche all'esterno del ristretto contesto dell'Ente;

b) accedere a server web trattanti materie o soggetti ricadenti nelle categorie sopra elencate;

c) tenere comportamenti che possano indurre taluno ad effettuare invii di materiale rientrante nelle tipologie sopra elencate; laddove l'utente riceva - anche involontariamente - tali materiali, è tenuto a informare il personale dei Sistemi Informativi ed attenersi alle istruzioni impartite circa il trattamento di tali materiali;

d) utilizzare le risorse della Provincia di Teramo con fini di molestia, minaccia o comunque violando le norme di legge in vigore;

e) caricare, memorizzare, trasmettere o utilizzare programmi, software, procedure o altra utilità che siano protetti dalle leggi sulla proprietà intellettuale, a meno che la Provincia di Teramo non ne detenga regolare licenza e/o autorizzazione del produttore;

f) utilizzare strumentazioni, programmi, software, procedure, etc. messi a disposizione dalla Provincia di Teramo in violazione delle leggi sulla proprietà intellettuale, delle regole di buona condotta applicabili e delle prescrizioni emanate dalla Provincia stessa;

g) caricare o trasmettere, con volontà, archivi o programmi contenenti virus o dati alterati;

h) manomettere sistemi o archivi in maniera tale da inficiare la riservatezza, la disponibilità e/o l'integrità dei dati;

i) inviare messaggi in massa ("spam") o favorire il propagarsi di notizie riconducibili a ciò che abitualmente viene definito "catena di S. Antonio";

j) utilizzare le risorse della Provincia di Teramo in modo da consentire a soggetti non abilitati l'accesso ai dati e ad alle informazioni riservate, se non nei casi espressamente previsti dalla legge e/o da regolamenti interni.

12. Oltre alle eventuali conseguenze di natura disciplinare o contrattuale in caso di violazione, rimane ferma la personale responsabilità del trasgressore, qualora taluna delle attività elencate al comma precedente possa avere conseguenze di natura penale.

12. In caso di anomalie dell'hardware e del software affidatogli, l'utente deve immediatamente bloccarne l'operatività, fermare le eventuali elaborazioni in corso ed informare immediatamente i Sistemi Informativi per le incombenze di competenza.

13. L'esecuzione automatica dei contenuti dinamici (es. macro) presenti nei file deve essere mantenuta disattivata.

ART. 8 - UTILIZZO NOTEBOOK E ALTRI DISPOSITIVI ELABORATIVI PORTATILI

1. Ai dispositivi portatili si applicano le regole di utilizzo previste per i personal computer connessi alla rete.
2. Gli utenti di dispositivi portatili sono tenuti, dovunque dovessero trovarsi, a mettere in sicurezza la strumentazione utilizzata e i dati nella stessa contenuti.
3. Danni arrecati alle attrezzature o loro perdita dovuti ad incauta custodia saranno a carico dell'utente utilizzatore.
4. L'utente è responsabile delle attrezzature informatiche portatili assegnategli dalla Provincia di Teramo e deve custodirle con diligenza, sia durante gli spostamenti sia durante l'utilizzo presso i luoghi di lavoro.
5. Il dispositivo non deve essere lasciato incustodito in zone a libero accesso, al fine di ridurre il rischio di furti. In caso di trasferte, il dispositivo non deve essere lasciato in macchina, nemmeno per brevi periodi, in parcheggi pubblici o comunque in zone non custodite.
6. Qualora tali dispositivi dovessero essere smarriti o rubati, l'affidatario deve immediatamente segnalare l'evento all'Amministratore di sistema, al fine di approntare le necessarie misure di mitigazione del danno.
7. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna. Prima dell'apertura del supporto deve provvedere alla sua scansione tramite il software antivirus. L'utente deve avvertire immediatamente l'Amministratore di Sistema nel caso in cui vengano rilevate minacce.
8. L'utente deve avvertire immediatamente i Sistemi Informativi nel caso in cui vengano rilevate minacce.
9. L'esecuzione automatica dei contenuti dinamici (es. macro) presenti nei file deve essere mantenuta disattivata.
10. Nei casi in cui i dispositivi portatili siano di utilizzo condiviso e vengano messi a disposizione per attività episodiche (es. trasferte, presentazioni, meeting, etc.), l'utente deve considerare che tali risorse saranno messe a disposizione di altri utenti in momenti successivi, pertanto deve tassativamente rimuovere eventuali dati personali e qualsiasi contenuto elaborato sui dispositivi prima della riconsegna, al fine di evitare incontrollate diffusioni di dati.
11. È consentito conservare documenti di natura professionale sui dispositivi portatili dati in dotazione, con la consapevolezza che non sono sottoposti a procedure di backup e che pertanto la messa in sicurezza di tali dati è demandata alla responsabilità degli utenti che hanno ricevuto tali attrezzature in dotazione.

ART. 9 - DISPOSITIVI MOBILI DATI IN DOTAZIONE

1. Tablet e altri dispositivi mobili forniti in dotazione ad utenti della Provincia di Teramo costituiscono uno strumento finalizzato al perseguimento di attività istituzionali e di carattere professionale.
2. L'utente deve adottare ogni misura per prevenire eventuali furti di dispositivi in dotazione, prestando cautela nella loro custodia.
3. Al fine di ridurre il rischio di accesso ai dati residenti sul tablet da parte di soggetti non autorizzati, l'utente deve attivare sistemi di blocco schermo con protezione con password numerica, con segno grafico composto sullo schermo o tramite riconoscimento dell'impronta digitale (in quest'ultimo

caso deve essere messa a disposizione una modalità alternativa di accesso, per consentirne l'utilizzo anche ad altri utenti autorizzati).

4. Deve inoltre essere attivato automaticamente il blocco dello schermo entro un massimo di 3 minuti di inattività.
5. Il titolare del tablet è responsabile dell'aggiornamento software, delle APP installate nel dispositivo e del sistema Antivirus.
6. A causa della sempre maggiore interazione tra i dispositivi mobili e i sistemi informatici, l'abuso di tali strumenti può costituire una potenziale fonte di minaccia ai sistemi della Provincia di Teramo. Pertanto è vietato:
   a) navigare su siti ritenuti non in linea con le indicazioni specificate nei precedenti capitoli relativi alla navigazione Internet;
   b) installare applicazioni sui dispositivi mobili assegnati dalla Provincia di Teramo senza prima aver concordato la cosa con il responsabile dell'ufficio che ha in dotazione i dispositivi, sentito il parere dei Sistemi Informativi
   c) installare sulle postazioni di lavoro in ufficio programmi di sincronizzazione/backup dei dati contenuti sui dispositivi cellulari potenzialmente dannosi senza la preventiva autorizzazione del responsabile dell'ufficio che ha in dotazione i dispositivi, sentito il parere dei Sistemi Informativi.
7. In caso di disservizio o di problemi di funzionamento software, i Sistemi Informativi e le altre strutture preposte alla manutenzione dei dispositivi potranno effettuare dei controlli sulla configurazione dei programmi installati sull'apparato concesso in uso con finalità di protezione del patrimonio informativo. I controlli verranno effettuati nel rispetto della libertà e della dignità dei lavoratori; il trattamento di eventuali dati personali verrà effettuato nel rispetto dei principi di pertinenza e non eccedenza.
8. La Provincia di Teramo effettua dei controlli della spesa relativa ai consumi di traffico dati, che non comportano la consultazione dei siti visitati. Nel caso vengano ravvisati costi non previsti o spese eccedenti rispetto a quanto contrattualmente definito derivanti dall'utilizzo del dispositivo, potranno essere attivati dei controlli sul dispositivo stesso e sul suo impiego, ai fini del controllo della spesa e di tutela del patrimonio della Provincia di Teramo.
9. Qualora da tali controlli sopra menzionati dovesse emergere un utilizzo inadeguato delle attrezzature (fra cui l'installazione di programmi potenzialmente dannosi), che contravvenga le prescrizioni impartite, tale circostanza verrà comunicata alle strutture competenti che valuteranno l'eventuale adozione di provvedimenti.
10. Al momento della restituzione dei dispositivi, il personale assegnatario dovrà cancellare eventuali contenuti personali (es. e mail, contenuti multimediali, etc).
11. Se il dispositivo restituito contenga dati personali, questi verranno cancellati indiscriminatamente dal personale incaricato dalla Provincia di Teramo prima di un'eventuale assegnazione successiva.
12. APP o informazioni di natura lavorativa che possano essere di utilità per la Provincia di Teramo dovranno essere lasciati a disposizione.
13. Per dispositivi particolari utilizzati per specifiche finalità (es. bodycam, attrezzature fotografiche mobili, etc) si rimanda a specifiche disposizioni dettate dai Sistemi Informativi.
14. In caso di smarrimento o furto di un dispositivo, è necessario segnalare immediatamente la circostanza ai Sistemi Informativi, al fine di valutare eventuali azioni di mitigazione del danno.

ART. 10 - TELEFONIA FISSA E MOBILE

1. Per i dispositivi mobili valgono tutte le prescrizioni relative ai dispositivi mobili dati in dotazione di cui al precedente articolo.
2. Si raccomanda di rimuovere tempestivamente immagini, video e audio e altri contenuti multimediali acquisiti tramite i dispositivi per qualsiasi motivo, al fine di evitare il rischio di divulgazione di dati personali in caso di furto o di smarrimento degli apparati.
3. Potrebbero inoltre essere effettuati controlli dei dati contabili relativi al traffico telefonico, per finalità di controllo della spesa. Tali controlli potranno prevedere la consultazione dei numeri chiamati parzialmente oscurati, che non potranno essere visionati per intero; potrà essere chiesto all'utente di indicare le telefonate effettuate per attività professionale e quelle effettuate per fini privati.
4. In relazione alle telefonate in entrata e in uscita effettuate verso o mediante i telefoni della Provincia di Teramo sono memorizzate le seguenti informazioni:
   - giorno e ora della telefonata;
   - numero chiamato o chiamante;
   - durata della telefonata.

ART. 11 - UTILIZZO DEI SUPPORTI RIMOVIBILI

1. I supporti di memorizzazione rimovibili, attraverso i quali sono trattati dati, forniti dalla Provincia di Teramo devono essere utilizzati solo per attività lavorative.
2. Tutti i supporti esterni (cassette, secure drive, cd, dvd, dischi esterni USB, chiavette USB, SD cards, etc…) contenenti dati personali trattati in ambito professionale devono essere utilizzati con particolare cautela onde evitare che il loro contenuto possa essere trattato da soggetti non autorizzati e ne deve essere assicurata la custodia in sicurezza.
3. L'utente è responsabile dei supporti portatili assegnatigli dai Sistemi Informativi della Provincia di Teramo e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
4. Possono essere utilizzati anche supporti rimovibili privati, a condizione che, qualora su tali supporti si trattino dati di carattere professionale, si applichino le stesse cautele previste per i supporti forniti dalla Provincia di Teramo, assicurando l'esclusivo utilizzo per finalità lavorative e la custodia in sicurezza.
5. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna. Prima dell'apertura del supporto deve provvedere alla sua scansione tramite il software antivirus. L'utente deve avvertire immediatamente i Sistemi Informativi nel caso in cui vengano rilevate minacce.
6. Occorre mantenere impostata la disattivazione dell'esecuzione automatica dei contenuti al momento della connessione dei dispositivi rimovibili.

ART. 12 - STRUMENTI DI FIRMA DIGITALE

1. L'uso del kit di firma digitale, anche remota, è strettamente personale e non cedibile a terzi.

2. Il dispositivo di firma digitale è assegnato:
    a. al Presidente della Provincia;
    b. al Segretario Generale, ai Dirigenti responsabili di Area e ai responsabili dei Settori non incardinati in Area;
    c. ai funzionari titolari di incarico di Elevata Qualificazione;
    d. ai RUP individuati con specifico provvedimento.
3. L'utente titolare del certificato di firma digitale è tenuto ad assicurare la custodia del dispositivo di firma o degli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma da remoto e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri. È altresì tenuto ad utilizzare personalmente il dispositivo di firma.
4. Il PIN utilizzato per la generazione della firma è:
    a. riservato e strettamente personale;
    b. non può essere derivato e la relativa firma è protetta da contraffazioni;
    c. deve essere sufficientemente protetto dal titolare dall'uso da parte di terzi.
5. L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.
6. Gli Utenti titolari di firma digitale sono tenuti a prestare la massima collaborazione, prima della scadenza della validità del certificato di firma, per le attività di rinnovo della firma digitale stessa, nel rispetto delle modalità organizzative definite dal Responsabile dei Servizi Informativi e preventivamente comunicate agli utenti.

ART. 13 - POSTA ELETTRONICA

1. Qualsiasi attività istituzionale realizzata tramite utilizzo di posta elettronica deve essere svolta con l'esclusivo utilizzo di caselle di posta elettronica registrate sotto il dominio di posta della Provincia di Teramo o tramite caselle di posta elettronica certificata registrate dalla Provincia stessa.
2. L'utilizzo della casella di posta elettronica è strumentale all'attività istituzionale della Provincia di Teramo, ma non è il canale ufficiale per le comunicazioni che impegnino l'Ente verso terzi, per le quali occorre utilizzare canali collegati al protocollo informatico della Provincia di Teramo, come la posta elettronica certificata istituzionale.
3. Le caselle di posta elettronica in uso presso la Provincia di Teramo sono di 2 tipologie:
    a) caselle nominative, assegnate con la convenzione <iniziale_del_nome>.<cognome>@provincia.teramo.it. Tali caselle sono intestate personalmente agli utenti: nonostante le caselle siano intestate ad un individuo, sono da considerarsi esclusivamente uno strumento di lavoro e non corrispondenza privata; pertanto, l'utilizzo verso destinatari esterni dovrà essere corretto e coerente con le funzioni istituzionali. L'utilizzo di questa tipologia di caselle di posta elettronica personali è di norma evitato per attività o comunicazioni afferenti al servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account di servizio istituzionale, come riportato nel successivo punto 2. Le caselle di posta individuali hanno validità pari alla durata della permanenza in servizio del dipendente, fatte salve eventuali situazioni di congedo, distacco e comando.

b) caselle di posta assegnate ad un ufficio o ad una funzione sul dominio <nome_servizio>@provincia.teramo.it. Tali caselle sono configurate per lo scambio di posta verso l'esterno e possono essere assegnate a più persone. La continuità nella gestione della corrispondenza e delle attività ad essa correlate dovrà essere assicurata dal Responsabile di competenza, o dai Sistemi Informativi, attraverso opportune scelte organizzative.

4. La casella di posta elettronica, assegnata dalla Provincia di Teramo all'utente, è uno strumento esclusivo di lavoro e può essere utilizzata solo per finalità correlate alle attività istituzionali. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse e del contenuto dei messaggi inviati. *Ciascun messaggio in uscita deve consentire l'identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile.*
5. È fatto divieto di utilizzare le caselle di posta elettronica della Provincia di Teramo per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list, salvo che ciò non sia strumentale ad esigenze di lavoro o diversa ed esplicita autorizzazione da parte del proprio Dirigente o Responsabile del Settore non incardinato in Area.
4. È vietato l'invio di messaggi di posta elettronica, all'interno o all'esterno dell'amministrazione, che siano oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità dell'amministrazione.
5. È inoltre da evitare, ove possibile, l'invio di messaggi con allegati di grandi dimensioni al fine di evitare eventuali sovraccarichi al sistema informatico e nuocere all'efficacia della comunicazione.
6. È vietato inviare email con allegati i cui formati sono convenzionalmente ritenuti pericolosi (es. estensione .exe, .bat, etc.). I Sistemi Informativi dell'Ente potranno impostare attraverso sistemi hardware o software il blocco di invio o ricezione di tipologie di file ritenute pericolose o non attinenti all'attività istituzionale ai fini della protezione dei dati e dei sistemi informatici.
7. È vietato aderire a catene telematiche (o di S. Antonio) che richiedono la divulgazione e circolazione di messaggi di posta di carattere non lavorativo. Se si dovessero ricevere messaggi di tale tipo, si dovrà cancellare il messaggio ricevuto senza divulgarlo in alcun modo. Non si dovranno in alcun caso attivare gli allegati di tali messaggi.
8. Qualora si ricevessero messaggi sospetti di richiesta di password o altre informazioni oppure di invito a svolgere operazioni sulla propria postazione di lavoro (es. apertura o cancellazione di file, installazione aggiornamenti, apertura di una pagina web che richieda l'inserimento di credenziali, etc) di cui non è certa la provenienza, l'utente è tenuto a verificarli e, nel caso lo ritenga necessario per attività di prevenzione, a segnalarli immediatamente ai Sistemi Informativi dell'Ente prima di effettuare qualsiasi azione.
9. Al fine di garantire la continuità di servizio, sono previste 2 differenti modalità per la gestione delle assenze, programmate o non, degli operatori preposti alla lettura dei messaggi di una specifica casella di posta:

   a) ASSENZA PROGRAMMATA: attivazione da parte dell'utente di un risponditore automatico che segnali la temporanea indisponibilità all'accesso alla casella di posta, indicando eventualmente un indirizzo di posta alternativo a cui inviare il messaggio in caso di necessità di carattere professionale;

   b) ASSENZA NON PROGRAMMATA: in caso di necessità, su specifica richiesta da parte del responsabile dell'utente assente, quest'ultimo verrà contattato da un Amministratore di Sistema il quale gli chiederà l'esplicito permesso verbale di accesso alla casella di posta elettronica. A seguito di tale assenso, l'Amministratore di Sistema provvederà ad inoltrare al responsabile o ad un suo incaricato i messaggi di posta ritenuti necessari. In caso non sia stato

possibile raggiungere l'utente assente, il suo responsabile autorizzerà l'Amministratore di Sistema all'accesso alla casella di posta dell'utente assente, richiedendo l'inoltro dei messaggi ritenuti necessari. Al termine dell'operazione, l'Amministratore di Sistema redigerà un rapporto dell'intervento effettuato, indicando il nominativo di colui che ha autorizzato l'accesso. Il rapporto verrà inviato all'utente assente, al suo responsabile e ai Sistemi Informativi.

10. È vietato utilizzare client di posta elettronica differenti da quelli installati e configurati dall'Amministratore di Sistema, a meno che la cosa non sia stata preventivamente concordata con i Sistemi Informativi dell'Ente. L'apertura automatica dei messaggi di posta elettronica deve essere disattivata.
11. Gli Amministratori di Sistema, nell'espletamento delle loro funzioni, potranno accedere alle caselle di posta assegnate per finalità manutentive solo in presenza dell'assegnatario (o su sua esplicita autorizzazione) della casella o su richiesta del diretto superiore in caso di indisponibilità dell'assegnatario stesso.
12. Al termine del rapporto di servizio/collaborazione, sulle caselle di posta nominative verrà attivato un risponditore automatico che segnalerà la cessazione del rapporto e indicherà un indirizzo alternativo nel dominio della Provincia di Teramo da contattare in caso di necessità di carattere professionale. La casella non sarà oggetto di consultazione, salvo che sia espressamente richiesto per finalità di continuità di servizio dell'Ente: in tal caso l'accesso dovrà essere adeguatamente motivato ed espressamente autorizzato dal responsabile dell'utente e il trattamento effettuato dovrà essere documentato.
13. La casella di posta verrà chiusa definitivamente entro 3 mesi dalla cessazione del rapporto di servizio/collaborazione, per garantire che eventuali comunicazioni su rinnovi automatici di servizi associati alla casella vengano adeguatamente reindirizzati.
14. In caso di situazioni di contenzioso o di precontenzioso tra l'utente e la Provincia di Teramo, il contenuto della casella potrà essere conservato per tutta la durata del correlato procedimento, fino alla conclusione di tutti i gradi di giudizio.
15. La Provincia di Teramo può inviare agli indirizzi di posta elettronica personali dei dipendenti e dei collaboratori:
    - comunicazioni istituzionali e di servizio
    - buste paga;
    - CUD.
16. Il CRAL provinciale può inviare, agli indirizzi di posta elettronica personali dei soci, comunicazioni inerenti le proprie attività istituzionali, su richiesta ed esplicito consenso del dipendente ai sensi del D.lgs 196/2003 da manifestare nel modulo di adesione all'associazione.
17. In calce ad ogni e-mail inviata dalle caselle di posta elettronica personale o di Servizio potrà essere inserito dal sistema in maniera automatica del testo informativo relativo alle policies dell'Ente in materia di privacy;

ART. 14 - NAVIGAZIONE INTERNET

1. Per lo svolgimento delle proprie mansioni lavorative, è consentita la navigazione internet agli utenti.

2. La connessione ad Internet è uno strumento messo a disposizione per lavoro e comunque per finalità correlate all'attività della Provincia di Teramo: è consentita la navigazione per motivi diversi da quelli strettamente legati all'attività istituzionale a condizione che
   a) l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali;
   b) non sia contraria alle regole di condotta indicate nel presente Regolamento e non possa in alcun modo ledere l'immagine della Provincia di Teramo;
   c) non danneggi in alcun modo, diretto o indiretto, le proprietà della Provincia di Teramo;
   d) non comporti alcuna violazione di leggi;
   e) sia esplicito verso terzi che la responsabilità di qualsiasi operazione svolta per finalità personali sia imputabile esclusivamente all'utente.
3. Ogni utilizzo non inerente all'attività istituzionale può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

   Pertanto, per garantire quanto previsto dalla normativa vigente, presso il sistema informativo della Provincia di Teramo è attivo un filtro che blocca l'accesso ai siti ritenuti pericolosi per la sicurezza dei sistemi e dei dati personali.

   Il filtro adottato utilizzerà sistemi di scarto di siti facenti parte di categorie appositamente selezionate. Qualora, per lo svolgimento delle attività istituzionali, un utente necessitasse di accedere a un sito scartato dai sistemi di filtraggio, potrà richiedere l'autorizzazione ai Sistemi Informativi che provvederanno a consentirne l'accesso, se ritenuto opportuno all'abilitazione di navigazione.
4. È fatto assoluto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato dai siti internet, se non espressamente autorizzato dai Sistemi Informativi dell'Ente.
5. A fini statistici, di qualità del servizio e di sicurezza, l'occupazione di banda generata dal traffico internet e dallo scambio di posta elettronica è soggetta a periodiche verifiche e controlli da parte della Provincia di Teramo sotto forma di dati aggregati ed anonimi, in osservanza dei limiti posti dalla legge in materia di protezione dei dati personali.
6. Qualora i sistemi di sicurezza segnalino delle potenziali criticità che possano minare l'integrità dei dati e la stabilità del sistema stesso, potrebbero essere effettuati dei controlli sulla navigazione internet effettuata tramite la rete della Provincia di Teramo. Tali controlli si opereranno secondo stadi successivi:
   a) controlli generici sulle pagine visitate, senza che vengano tracciati gli utenti che le visitano;
   b) controlli aggregati sulle pagine visitate con suddivisione del traffico effettuato per aree lavorative;
   c) controlli specifici sulle pagine visitate, con tracciamento dell'indirizzo IP da cui si effettua la visita o dell'utente che la effettua.
7. I controlli aggregati e specifici verranno effettuati solo qualora i trattamenti generici non abbiano consentito di risolvere le criticità riscontrate e verranno comunque segnalati in forma preventiva agli utenti.
8. Tutti i dati di traffico internet sono comunque sottoposti a tracciamento da parte di sistemi automatici implementati presso la Provincia di Teramo e custoditi per limitati periodi di tempo. La consultazione e conservazione di tali dati, al di fuori dei casi indicati precedentemente, è consentita:

a) alla Provincia di Teramo stessa per attività difensive ovvero per far valere o difendere un diritto in sede giudiziaria. Qualsiasi trattamento verrà svolto dalla Provincia di Teramo nel rispetto della libertà e della dignità del lavoratore, in osservanza ai principi di pertinenza e non eccedenza;

b) alle forze dell'ordine per attività di carattere ispettivo consentite dalla normativa sulla protezione dei dati delle persone fisiche.

ART. 15 - SOCIAL NETWORK (SNS)

1. La Provincia di Teramo individua nell'utilizzo dei SNS un'occasione di comunicare con target di utenti spesso non raggiungibili con i servizi tradizionali; per offrire servizi di rete e servizi digitali in formula remota e per dialogare con le altre amministrazioni pubbliche presenti sui SNS.
2. I SNS rappresentano un utile strumento di multicanalità per informare e far partecipare i cittadini alla vita istituzionale dell'ente e possono rappresentare strumenti di e-democracy, ovvero luoghi virtuali di partecipazione e di espressione di necessità, opinioni ed interessi. L'accesso agli SNS attraverso le credenziali della Provincia, quindi è consentito a tutti i servizi con esigenze di front office e che gestiscono sportelli con l'utenza al fine di realizzare gli obiettivi dell'Agenda Digitale e dell'Agenda della Semplificazione.
3. Sarà cura dei Dirigenti di Area e dei responsabili dei Settori non incardinati in Area individuare i servizi che possono avere libero accesso ai SNS e individuare i dipendenti che, attraverso le credenziali rilasciate dal servizio/stampa/comunicazione/web, avranno anche la funzione di amministratori o editor.
4. La Provincia di Teramo, quindi, consente di utilizzare i SNS per finalità istituzionali, ed in particolare per:
   a) diffondere informazioni inerenti alle attività dell'Ente al fine di garantire la trasparenza;
   b) informare i cittadini sui servizi offerti e le relative modalità di fruizione;
   c) promuovere la condivisione di eventi ed iniziative organizzate dall'Ente, pubblicare sondaggi;
   d) creare nuovi spazi di dialogo con i cittadini e nuovi canali per raccogliere le loro opinioni e valutare la soddisfazione degli utenti su servizi ed attività istituzionali.
   e) confrontarsi con le altre amministrazioni dello Stato;
   f) attività di customer services sui servizi erogati.
5. La Provincia ha un proprio profilo pubblico identificabile come "Provincia di Teramo".
6. Il Presidente, su proposta del Dirigente competente, autorizza l'eventuale attivazione i nuovi profili pubblici riferiti a specifici servizi previo parere del Responsabile della Comunicazione che valuta la richiesta sulla base degli elementi di cui all'articolo precedente.
7. Il Dirigente richiedente incarica almeno due operatori alla gestione dei contenuti del profilo pubblico di SNS attivato. Gli operatori incaricati, a seconda dei meccanismi di accesso e gestione dello specifico SNS, possono accedere con il proprio account personale o, se ciò non è tecnicamente possibile, utilizzano congiuntamente le credenziali di accesso del profilo pubblico assegnate all'Ente dal SNS (es. cfr. Pagine Facebook vs Twitter).
8. Nel caso di un unico profilo pubblico di SNS gli operatori sono responsabili in solido della custodia delle credenziali di accesso.

9. Il Responsabile della Comunicazione effettua il monitoraggio dei contenuti pubblicati sui profili di SNS pubblici ed è autorizzato ad intervenire in caso di contenuti non congruenti.
10. Per quanto riguarda l'accesso ai profili personali dei dipendenti sui social network si rimanda a quanto previsto nel DPR n. 62/2013 e ss.mm.ii. e alle disposizioni presenti nel codice di comportamento integrativo e nel codice disciplinare della Provincia di Teramo.

ART. 16 - TRATTAMENTO DI DATI TRAMITE DISPOSITIVI DI PROPRIETÀ

1. È possibile utilizzare dispositivi di proprietà (Bring Your Own Device - BYOD) per trattare dati della Provincia di Teramo, solo se tale utilizzo è compatibile con le procedure di sicurezza previste nel contesto lavorativo e se preventivamente approvato dal rispettivo Responsabile. Sul dispositivo dovranno essere applicate le medesime misure di sicurezza in uso per gli strumenti aziendali.
2. Per garantire l'utilizzo in sicurezza di tali strumenti potranno essere previste specifiche procedure e istruzioni per l'uso ad integrazione del presente Regolamento.
3. Nel caso di utilizzo di dispositivi di proprietà e di acquisizione sugli stessi di dati personali trattati per conto del Titolare (es. immagini, fotografie, filmati, registrazioni audio, documenti, etc.) durante lo svolgimento di attività correlate alle funzioni svolte per conto del Titolare, gli utenti sono tenuti a rimuoverli tempestivamente dagli archivi del proprio dispositivo.
4. Qualora gli utenti consultino caselle di posta elettronica del Titolare tramite un dispositivo privato, è obbligatorio bloccare il dispositivo tramite sistemi di blocco schermo con protezione con password numerica, con segno grafico composto sullo schermo o tramite riconoscimento dell'impronta digitale.
5. In caso di smarrimento o furto di un dispositivo privato contenente dati personali trattati per conto della Provincia di Teramo, è necessario segnalare immediatamente l'accadimento al Servizio Sistemi Informativi dell'Ente, al fine di valutare eventuali azioni di mitigazione del danno.

ART. 17 - ACCESSO REMOTO ALLE RISORSE INFORMATICHE DELLA PROVINCIA DI TERAMO

1. Per lo svolgimento del lavoro a distanza (ad es. lavoro agile, telelavoro e Trasferta) potranno essere previste in appositi disciplinari, ad integrazione del presente Regolamento, una serie di misure di sicurezza, per assicurare la sicurezza dei dispositivi aziendali e delle Informazioni in essi gestite. Sono da considerarsi dispositivi aziendali solo i device registrati e gestiti dalla Provincia di Teramo.
2. All'utente che riceve dispositivi aziendali devono essere fornite indicazioni puntuali sui comportamenti da adottare per garantire la protezione e la sicurezza dell'asset e delle Informazioni in esso contenute da eventi quali il furto, lo smarrimento o l'utilizzo incauto o non conforme alle politiche di sicurezza aziendali. Per quanto concerne gli applicativi aziendali, devono essere accessibili solo tramite canali di comunicazione cifrati (ad es.: SSL VPN, IPSec VPN). Gli apparati forniti devono essere dotati di software di sicurezza aggiornati sistematicamente e regolarmente verificato. Il trattamento delle Informazioni aziendali da parte degli utenti deve essere ammesso solo su software licenziato dall'azienda e la navigazione via Internet deve essere effettuata utilizzando solo reti sicure, evitando l'utilizzo di reti aperte o gratuite.

ART. 18 - UTILIZZO DELLA RETE LAN E DELLE RISORSE CONDIVISE

1. Al fine di garantire la disponibilità dei dati e un'efficace politica di backup, gli utenti che operano con postazioni fisse collegate alla LAN della Provincia di Teramo devono salvare su cartelle di rete sincronizzate con il cloud privato utilizzato dall'Ente (Nextcloud, rif. art. 20), tutti i file di lavoro ed astenersi dal salvarli sul disco locale della postazione informatica (si specifica che la cartella "desktop" si trova sulla postazione in locale, pertanto è inadatta al salvataggio dei file perché non sottoposta a procedure di backup).
2. Lo spazio di condivisione su file server presso la server farm o cloud assegnato all'utente viene configurato con una capienza massima prestabilita uguale per tutti i dipendenti, ad eccezione delle cartelle destinate a gruppi di lavoro. In casi particolare e dietro specifica richiesta del responsabile del servizio potrà essere aumentata la quantità di spazio assegnato.
3. Le cartelle/unità di rete sono aree di condivisione di dati strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto nessun file che non sia legato all'attività lavorativa può essere dislocato, nemmeno per brevi periodi, in queste unità.
4. I file e i documenti di lavoro devono essere obbligatoriamente memorizzati nello spazio di condivisione apposito al fine di impedire la perdita di dati aziendali, a seguito di guasti alle PdL.
5. In caso di comprovato pericolo per la sicurezza dei sistemi, la Provincia potrà procedere anche senza preavviso alla rimozione di file e/o applicazioni presenti negli spazi di condivisione degli Utenti, dandone successiva e tempestiva comunicazione agli interessati.
6. Le credenziali di ingresso alla rete ed ai programmi sono personali: è assolutamente vietato entrare nella rete e nei programmi con credenziali assegnate ad altri utenti.
7. L'Amministratore di Sistema, nell'espletamento delle mansioni attribuitegli per l'esercizio delle proprie attività, può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere potenzialmente pericoloso per la sicurezza, sia sulle postazioni di lavoro sia sui server.
8. Per la condivisione di file all'interno della Provincia di Teramo è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati oppure è possibile utilizzare le funzionalità di condivisione dell'accesso in sola lettura o in lettura / scrittura offerte dalla piattaforma di cloud privato (Nextcloud). Le cartelle di rete devono essere tenute in ordine, eliminando i file non più necessari anche al fine di non consentire il trattamento dei dati da parte di persone non espressamente autorizzate.
9. È consentito il collegamento alla rete interna di personal computer portatili o di attrezzature informatiche non di proprietà della Provincia di Teramo, solo se preventivamente autorizzati dal Servizio Sistemi Informativi e secondo quanto disciplinato dal presente Regolamento.

ART. 19 - UTILIZZO DI PIATTAFORME IN CLOUD DI FILE SHARING

1. L'Ente si è dotata di una piattaforma di cloud privato opensource raggiungibile dagli utenti sia come cartella di rete sui pc aziendali, sia tramite servizio web per l'accesso dall'esterno della rete aziendale; la soluzione individuata offre tutte le principali funzionalità disponibili sulle piattaforme più diffuse di cloud (es. Dropbox, Google Drive, Microsoft OneDrive, Apple iCloud) e pertanto utilizzare un servizio alternativo di cloud computing per memorizzare dati personali o sensibili, espone l'Ente a potenziali problemi di violazione delle regole sulla riservatezza dei dati personali.
2. È vietato agli Utenti l'utilizzo di sistemi cloud non espressamente approvati dall'Ente, in particolare è vietato condividere o registrare su sistemi cloud dati particolari ai sensi del Regolamento UE 679/2016 (GDPR).

3. L'Ente, tramite il Sevizio Sistemi Informativi, si riserva di identificare tecnologie e/o servizi cloud conformi alla normativa in materia di trattamento dei dati personali da mettere a disposizione degli Utenti.
4. Gli spazi di condivisione file server o cloud, devono essere utilizzati per la memorizzazione dei file ad uso strettamente lavorativo. Per la sicurezza dei sistemi, il Servizio Sistemi Informativi potrà procedere anche senza preavviso alla rimozione di file e/o applicazioni, dandone successiva e tempestiva comunicazione agli utenti.
5. Non è consentito fare uso di software di file sharing non preventivamente autorizzati dal Servizio Sistemi Informativi.

   A tal fine è vietato:

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

ART. 20 - ACQUISIZIONE SOFTWARE

1. Sulle postazioni è consentita l'installazione esclusivamente delle seguenti categorie di software:

   a) software commerciale dotato di licenza d'uso (es. pacchetti di Office Automation);

   b) software gestionale acquisito specificatamente dalla Provincia di Teramo per lo svolgimento delle proprie mansioni lavorative (es. applicativi in uso ai vari servizi);

   c) software gratuito (freeware) e shareware prelevato dai siti internet, solo se espressamente autorizzato dai Sistemi Informativi della Provincia di Teramo;

   d) qualsiasi altro software si renda necessario per l'esercizio delle attività lavorative, provvisto di una licenza non in contrasto con la normativa sul diritto d'autore ed a seguito di autorizzazione da parte dei Sistemi Informativi.

2. I Sistemi Informativi della Provincia di Teramo elaborano e mantengono un documento chiamato "Configurazione standard delle postazione di lavoro" in cui sono indicati gli specifici software autorizzati e definiti come base per le postazioni di lavoro. Ogni ulteriore necessità dovrà essere valutata con i Sistemi Informativi al fine di individuare la soluzione applicativa che soddisfi le esigenze di attività lavorativa e non comprometta la sicurezza del sistema informatico e dei dati.
3. L'acquisto e la conseguente installazione di software devono essere sempre preventivamente valutati, autorizzati ed effettuati in collaborazione con i Sistemi Informativi della Provincia di Teramo, al fine di garantire la stabilità dei sistemi presenti e la compatibilità del software con gli stessi.

ART. 21 - UTILIZZO DI STAMPANTI, MULTIFUNZIONI E FAX-SERVER

1. È vietato l'utilizzo delle stampanti, delle fotocopiatrici (MF) e dei Fax aziendali per fini personali. La stampa di documenti informatici dovrà essere limitata ai casi per cui esiste l'assoluta necessità di disporre della copia cartacea. Il materiale stampato deve essere immediatamente prelevato per evitare che possa essere visionato da personale non autorizzato.
2. Nella trasmissione di documenti tra le pubbliche amministrazioni è vietato l'utilizzo del Fax o del Fax Server (d.lgs. 82/2005 e ss.mm.ii: l'inosservanza della disposizione, ferma restando l'eventuale responsabilità per danno erariale, comporta responsabilità dirigenziale e responsabilità disciplinare).
3. Nelle stampanti multifunzione (MF), la scansione dei documenti potrebbe venir configurata come "scan-to-mail" - invio del documento digitalizzato ad una casella di posta - e/o "scan-to-disk" - salvataggio delle scansioni su una cartella locale della multifunzione o su cartella di rete. Nell'utilizzo in modalità "scan-to-mail" non è consentito l'invio di scansioni dalla multifunzione verso e-mail non aziendali: in tali casi è necessario inoltrare il documento alla propria e-mail istituzionale – per verificarne il contenuto - e solo successivamente, utilizzando la propria casella e-mail, inoltrare l'allegato al destinatario.

ART. 22 - DISPOSITIVI CON IMPATTO SUI SISTEMI INFORMATICI

1. La messa in opera di qualsiasi dispositivo o strumento che interagisca con la rete e/o la strumentazione informatica della Provincia di Teramo o possa avere un impatto con essi, qualora non venga eseguita direttamente dai Sistemi Informativi della Provincia di Teramo, deve essere concordata preventivamente con questi, onde evitare malfunzionamenti, inadeguatezze prestazionali o altri problemi alla sicurezza e all'immagine della Provincia stessa.
2. Qualora nell'esercizio di attività istituzionali sia prevista la fornitura di software accessorio, l'area competente provvede a consultare i Sistemi Informativi dell'Ente nelle fasi preliminari del processo di acquisizione per la corretta definizione delle caratteristiche del software, al fine della verifica che esso risulti:
   a) compatibile con il sistema informatico preesistente,
   b) conforme alle misure di sicurezza adottate dalla Provincia di Teramo con particolare riguardo alla sicurezza degli accessi logici,
   c) certificato per l'installazione sulle macchine in dotazione (server e postazioni di lavoro),
   d) installato correttamente.
3. In caso di mancata consultazione preventiva dei Sistemi Informativi della Provincia di Teramo non verrà effettuata alcuna installazione.
4. Qualora venga affidata all'esterno la gestione di dati della Provincia di Teramo per l'erogazione di servizi, l'ufficio competente deve concordare preventivamente con i Sistemi Informativi dell'Ente le modalità e i formati con cui questi dati devono essere scambiati, sia in ingresso che in uscita, e le condizioni di consegna dei dati al termine del rapporto di collaborazione.

ART. 23 - ATTIVITÀ DI BACKUP DEI DATI UTENTE

1. Sono oggetto di attività di salvataggio centralizzato:
   a. i file salvati sulle cartelle/unità di rete messe a disposizione dai Sistemi Informativi della Provincia di Teramosecondo le politiche di backup definite a livello organizzativo;

b. le banche dati di applicativi ed i relativi file di sistema in uso per funzioni istituzionali, secondo le politiche di sicurezza definite;

c. il contenuto delle caselle di posta elettronica gestite all'interno della piattaforma utilizzata dalla Provincia di Teramo, secondo le politiche di backup definite a livello organizzativo;

2. I dati che risiedono sulle postazioni di lavoro non sono soggetti a operazioni di backup centralizzato.

ART. 24 - ATTIVITÀ E STRUMENTI DI ASSISTENZA REMOTA

1. Gli Utenti possono far pervenire richieste di assistenza e segnalazioni di malfunzionamento dei computer e della rete inviando una email a assistenza@provincia.teramo.it o compilando un form web all'indirizzo login.provincia.teramo.it
2. Ad ogni richiesta o segnalazione il Servizio Informatico attribuisce un codice di priorità.
3. Gli interventi sono organizzati sulla base del livello di priorità attribuito e sono espletati dal Responsabile del sistema informatico o da suoi collaboratori appositamente autorizzati.
4. Per finalità di carattere manutentivo sono utilizzati sui dispositivi in dotazione strumenti di assistenza remota che consentono agli Amministratori di Sistema di connettersi alle postazioni degli utenti per fornire supporto in tempo reale e assistere gli utenti nella risoluzione di problematiche di carattere informatico.
5. Gli strumenti utilizzati manifestano esplicitamente la connessione alla postazione da parte dell'Amministratore: l'utente dovrà consentire tramite autorizzazione verbale o informatica l'intervento remoto.
6. Qualora sia necessario consentire l'accesso e/o il controllo remoto da parte di soggetti esterni alla Provincia di Teramo per attività di carattere professionale, questo può essere fatto solo previa verifica dell'identità del soggetto che si connette alla risorsa e dell'effettiva necessità. Le attività effettuate da remoto devono essere monitorate durante il loro svolgimento da parte dell'utente assegnatario della macchina.

ART. 25 - DISMISSIONE DI DISPOSITIVI O SUPPORTI

1. In caso di necessità di dismissione di un dispositivo, lo stesso dovrà essere preso in carico dal Servizio Sistemi Informativi dell'Ente, che si occuperà di effettuare una dismissione sicura dello strumento rendendo illeggibili i dati contenuti e dismettendolo nella maniera corretta.
2. In caso di dismissione di supporti di memorizzazione (es DVD, chiavette USB o hard disk esterni, questi potranno essere consegnati al Servizio Sistemi Informativi dell'Ente o dismessi direttamente dall'utente assegnatario effettuando una dismissione sicura che garantisca l'illeggibilità dei dati precedentemente custoditi e l'eventuale distruzione del supporto.
3. Nel caso di riutilizzo di un dispositivo, i Sistemi Informativi effettueranno la cancellazione dei dati precedentemente presenti prima di metterlo a disposizione per il nuovo utilizzo.

ART. 26 - SICUREZZA GENERALE E PERIMETRALE

1. All'interno dell'infrastruttura tecnologica è attivato un sistema di sicurezza perimetrale a difesa dei sistemi e dei dati, che traccia eventi che possono essere indizio di minacce informatiche. Il sistema è soggetto a procedure di aggiornamento automatico per quanto riguarda la lista e le caratteristiche delle minacce.
2. Il sistema è gestito da soggetti debitamente designati dalla Provincia di Teramo, i quali effettuano attività di verifica delle segnalazioni attivate dal sistema stesso, con lo scopo di comprendere e prevenire eventuali minacce esterne.
3. Qualora il sistema attivato rilevi delle minacce a specifici indirizzi IP interni delle postazioni di lavoro, i Sistemi Informativi dell'Ente verificheranno le cause della minaccia rilevata insieme all'utente/utenti che abitualmente utilizza/utilizzano la postazione, con l'obiettivo di comprendere la natura dell'intrusione e prevenire eventuali danni.
4. Una volta individuate le cause dell'evento rilevato verranno adottati provvedimenti correttivi, con segnalazione al Titolare dei trattamenti di eventuali violazioni alle regole indicate nel presente Regolamento.
5. Il sistema informatico ed i PC collegati alla rete aziendale sono protetti da software antivirus aggiornati quotidianamente.
6. Ogni Utente è comunque tenuto a comportarsi in modo responsabile tale da ridurre il rischio di attacco al sistema informatico aziendale da parte di virus o qualsiasi altro software "aggressivo". Le stesse regole dovranno essere rispettate da parte di Soggetti terzi fornitori/gestori di apparecchiature e servizi informatici che vengono utilizzati a qualsiasi titolo all'interno della rete aziendale.

ART. 27 - CONTROLLI

1. Le risorse informatiche e digitali messe a disposizione degli utenti sono strumenti attraverso i quali vengono perseguiti gli obiettivi istituzionali e sugli stessi la Provincia di Teramo gode di diritti esclusivi di proprietà e utilizzo.
2. Il Titolare ha diritto di ottenere una corretta prestazione lavorativa e di attuare misure di sicurezza idonee alla difesa del patrimonio informativo.
3. Sulle risorse messe a disposizione possono essere effettuati dei controlli, con le seguenti finalità:
    a. difendere il patrimonio della Provincia di Teramo;
    b. far valere o difendere un diritto in sede giudiziaria;
    c. tutelare gli interessi dei soggetti terzi che la Provincia di Teramo è tenuta a salvaguardare nel perseguimento delle proprie attività istituzionali.
4. A questi fini, è prevista la possibile attuazione dei seguenti controlli:
    a. verifica di file e programmi presenti sui dispositivi che possano contravvenire le indicazioni specificate nel presente Regolamento, con la finalità di prevenire eventuali reati;
    b. controllo dei sistemi di accesso internet e di sicurezza perimetrale in caso di minacce segnalate dai sistemi di sicurezza o di lentezza di banda, con il fine di garantire il buon funzionamento della rete della Provincia di Teramo. Il controllo potrà riguardare l'occupazione di banda, l'utilizzo di sistemi di file sharing o la verifica di minacce segnalate dai sistemi di sicurezza;
    c. controllo della navigazione internet al fine di prevenzione di possibili minacce che possano compromettere la sicurezza dei sistemi informativi della Provincia di Teramo. Il controllo verrà effettuato a seguito della rilevazione di eventi non conformi agli standard di buon funzionamento, e verrà effettuato con profondità graduale come specificato nel precedente articolo.
    d. accesso alla casella di posta degli utenti in caso di loro assenza e di necessità di dovervi accedere per motivi di continuità dell'attività lavorativa della Provincia di Teramo. In caso di accesso alla casella di posta, verrà redatto un apposito rapporto di intervento in cui verranno specificate le azioni intraprese, che verrà consegnato all'utente al termine del periodo di assenza;
    e. analisi dei dispositivi mobili messi a disposizione per attività di tipo professionale, con finalità di controllo della spesa e protezione dei dati ivi presenti. Le modalità di controllo sono specificate nei precedenti articoli 10 e 11 del presente Regolamento, relativi ai dispositivi mobili in dotazione e alla telefonia mobile;
    f. controllo dell'esito dei backup effettuati sui sistemi server della Provincia di Teramo, con la finalità di garantire l'eventuale ripristino di dati o documenti in caso di necessità. Le verifiche potrebbero riguardare il controllo dell'esito dei backup o il ripristino casuale di un dato durante le fasi di test di ripristino effettuate per esaminare il buon funzionamento del sistema;
    g. controllo della messa in sicurezza dei dati lavorativi residenti sui dispositivi dati in uso, con la finalità di garantire la riservatezza e la disponibilità dei dati della Provincia di Teramo. Tale controllo riguarderà la verifica della localizzazione dei dati in spazi logici protetti e di misure di backup.
5. Qualsiasi controllo verrà effettuato nel rispetto della libertà e delle dignità dei lavoratori. Eventuali dati privati rilevati saranno trattati nel rispetto dei principi di pertinenza e non eccedenza.

6. Qualora da tali controlli si rilevassero dei comportamenti non conformi rispetto a quanto indicato nel presente Regolamento e/o rispetto alle misure di sicurezza definite, la Provincia di Teramo si riserva di intraprendere provvedimenti disciplinari.
7. A seguito di eventi che abbiano comportato un danneggiamento del patrimonio di proprietà della Provincia di Teramo, qualora emergano degli elementi che possano fondatamente evidenziare degli atteggiamenti inadeguati potenziale causa dei danni rilevati, l'Ente ha diritto di attuare controlli difensivi occulti con la finalità tutelare le risorse in uso, se da essi fosse possibile riscontrare e sanzionare un comportamento improprio da parte degli utenti.

ART. 28 - SISTEMI DI MONITORAGGIO ATTIVO DEI DISPOSITIVI E DEL SOFTWARE

1. I dispositivi elettronici tracciano una serie di eventi di sistema per attività amministrative, manutentive e/o di sicurezza, che variano a seconda della tipologia dei dispositivi stessi.
2. Sono attivi specifici sistemi di monitoraggio su apparecchiature di rete, server, personal computer, notebook, che permettono di ottenere informazioni sui sistemi e sul traffico generato dagli stessi, al fine di monitorare il corretto funzionamento di tutto il sistema informativo, prevenire e correggere eventuali disfunzioni.
3. Tali sistemi effettuano il monitoraggio in maniera automatica e senza richiedere il consenso agli utenti delle postazioni monitorate.
4. Esempi di tali tipologie di monitoraggio sono:
   - Rilevazione e inventario dispositivi hardware utilizzati
   - Rilevazione e inventario dei software presenti sui dispositivi
   - Analisi del software presente sui dispositivi non compreso nell'elenco dei software autorizzati
   - Monitoraggio ed alert in caso di anomalie del traffico di rete interna e del funzionamento delle postazioni di lavoro
   - Installazione automatica sulle postazioni di lavoro di applicazioni ed aggiornamenti
   - Filtraggio dei messaggi di posta elettronica con sistemi antispam o similari
   - Filtraggio dei messaggi di posta elettronica per blocco tipologie di file ritenute pericolose
   - Analisi dei contenuti del traffico web per filtraggio tipologie di file ritenute pericolose
   - Blocco di esecuzione di file ed applicativi ritenuti pericolosi attraverso il sistema di antivirus
   - Raccolta log di sistemi operativi, applicativi, utility, sistemi di protezione
   - Filtraggio e blocco siti web ritenuti non adeguati
   - Filtraggio e segnalazione trasferimenti di files criptati non previsti
   - Analisi ed identificazione delle vulnerabilità e dei sistemi
   - Discovery di sistemi e attività che possano ledere la sicurezza delle risorse
   - Tracciamento dati contabili relativi al traffico telefonico ed internet di smartphone e tablet.
5. I Sistemi Informativi potranno impostare attraverso sistemi hardware o software il blocco di invio o ricezione di tipologie di file ritenute pericolose ai fini della protezione dei dati e dei sistemi informatici.
6. Per quanto riguarda i controlli che potrebbero essere svolti sulla navigazione internet degli utenti si rimanda al precedente articolo.
7. I sistemi di protezione degli Endpoint (ovvero delle postazioni di lavoro) e di sicurezza perimetrale (protezione del perimetro interno/esterno della rete), allo scopo di permettere la configurazione delle politiche di sicurezza dei sistemi, possono raccogliere dati relativi alle minacce informatiche

rilevate sui sistemi e sulle postazioni di lavoro inviando gli stessi a sistemi centralizzati per l'analisi delle minacce informatiche.

ART. 29 - GESTIONE CHIAVI E ALTRI STRUMENTI DI ACCESSO FISICO

1. Per lo svolgimento delle proprie attività correlate con le finalità perseguite dalla Provincia di Teramo, gli utenti possono essere dotati di chiavi o altri strumenti di accesso fisico (smartcard, chiavi RFID, codici alfanumerici) a risorse istituzionali.
2. Gli utenti sono tenuti ad utilizzare tali strumenti con la massima cautela, garantendone la messa in sicurezza. Tali strumenti non devono essere lasciati incustoditi in zone a libero accesso, al fine di ridurre il rischio di furti. In caso di trasferte, non devono essere lasciati in macchina, nemmeno per brevi periodi, in parcheggi pubblici o comunque zone non custodite.
3. Qualora tali strumenti dovessero essere smarriti o rubati, l'affidatario deve immediatamente segnalare l'evento ai Sistemi Informativi, al fine di approntare le necessarie misure di mitigazione del danno.

ART. 30 - GESTIONE DOCUMENTI CARTACEI

1. La scrivania e i tavoli di lavoro non devono mostrare in chiaro dati personali di cui possano venire a conoscenza visitatori occasionali. I documenti devono essere sempre presidiati o messi in sicurezza.
2. I dati trattati devono essere custoditi in luoghi non accessibili a soggetti non autorizzati. La custodia in sicurezza può essere garantita attraverso la chiusura di armadi e/o interi locali.
3. È necessario procedere all'archiviazione definitiva, nei luoghi predisposti, dei supporti cartacei e dei supporti elettronici una volta terminate le attività di consultazione ed elaborazione.
4. I documenti cartacei non più utilizzati e non necessari devono essere eliminati con macchine distruggi-documenti o ridotti a "micro frammenti" che non rendano possibile la ricostruzione delle informazioni contenute.
5. Gli utenti dovranno effettuare la stampa dei dati solo se strettamente necessaria e dovranno ritirarla prontamente dai vassoi delle stampanti nel caso di utilizzo di stampanti condivise.

ART. 31 - RAPPORTO CON SOGGETTI TERZI

1. È vietato fornire tramite email, fax, accesso remoto o telefonicamente dati, credenziali o accessi ai sistemi senza specifica e preventiva identificazione del richiedente e conseguente autorizzazione da parte del proprio Responsabile.
2. In ogni caso, prima di rilasciare documenti, dati o credenziali a soggetti terzi, è obbligatorio verificare l'identità dei destinatari e la presenza di adeguate motivazioni ed autorizzazioni al rilascio.
3. Qualora le informazioni e le risorse vengano trattate in nome e per conto di soggetti terzi (Titolari del trattamento), per cui la Provincia di Teramo agisca in qualità di Responsabile ai sensi dell'art. 28 GDPR, il personale dell'Ente dovrà concordare con il referente del Titolare le azioni da intraprendere.

ART. 32 - INCIDENTI DI SICUREZZA E DATA BREACH

1. Un qualsiasi incidente, occorso su dati informatici, cartacei o credenziali di accesso, può compromettere la sicurezza dei dati personali e in generale delle informazioni.
2. In caso di particolare gravità, l'incidente può comportare una vera e propria violazione, denominata *data breach*, che è obbligatorio notificare all'Autorità Garante per la protezione dei dati personali ai sensi dell'art. 33 del GDPR.
3. Si intende per data breach (in elencazione solo esemplificativa e non esaustiva):
   a) Distruzione (dati non più disponibili)
   b) Perdita (dati non disponibili per il Titolare ma probabilmente in possesso di altri soggetti)
   c) Modifica (senza possibilità di ripristino)
   d) Divulgazione non autorizzata
   e) Accesso non autorizzato
   f) Indisponibilità temporanea del dato
4. Qualora si riscontri un incidente di sicurezza sulle risorse messe a disposizione dalla Provincia di Teramo è necessario comunicarlo immediatamente al proprio Responsabile e contattare il Responsabile Protezione dati scrivendo a rpd@provincia.teramo.it - documentando l'accaduto - al fine di approntare prontamente adeguate misure di mitigazione del danno. Per disciplinare le procedure di gestione degli incidenti, potranno essere previste specifiche procedure ad integrazione del presente Regolamento.

ART. 33 - OBBLIGO DI RISPETTO DEL PRESENTE REGOLAMENTO

1. Il rispetto del presente Regolamento è un obbligo per tutti coloro che utilizzano le risorse della Provincia di Teramo, in quanto rappresenta una garanzia di corretta gestione della sicurezza dei sistemi e dei dati personali.
2. Il mancato rispetto delle regole e delle misure di sicurezza elencate nel presente Regolamento implica la responsabilità personale dell'utente e costituisce una violazione, che potrà avere conseguenze di natura disciplinare o contrattuale – oltre che di potenziale rilevanza amministrativa o penale - in relazione e rapporto alla gravità del comportamento e dei potenziali rischi per il sistema e per i dati personali.
3. Nel caso in cui si riscontrino delle criticità che possano ledere la sicurezza del sistema informativo, la Provincia di Teramo potrà effettuare verifiche sull'utilizzo delle risorse strumentali concesse in dotazione agli utenti in conformità alle indicazioni riportate nel presente Regolamento. Qualora l'utilizzo delle risorse fornite in dotazione possa rivelare dati personali relativi agli utilizzatori, la rilevazione verrà effettuata secondo i principi di pertinenza e non eccedenza del trattamento dei dati rispetto alle finalità di sicurezza per cui tali dati sono trattati.

ART. 34 - OSSERVANZA DELLE REGOLE RELATIVE ALLA NORMATIVA IN TEMA DI PROTEZIONE DEI DATI PERSONALI E AGLI STANDARD DI SICUREZZA DELL'ORGANIZZAZIONE

1. Oltre a quanto indicato nel presente Regolamento è obbligatorio per ogni utente tenere comportamenti conformi alla normativa vigente in tema di protezione dei dati personali e relativa regolamentazione in essere nella Provincia di Teramo.

2. In particolare gli utenti, nei contesti operativi di propria competenza, sono tenuti a fare quanto nelle loro possibilità per l'adozione di adeguate misure di sicurezza, ai sensi dell'art. 32 del GDPR.
3. Qualora, nell'ambito delle proprie attività lavorative, un soggetto riscontri che il trattamento di dati effettuato possa contravvenire alle prescrizioni del GDPR o del D. Lgs. 196/2003, è tenuto ad informarne tempestivamente il proprio Responsabile e i Sistemi Informativi dell'Ente, al fine di concordare ed intraprendere i necessari interventi di adeguamento e eventuale mitigazione del rischio.
4. Ogni utente deve improntare le proprie attività al rispetto della massima riservatezza sulle informazioni di cui abbia conoscenza per motivi istituzionali o conoscenza incidentale.
5. L'impegno alla riservatezza dovrà essere osservato anche a seguito di modifica dell'incarico e/o cessazione del rapporto di lavoro.

ART. 35 - ENTRATA IN VIGORE E AGGIORNAMENTI SUCCESSIVI

1. Il presente Regolamento è in vigore a partire dalla data di esecutività della relativa deliberazione di approvazione.
2. Dal momento di entrata in vigore del presente regolamento è abrogato il "Regolamento sull'utilizzo degli strumenti informatici" approvato con deliberazione del Presidente della Provincia n. 388 del 12/10/2015.
3. Dal momento di entrata in vigore del presente regolamento sono altresì abrogate tutte le altre disposizioni in essere comunque in contrasto con lo stesso.
4. Le disposizioni contenute nel presente Regolamento possono essere soggette ad aggiornamenti, integrazioni e/o correzioni, ogni volta che se ne ravvisi la necessità, in relazione all'evolversi della tecnologia, all'entrata in vigore di sopravvenute disposizioni di legge o al modificarsi delle esigenze dell'Amministrazione.