PROVINCIA
DI TERAMO

REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI

Indice generale

Capo I Ambito di applicazione....5
Art. 1 - Oggetto del documento ed ambito di applicazione....5
Art. 2 - Definizioni....5
Art. 3 - Principi generali....6
Art. 4 - Ambito di applicazione....7
Art. 5 - Titolarità....7
Art. 6 - Competenze e responsabilità....8
Capo II Gestione delle credenziali di autenticazione e autorizzazione....10
Art. 7 - Attribuzione delle credenziali....10
Art. 8 - Caratteristiche delle password....10
Art. 9 - Scadenza delle password....10
Art. 10 - Perdita della segretezza....11
Art. 11 - Disattivazione delle credenziali....11
Art. 12 - Accesso al sistema informatico della Provincia da parte di Utenti autorizzati. .11
Art. 13 - Violazioni....11
Capo III Uso del personal computer....12
Art. 14 - Il Personal Computer....12
Art. 15 - Utilizzo del Personal Computer da parte degli Operatori....12
Art. 16 - Help desk e assistenza remota....13
Art. 17 - Accesso alle cartelle di lavoro dell'Operatore....13
Art. 18 - Acquisizione ed installazione degli strumenti informatici e telematici....13
Art. 19 - Creazione di programmi o documenti automatizzati....14
Art. 20 - Supporti e dispositivi informatici per la memorizzazione....14
Art. 21 - Dispositivi di comunicazione....14
Art. 22 - Allontanamento momentaneo dalla postazione di lavoro....14
Art. 23 - Controlli....15
Art. 24 - Cartella per il salvataggio dei Documenti....15
Art. 25 - Utilizzo di PC portatili e/o accessori temporaneamente assegnati....15
Art. 26 - Protezione e aggiornamento software dei pc....15
Art. 27 - Utilizzo personale....15
Capo IV Posta Elettronica Certificata....16
Art. 28 - PEC Istituzionale....16
Art. 29 - Attivazione PEC per Settori e Servizi....16
Capo V Uso della posta elettronica....17
Art. 30 - Informazioni Generali....17

Art. 31 - Attivazione del servizio.....17
Art. 32 - Gestione delle credenziali di accesso.....18
Art. 33 - Accesso alla casella personale in caso di assenza del titolare.....18
Art. 34 - Accesso alla casella di posta elettronica personale dei Dirigenti e degli Amministratori in caso di assenza del titolare.....18
Art. 35 - Utilizzo degli indirizzi da parte dell'Ente.....18
Art. 36 - Utilizzo da parte del CRAL e della RSU.....19
Art. 37 - Utilizzo delle caselle di posta elettronica da parte dei dipendenti e dei collaboratori.....19
Art. 38 - Contenuto delle Comunicazioni.....19
Art. 39 - Comunicazioni da e verso l'esterno.....20
Art. 40 - Avvisi in calce alle e-mail.....20
Art. 41 - Comunicazioni personali.....20
Capo VI Firme Digitali.....21
Art. 42 - Soggetti abilitati.....21
Art. 43 - Definizione dei Ruoli.....21
Art. 44 - Tipo di utilizzo.....22
Art. 45 - Presentazione telematica di istanze e dichiarazioni.....22
Art. 46 - Compiti e responsabilità degli incaricati di firma.....22
Art. 47 - Obblighi del titolare.....23
Art. 48 - Procedure di attribuzione / identificazione.....23
Art. 49 - Causa di revoca e di sospensione.....24
Art. 50 - Procedura di revoca e di sospensione.....24
Capo VII Intranet ed internet.....25
Art. 51 - Orario di accesso alla rete.....25
Art. 52 - Risorse condivise.....25
Art. 53 - Collegamento alla Rete.....26
Art. 54 - Internet.....26
Art. 55 - Chat.....26
Art. 56 - Responsabilità nella navigazione web.....26
Art. 57 - Filtri web.....26
Art. 58 - E-Learning.....27
Art. 59 - Divieti di navigazione.....27
Art. 60 - Utilizzo dei SNS per fini istituzionali.....28
Art. 61 - Comunicazione istituzionale mediante i SNS.....29
Art. 62 - Attivazione di nuovi profili SNS dell'Ente.....29
Capo VIII Altri strumenti stampanti, fax e fotocopiatrici.....30

Art. 63 - Utilizzo Stampanti.....30
Art. 64 - Telefoni fissi.....30
Capo IX Monitoraggi e controlli.....30
Art. 65 - Principi generali.....30
Art. 66 - Monitoraggi.....30
Art. 67 - Controlli.....31
Capo X Sanzioni.....33
Art. 68 - Sanzioni.....33
Capo XI Disposizioni finali.....33
Art. 69 - Aggiornamento e revisione.....33

Capo I
Ambito di applicazione

Art. 1 - Oggetto del documento ed ambito di applicazione

1. Il presente regolamento definisce le condizioni di utilizzo del Sistema Informatico e Digitale da parte degli Operatori della Provincia di Teramo (così come individuati nell'art. 2 lett. d) e g)), attraverso gli strumenti messi a disposizione dall'ente per il pieno ed efficace svolgimento delle attività proprie dell'amministrazione e dei servizi ad esse correlati.

2. Il Sistema Informatico e digitale risponde ad usi ed obiettivi pubblici ed istituzionali e a tali scopi deve essere orientato il comportamento dell'Operatore che lo utilizza. L'utilizzo del Sistema è costantemente monitorato, nel rispetto della normativa sulla privacy e delle norme a tutela del lavoratore. L'uso improprio del Sistema è sanzionato.

3. L'Utilizzo dei servizi e degli strumenti predisposti nell'ambito del Sistema informatico della Provincia è consentito solo nel pieno rispetto del presente Regolamento.

Art. 2 - Definizioni

1. Ai fini dell'applicazione del presente Regolamento deve intendersi:

a) per Sistema Informatico della Provincia di Teramo di seguito denominato SITer: l'insieme coordinato dell'infrastruttura di rete telematica e degli apparati, elaboratori, software, archivi dati e/o risorse informative a qualsiasi titolo archiviate in modo digitale, in dotazione ed uso all'Amministrazione Provinciale di Teramo.

b) per Responsabile del Sistema Informatico: il soggetto responsabile del Servizio Informatico della Provincia di Teramo.

c) per 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.

d) per 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.

e) per Amministratori: il Presidente, i Consiglieri e i consiglieri delegati;

f) per Utenti della Provincia di Teramo: i soggetti pubblici ed privati che hanno con la Provincia di Teramo rapporti diversi dagli operatori del Sistema Informatico di cui alla lettera d).

g) per Utenti autorizzati: gli utenti esterni della Provincia di Teramo, così come definiti nel punto precedente, espressamente autorizzati dal Responsabile del Servizio Informatico ad accedere e utilizzare i sistemi informatici e telematici della Provincia di Teramo.

h) per 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.

i) per 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.

j) per Casella di posta elettronica istituzionale: la casella di posta elettronica certificata dell'ente, del Settore, del Servizio o dell'Ufficio.

k) per Cartelle di lavoro dell'Utente: le cartelle (directories) dell'ambiente di lavoro virtuale (desktop) dell'Utente.

l) per Cartella personale dell'Utente: la cartella denominata "personale" contenuta nell'ambiente di lavoro virtuale (desktop) dell'Utente in cui sono memorizzati informazioni personali o dati personali dell'Utente non attinenti all'attività lavorativa.

m) per Comunicazioni interne: le comunicazioni tra gli Utenti del Sistema Informatico di cui alla lettera d)

n) per Comunicazioni esterne: le comunicazioni verso Utenti della Provincia.

o) per Archivio di rete: le cartelle condivise in rete per la memorizzazione di informazioni in formato digitale a scopo esclusivamente lavorativo.

p) per Smartphone: il dispositivo portatile che abbina funzionalità di gestione di dati personali e di telefono.

q) Per Social Network Sites (SNS – Sito di Social Network): servizi web (social network, newsletter, mailing list, forum, instant messaging, wiki, etc.) utilizzati per creare e mantenere reti virtuali e comunità on-line costituite da gruppi di persone che si relazionano tra loro da un qualsiasi tipo di legame (amicizia, di interessi, lavorativo, etc.).

Art. 3 - Principi generali

1. I trattamenti dei dati raccolti durante l'utilizzo degli strumenti informatici e dell'accesso alla rete internet devono rispettare le garanzie in materia di protezione dei dati e svolgersi nell'osservanza di alcuni cogenti principi:

a) il principio di necessità, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati

personali e di dati identificativi in relazione alle finalità perseguite (art. 3 del Codice; par. 5.2);

b) il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art. 11, comma 1, lett. a), del Codice). Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati (v. par. 3);

c) i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art. 11, comma 1, lett. b), del Codice: par. 4 e 5), osservando il principio di pertinenza e non eccedenza (par. 6). Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti (par. 8) ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza" (Parere n. 8/2001, cit., punti 5 e 12).

Art. 4 - Ambito di applicazione

1. Le apparecchiature informatiche, i programmi e tutte le varie funzionalità che la Provincia di Teramo mette a disposizione dei suoi utenti, ed in particolar modo i servizi telematici di accesso ad Internet e posta elettronica, devono essere utilizzate nel pieno rispetto delle norme del presente Regolamento al fine di evitare possibili danni erariali, finanziari e di immagine all'Ente stesso.

2. Tutti gli Operatori ed i terzi autorizzati sono interessati dalle disposizioni del presente Regolamento e sono tenuti a contattare il Responsabile del Servizio Informatico prima di intraprendere qualsiasi attività non esplicitamente ricompresa nelle disposizioni che seguono, al fine di garantire che tali attività non siano in contrasto con gli standard di sicurezza informatica stabiliti dall'Ente.

3. Il presente regolamento per l'utilizzo degli strumenti informatici e dei servizi di telefonia e modalità di controllo viene pubblicato sul sito istituzionale della Provincia di Teramo, nell'apposita sezione Regolamenti. La notifica individuale agli Operatori dell'adozione del presente Regolamento viene demandata ai singoli dirigenti, ciascuno per il settore di propria competenza, con propria nota informativa che ne assicuri la più ampia diffusione, compresa la sottoscrizione per presa visione e accettazione.

4. L'Ente, contestualmente alla sottoscrizione del contratto di lavoro o, in mancanza, all'atto di conferimento dell'incarico, consegna e fa sottoscrivere ai nuovi assunti, con rapporti comunque denominati, copia del presente Regolamento.

Art. 5 - Titolarità

1. La Provincia di Teramo è titolare di tutte le risorse informatiche ed informative dell'Ente. Il personale dipendente e/o assimilato deve essere informato su quali siano gli usi consentiti e proibiti di tali risorse.

2. Ogni infrazione alle regole di cui al presente Regolamento costituisce una violazione della sicurezza ed esporrà l'utente ai provvedimenti previsti in tali casi, come meglio esplicitato al capo VII del presente Regolamento.

Art. 6 - 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 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 dei vari settori 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 i 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) elaborazione delle regole per un utilizzo ragionevolmente sicuro del sistema informatico;

c) implementazione e controllo delle policy di sicurezza;

d) predisposizione del materiale informativo e divulgativo in materia di sicurezza informatica.

6. Il personale provinciale 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 delle proprie credenziali di autenticazione (username e password).

Capo II
Gestione delle credenziali di autenticazione e autorizzazione

Art. 7 - Attribuzione delle credenziali

1. L'accesso al sistema informatico della Provincia di Teramo (computer, rete, casella di posta elettronica, ecc.) è protetto con credenziali di autenticazione (username e password) attribuite dal Responsabile del sistema informatico.

2. A tal fine il Servizio Gestione delle Risorse umane comunica, entro il 31 gennaio di ogni anno, al Servizio Informatico l'elenco ufficiale degli amministratori e dei lavoratori subordinati e parasubordinati, nonché tutte le successive modifiche.

3. I Dirigenti, con apposito modulo, richiedono l'attivazione, la sospensione o la disattivazione delle credenziali per le altre categorie di Operatori.

4. All'atto del primo accesso ai servizi (login), l'utente deve modificare la password comunicatagli dal Responsabile del sistema informatico con una password personale scelta autonomamente, in base alle direttive contenute nel presente capo e mantenerla segreta custodendola con la massima diligenza.

5. La username attribuita dal Responsabile del sistema informatico è immodificabile.

6. Nessuno è autorizzato a richiedere ad un dipendente la propria username e password.

7. Nell'utilizzo del sistema informatico della Provincia ogni Utente è identificato dalle proprie credenziali, che viene registrata dai vari servizi informatici.

8. L'utente è considerato unico responsabile dell'attività espletata tramite la propria Username, vige a tal fine una presunzione di corrispondenza tra utente (dipendente o collaboratore) ed Username.

9. L'Utente si impegna a mantenere un comportamento che tenda ad evitare, o comunque minimizzare, il verificarsi di rischi informatici.

Art. 8 - Caratteristiche delle password

1. Le password devono essere lunghe almeno 8 caratteri, (salvo impedimenti tecnici delle applicazioni), evitando contenuti di senso logico ed immediato, facilmente individuabili (ad es. nomi, date di nascita, parole del vocabolario) e riferimenti agevolmente riconducibili all'incaricato.

Art. 9 - Scadenza delle password

1. Le password per l'accesso al sistema informatico e telematico della Provincia di Teramo ed ai relativi servizi devono essere modificate almeno ogni 6 mesi o 3 mesi in caso di trattamento di dati sensibili o giudiziari, a tal fine è predisposto un meccanismo di richiesta automatica di sostituzione, che alla scadenza del termine richiede all'utente la sostituzione della vecchia password con una nuova.

Art. 10 - Perdita della segretezza

1. Nel caso in cui si sospetti che la password abbia perso il requisito essenziale della segretezza, deve esserne data immediata comunicazione al Responsabile del sistema informatico ed al Dirigente competente.

2. Qualora l'utente venga a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al Responsabile del sistema informatico ed al Dirigente competente.

Art. 11 - Disattivazione delle credenziali

1. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica

2. Almeno 7 giorni prima del termine del rapporto con la Provincia, l'utente deve eliminare i dati digitali non attinenti all'attivà lavorativa dalla casella di posta elettronica personale o dalla memoria del PC, in caso di inadempimento l'Amministratore di sistema incaricato potrà a provvedere alla eliminazione dei detti contenuti digitali.

3. In ogni caso, gli Operatori, entro 60 giorni dalla cessazione del rapporto con la Provincia, possono chiedere il recupero di eventuali contenuti digitali di carattere personale non eliminati dalla casella di posta elettronica personale o dalla memoria del PC.

4. I contenuti della casella di posta elettronica vengono conservati per 1 anno dalla cessazione del rapporto di lavoro.

Art. 12 - Accesso al sistema informatico della Provincia da parte di Utenti autorizzati

1. I soggetti di cui all'art. 2 let. g) possono accedere al sistema informatico della Provincia di Teramo mediante le credenziali loro assegnate dal Responsabile del sistema informatico, utilizzando PC in dotazione della Provincia appositamente predisposti a tal fine.

2. Gli Operatori non possono consentire l'accesso al sistema informatico della Provincia di Teramo mediante le loro credenziali a soggetti terzi, anche nel caso di terzi autorizzati.

Art. 13 - Violazioni

1. In caso di violazione del presente regolamento da parte dell'Utente, la Provincia può revocare le credenziali di autenticazione ed autorizzazione, ovvero sospenderne temporaneamente l'utilizzo.

Capo III
Uso del personal computer

Art. 14 - Il Personal Computer

1. Il Personal Computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

2. Il Responsabile del Servizio Informatico provvede a dotare tutti i personal computer assegnati agli Operatori 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.

3. 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.

4. L'accesso all'elaboratore è protetto con credenziali di autenticazione ed autorizzazione (username e password), attribuite dal Responsabile del sistema informatico secondo le modalità di cui all'art. 6 del presente Regolamento, le dette credenziali consentono anche l'autenticazione e l'autorizzazione informatica alla rete locale (LAN) della Provincia ed alla rete Internet.

5. 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.

6. E' fatto obbligo, inoltre, di mantenere segreta la propria password e di custodirla con la massima diligenza.

7. La username attribuita dal Responsabile del sistema informatico è immodificabile.

8. Gli Operatori non possono modificare le caratteristiche impostate sui PC a loro assegnati, i punti rete di accesso e le configurazioni delle reti LAN/WAN presenti nelle sedi, salva autorizzazione scritta del Responsabile del sistema informatico.

9. Non è consentita l'attivazione della password di accensione al BIOS (Basic Input-Output System) senza preventiva autorizzazione da parte del Responsabile del Sistema Informatico.

Art. 15 - Utilizzo del Personal Computer da parte degli Operatori

1. L'accesso ai personal computer della Provincia è consentito agli Operatori solo mediante le proprie credenziali di autenticazione ed autorizzazione.

2. Le dette credenziali identificano in modo univoco l'Utente e vengono registrate dai vari servizi informatici della Provincia (es. navigazione web, accesso a risorse condivise).

Art. 16 - Help desk e assistenza remota

1. Al fine di migliorare il servizio di assistenza, il Servizio Informatico ha predisposto un form web all'indirizzo assistenza.provincia.teramo.it oppure inviando una semplice email a assistenza@provincia.teramo.it, mediante il quale gli Operatori possono far pervenire richieste di assistenza e segnalazioni di malfunzionamento dei computer e della rete.

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. Il Responsabile del sistema informatico ed i suoi collaboratori, per l'espletamento delle funzioni e delle mansioni assegnate loro, possono accedere ai personal computer in dotazione all'Ente, mediante le proprie credenziali di autenticazione, in relazione agli scopi di volta in volta identificati, anche mediante sistemi di accesso remoto (es. vnc), stando ben attenti a non acquisire informazioni personali e dati personali, in particolare dati sensibili o giudiziari, degli Operatori.

Art. 17 - Accesso alle cartelle di lavoro dell'Operatore

1. Nel caso in cui, durante un periodo di assenza improvviso o prolungato dell'utente e per improrogabili necessità legate all'attività lavorativa, si debba accedere alle cartelle di lavoro dello stesso e non sia possibile richiedere l'intervento diretto dell'interessato, il Dirigente competente e il Responsabile del sistema informatico avvieranno la necessaria procedura di accesso, prevista nell'allegato "A" al presente Regolamento, redigendo apposito verbale ed informando il lavoratore interessato con tempestività e per iscritto, trasmettendogli altresì copia del verbale redatto.

2. Nelle medesime fattispecie di cui al comma 1, nei casi di necessità di accesso alle cartelle di lavoro di un operatore di Polizia Provinciale, durante la procedura di accesso va garantita la presenza del Comandante del Corpo di Polizia Provinciale o di Ufficiale del Corpo di Polizia Provinciale.

Art. 18 - Acquisizione ed installazione degli strumenti informatici e telematici

1. Per prevenire l'introduzione di virus e/o altri programmi dannosi e per proteggere l'integrità del sistema informatico della Provincia, anche al fine di garantire la compatibilità funzionale, tecnica ed il mantenimento dell'efficienza operativa dei sistemi e delle reti, l'hardware ed il software in dotazione agli uffici devono essere acquisiti ed installati previo parere del Responsabile del sistema Informatico.

2. A tal fine il dirigente interessato deve formulare richiesta scritta, al Responsabile del sistema informatico.

3. Non è consentito agli Operatori installare autonomamente programmi per elaboratore non attinenti a ragioni di servizio.

4. Solo il Responsabile del Servizio Informatico ed il personale appositamente autorizzato possono procedere all'installazione, duplicazione ed utilizzo dei software di cui l'Ente è titolare, nei limiti di quanto consentito dalle licenze d'uso o da eventuali accordi contrattuali.

Art. 19 - Creazione di programmi o documenti automatizzati

1. In caso di creazione di software e altre procedure informatiche da parte di Uffici o personale dell'Ente, o commissionati a soggetti terzi, devono essere resi disponibili alla Provincia: l'accesso al codice sorgente (se disponibile) e alle base dati; l'analisi e la documentazione sul funzionamento e l'installazione; i metadati sulle strutture dati, eventualmente implementate.

2. La proprietà di quanto sopra, inclusi i diritti derivanti, sono della Provincia di Teramo, salvo il diritto di essere riconosciuto autore dell'invenzione [Titolo IX del Libro Quinto del Codice Civile,, D. lgs. 518 del 29 dicembre 1992 che novella la legge 633/41].

Art. 20 - Supporti e dispositivi informatici per la memorizzazione

1. Al fine di garantire la corretta gestione delle politiche di sicurezza delle informazioni è fatto divieto a tutti gli Operatori di replicare su supporti e dispositivi informatici per la memorizzazione (dischi locali dei PC, memorie esterne) banche dati e documenti contenenti dati sensibili o giudiziari senza esplicita autorizzazione del Dirigente competente e senza l'adozione di adeguate misure di sicurezza.

2. Particolare attenzione deve essere, comunque, prestata nella memorizzazione di tutte le tipologie di dati su supporti e dispositivi informatici di memorizzazione "esterni" (c.d. memorie esterne), è assolutamente vietato effettuare inutili duplicazioni di dati su tali dispositivi.

3. I supporti e dispositivi informatici contenenti dati personali devono essere custoditi con la massima diligenza.

4. Gli Operatori devono provvedere periodicamente (almeno ogni 3 mesi) alla pulizia dei propri dispositivi e supporti informatici, con cancellazione dei file obsoleti o inutili.

5. È consentito l'utilizzo di memorie esterne (es. floppy disk, cd rom, nastri magnetici, chiavi usb) prestando particolare attenzione ai supporti di incerta attendibilità, avendo cura di effettuate la preventiva scansione antivirus.

Art. 21 - Dispositivi di comunicazione

1. Non è consentita l'installazione sul proprio PC o il collegamento alla rete LAN di dispositivi di comunicazione (come ad esempio modem, dispositivi wireless e bluetooth, pc portatili non in dotazione all'ente), se non con l'autorizzazione scritta del Responsabile del sistema informatico, previa richiesta scritta da parte del Dirigente.

2. I supporti e dispositivi informatici per la memorizzazione devono essere utilizzati prestando la massima attenzione, effettuando preventivamente la scansione antivirus del supporto ed avvertendo immediatamente il Responsabile del sistema informatico nel caso in cui siano rilevati virus informatici.

Art. 22 - Allontanamento momentaneo dalla postazione di lavoro

1. Al fine di evitarne l'indebito utilizzo da parte di terzi, nonché di consentire il risparmio energetico, l'Utente deve spegnere il Personal Computer alla fine di ogni giornata lavorativa, provvedendo altresì a scollegarlo dalla rete elettrica.

2. Sempre per la finalità di cui al primo comma, in caso di allontanamento dalla postazione di lavoro l'Utente deve attivare la sospensione del computer o, in alternativa lo screen saver protetto con password.

Art. 23 - Controlli

1. E' responsabilità del dirigente verificare il corretto utilizzo delle risorse assegnate al settore di riferimento ed evitarne l'uso improprio o l'accesso alle risorse da parte di personale non autorizzato, compreso l'utilizzo da parte di terzi di punti rete in luoghi non presidiati.

Art. 24 - Cartella per il salvataggio dei Documenti

1. I documenti informatici relativi all'attività lavorativa devono essere salvati nella cartella “Documenti” dell'Utente.

Art. 25 - Utilizzo di PC portatili e/o accessori temporaneamente assegnati

1. L'utente è responsabile del PC portatile e/o accessori (macchina fotografica, videoproiettore) a lui temporaneamente assegnati e deve custodirli con diligenza, sia all’interno degli uffici della Provincia, sia durante gli spostamenti esterni, fino alla loro riconsegna.

2. Ai PC portatili della Provincia si applicano le regole previste dal presente Regolamento anche al di fuori della rete e degli uffici dell’Ente.

3. Particolare attenzione deve essere prestata:

a) nell’utilizzo e nella custodia del PC portatile al di fuori della rete e degli uffici dell’Ente;

b) nella connessione a reti esterne;

c) nella rimozione di eventuali file personali memorizzati nel medesimo prima della riconsegna.

Art. 26 - Protezione e aggiornamento software dei pc

1. Ogni utente deve tenere comportamenti tali da ridurre al minimo il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

2. Ogni utente è tenuto a controllare il regolare funzionamento del sistema operativo e del software installato, ed a comunicare eventuali malfunzionamenti o avvisi sospetti al Responsabile del sistema informatico, secondo le procedure previste.

3. Nel caso di malfunzionamenti o avvisi sospetti, l'utente dovrà immediatamente:

a) sospendere ogni elaborazione in corso senza spegnere il computer;

b) segnalare l'accaduto al Responsabile del sistema informatico.

Art. 27 - Utilizzo personale

1. L’utente deve creare una apposita cartella “personale” all’esterno della cartelle documenti in cui salvare tutte i files personali, al fine di tenerli ben distinti dai files attinenti all’attività lavorativa.

2. Soltanto in caso di espressa richiesta dell'autorità giudiziaria sarà consentito l'accesso alla cartella “personale” così come prevista dal comma precedente.

Capo IV
Posta Elettronica Certificata

Art. 28 - PEC Istituzionale

1. La Posta Elettronica Certificata (detta anche PEC) è un sistema di comunicazione simile alla posta elettronica standard a cui si aggiungono delle caratteristiche di sicurezza e di certificazione della trasmissione tali da aggiungere un valore legale ai messaggi. Il valore legale è assicurato dai gestori di posta PEC del mittente e del destinatario che certificano:

a) Data e ora dell'invio del messaggio da parte del mittente;

b) Data e ora dell'avvenuta consegna del messaggio al destinatario;

c) Integrità del messaggio (ed eventuali allegati) nella trasmissione da mittente a destinatario.

2. Le certificazioni di cui al comma 1 sono assicurate solo per comunicazioni inviate da una casella PEC e ricevute da un'altra casella PEC.

3. La casella di posta elettronica certificata della Provincia di Teramo (provincia.teramo@legalmail.it) è pubblicata sul sito internet dell'Ente, in home page.

4. Le credenziali (user id e password) per accedere a tale casella di posta certificata devono essere a conoscenza unicamente dell'addetto al protocollo e del Responsabile dell'Ufficio Protocollo.

5. Tale casella di posta elettronica certificata è quotidianamente controllata dal dipendente addetto al protocollo, che provvede:

- a protocollare i messaggi, che non siano spam;
- a smistarli ai competenti Settori Provinciali;
- ad adempiere alle prescrizioni previste dalla legge 18 giugno 2009 n. 69.

Art. 29 - Attivazione PEC per Settori e Servizi

1. Ciascun dirigente di Settore della Provincia di Teramo è autorizzato a richiedere al Responsabile del sistema informatico una casella di posta elettronica certificata, qualora lo ritenga funzionale all'espletamento dei compiti del proprio Settore. In questo caso lo stesso Responsabile di Settore dovrà organizzare un servizio di controllo quotidiano della casella di posta elettronica certificata settoriale, provvedendo anche a tutte le operazioni di protocollazione e archiviazione.

Capo V
Uso della posta elettronica

Art. 30 - Informazioni Generali

1. La casella di posta elettronica affidata al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

2. L'account di posta elettronica (indirizzo di posta e password) è fornito gratuitamente, insieme ad un limitato spazio disco agli Operatori del sistema informatico della Provincia di Teramo, così come definiti nell'art. 2 let. d) del presente Regolamento.

3. Il formato dell'indirizzo di posta è il seguente:
[iniziale_del_nome].[cognome]@provincia.teramo.it.

4. Sono fornite, inoltre, una o più caselle di posta elettronica ad ogni servizio, dietro apposita richiesta scritta al Responsabile del sistema informatico.

5. Il Responsabile del sistema informatico ha l'obbligo di adottare tutte le misure di sicurezza ritenute necessarie e sufficienti a minimizzare il rischio di perdita di informazioni. A tal fine si avvarrà anche di strumenti idonei a verificare, mettere in quarantena o cancellare i messaggi che potrebbero compromettere il buon funzionamento del servizio.

6. Nell'attività di controllo per la gestione della sicurezza, il Responsabile del sistema informatico ed i suoi collaboratori potrebbero venire a conoscenza di informazioni contenute nelle caselle di posta elettronica personale degli Operatori.

7. Il Responsabile del sistema informatico ed i suoi collaboratori, nei limiti delle funzioni e delle mansioni assegnate loro, possono accedere alle caselle di posta elettronica personale ed a quelle istituzionali, in relazione agli scopi di volta in volta identificati, redigendo apposito verbale ed informando gli interessati con tempestività e per iscritto, trasmettendo altresì copia del verbale redatto.

8. I messaggi di posta elettronica vengono conservati nei server mail della provincia, finché non vengano cancellati dagli Operatori. I server sono gestiti dal Servizio Informatico dell'Ente, che ne cura anche il backup periodico. Alcuni messaggi cancellati dagli Operatori potrebbero essere comunque conservati nei dispositivi di salvataggio automatico (backup) dei dati.

9. L'utente deve comunicare al Responsabile del sistema informatico qualsiasi malfunzionamento o utilizzo abusivo del proprio indirizzo di posta elettronica, mediante il servizio di helpdesk di cui all'art. 16 del presente Regolamento.

10. L'utente deve conformarsi alle indicazioni tecniche fornite dal Responsabile del sistema informatico.

Art. 31 - Attivazione del servizio

1. L'attivazione degli account avviene a cura del Responsabile del sistema informatico secondo le modalità di cui all'art. 7.

Art. 32 - Gestione delle credenziali di accesso

1. L'accesso alla casella di posta elettronica è protetto con credenziali di autenticazione (username e password).

2. All'atto del primo accesso alla casella (login), l'utente deve modificare la password comunicatagli dal Responsabile del sistema informatico con una password personale scelta autonomamente, in base alle regole dettate nel capo II del presente Regolamento, e mantenerla segreta custodendola con la massima diligenza.

3. La username, invece, è rappresentato dallo stesso indirizzo di posta elettronica attribuito dal Responsabile del sistema informatico ed è immodificabile.

4. I messaggi di posta elettronica vengono conservati nel server mail della Provincia, gestito dal Servizio Informatico dell'Ente, che ne cura anche il backup periodico.

5. Nella gestione delle email di servizio (come definito nell'art. 30), gli operatori abilitati sono responsabili in solido della custodia delle credenziali di accesso.

Art. 33 - Accesso alla casella personale in caso di assenza del titolare

1. Nel caso in cui, durante un periodo di assenza improvviso o prolungato dell'interessato e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica dello stesso e non sia possibile richiedere l'intervento diretto dell'interessato, il dirigente competente e il Responsabile del sistema informatico avvieranno la necessaria procedura di accesso, prevista nell'allegato A al presente Regolamento, redigendo apposito verbale ed informando il lavoratore con tempestività e per iscritto, trasmettendogli altresì copia del verbale redatto.

2. Nelle medesime fattispecie di cui al comma 1, nei casi di necessità di accesso alle cartelle di lavoro di un operatore di Polizia Provinciale, durante la procedura di accesso va garantita la presenza del Comandante del Corpo di Polizia Provinciale o di Ufficiale del Corpo di Polizia Provinciale.

3. Per tutto il periodo di assenza l'Utente deve attivare il servizio di risposta automatica al fine di avvisare i mittenti di contattare, in caso di comunicazioni attinenti all'attività lavorativa, il Servizio o l'Ufficio competente.

Art. 34 - Accesso alla casella di posta elettronica personale dei Dirigenti e degli Amministratori in caso di assenza del titolare

1. Nel caso in cui, durante un periodo di assenza improvviso o prolungato di un Dirigente o di un Amministratore e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica dello stesso e non sia possibile richiedere l'intervento diretto dell'interessato, il sostituto del Dirigente o dell'Amministratore, appositamente individuato per iscritto dai medesimi, e il Responsabile del sistema informatico avvieranno la necessaria procedura di accesso, prevista nell'allegato A al presente Regolamento, redigendo apposito verbale ed informando ed informando il Dirigente e/o Amministratore interessato con tempestività e per iscritto, trasmettendogli altresì copia del verbale redatto.

Art. 35 - Utilizzo degli indirizzi da parte dell'Ente

1. 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.

Art. 36 - Utilizzo da parte del CRAL e della RSU

1. Il CRAL provinciale e la RSU possono inviare agli indirizzi di posta elettronica personali comunicazioni inerenti le attività delle stesse, sempre su richiesta ed esplicito consenso del dipendente ai sensi del D.lgs 196/2003.

Art. 37 - Utilizzo delle caselle di posta elettronica da parte dei dipendenti e dei collaboratori

1. L'utente è riconosciuto quale unico autore dei messaggi inviati dalla sua casella di posta elettronica personale fornitagli dalla Provincia di Teramo, egli è considerato, inoltre, unico responsabile dell'attività espletata tramite la detta casella personale.

2. L'Utente deve implementare, sulla propria stazione di accesso alla posta elettronica, tutte quelle misure idonee e necessarie ad evitare, o comunque minimizzare, la divulgazione di virus informatici e simili e garantire la funzionalità della stessa casella.

3. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. E' previsto un dimensionamento massimo per ciascuna casella in relazione alla disponibilità di spazio dei sistemi di posta di volta in volta disponibili, che non potrà essere superato per evitare l'appesantimento della gestione dei server stessi.

4. L'utente in servizio, dotato delle necessarie dotazioni informatiche, è tenuto ad accedere alla casella di posta elettronica almeno 2 volte durante la giornata lavorativa, preferibilmente all'inizio e alla fine della giornata lavorativa.

5. E' vietato agli Operatori configurare software client per la posta elettronica senza l'autorizzazione del Responsabile del sistema informatico.

Art. 38 - Contenuto delle Comunicazioni

1. Ogni utente è obbligato ad utilizzare il servizio di posta elettronica nel rispetto della legge, con particolar riguardo al Codice per la tutela dei dati personali (D.lgs. n. 196 del 2003), ponendo la massima attenzione alla sicurezza del sistema informatico e telematico della Provincia.

2. A tal fine sono posti i seguenti divieti:

- divieto di utilizzare il servizio per scopi illegali, per inviare o ricevere materiale pornografico, diffamatorio, discriminatorio, pericoloso per il sistema informatico;
- divieto di utilizzare il servizio per inviare o ricevere messaggi o materiali che incoraggino terzi a mettere in atto una condotta illecita e/o criminosa passibile di responsabilità penale o civile;
- divieto di utilizzare il servizio per inviare catene di lettere, comunicazioni commerciali, messaggi politici;

- divieto di aprire messaggi di posta elettronica sospetti contenenti particolari tipologie di allegati (es. files con estensione exe, bat, com e file audio, video o immagini), senza l'autorizzazione dell'Amministratore di sistema;
- divieto di effettuare invii multipli senza mascherare gli indirizzi dei vari destinatari, se non strettamente necessario;
- divieto di sovraccaricare il sistema con l'invio di allegati troppo pesanti (max. 20 MB) ed evitare inutili immagini o grafismi;
- divieto di effettuare comunicazioni inerenti all'attività lavorativa con caselle di posta elettronica diverse da quella personale, di servizio o istituzionale di cui all'art. 2 lett. h, i, j.

Art. 39 - Comunicazioni da e verso l'esterno

1. Per le comunicazioni esterne, cosi come individuate nell'art. 2 let. n), oltre alle regole sopra esposte, occorre osservare le disposizioni del Manuale di Gestione del Protocollo Informatico e dei Flussi Documentali dell'Ente.

2. Sono vietate mediante la casella di posta personale comunicazioni esterne contenenti:

- dati personali sensibili o giudiziari ex D.lgs. 196/2003 degli Utenti della Provincia, definiti nell'art. 2 punto f);
- documenti della Provincia di Teramo per i quali l'accesso è regolato dalla L. 241/90, in modo particolare se riservati o protetti dal diritto d'autore.

Art. 40 - Avvisi in calce alle e-mail

1. In calce ad ogni e-mail inviata dalle caselle di posta elettronica personale verrà inserito dal sistema in maniera automatica il seguente testo:
"Si avvertono gli interessati che i messaggi inviati al presente indirizzo di posta elettronica potrebbero essere conosciuti anche da Operatori autorizzati ad accedere alla casella in caso di assenza del titolare, ai sensi degli artt. 33 e 34 del Regolamento per l'utilizzo degli strumenti informatici e telematici della Provincia di Teramo".

2. In calce ad ogni e-mail inviata dalla casella di posta elettronica assegnata al settore, Servizio ed Ufficio verrà inserito dal sistema in maniera automatica il seguente testo:
"Si avvertono gli interessati che i messaggi inviati al presente indirizzo di posta elettronica possono essere conosciuti da tutti gli Operatori addetti al presente Settore, Servizio, Ufficio".

Art. 41 - Comunicazioni personali

1. Gli Operatori devono ridurre al minimo le comunicazioni personali per motivi privati non inerenti al lavoro d'ufficio.

2. E' fatto, comunque, divieto di comunicazioni personali per motivi privati non inerenti al lavoro d'ufficio aventi ad oggetto dati sensibili o giudiziari ex D.lgs. n. 196 del 2003.

3. Gli Operatori devono creare una apposita cartella “personale” nelle cartelle posta in arrivo e posta inviata, in cui salvare tutte le e-mail personali al fine di tenerle ben distinte dalle e-mail attinenti all’attività lavorativa.

4. In nessun caso i soggetti autorizzati ad accedere alla casella personale ai sensi degli art. 33 e 34 potranno prendere visione delle e-mail contenute nella cartella personale.

5. Permane in ogni caso la responsabilità del singolo utente per il materiale salvato nella cartella “personale” e per eventuali omissioni.

Capo VI
Firme Digitali

Art. 42 - Soggetti abilitati

1. E’ assegnato il dispositivo di firma digitale a:

- Presidente;
- Segretario Generale;
- Dirigenti della Provincia di Teramo;
- Comandante della Polizia Provinciale;
- Funzionari incaricati di area di posizione organizzativa;
- Dipendenti autorizzati con provvedimento del proprio Dirigente.

Art. 43 - Definizione dei Ruoli

1. Operano nel processo di assegnazione e gestione del certificato digitale i seguenti soggetti:

a) La Provincia, che richiede il certificato a favore del titolare, provvede a fornire informazioni per ciò che attiene al ruolo e alle funzioni istituzionali dei dipendenti ai quali possono essere assegnati i certificati di firma digitale e individua e nomina gli incaricati del servizio; ha inoltre la facoltà, ai sensi dell'art. 36, comma 1 lettera c) del Codice dell'amministrazione digitale, di richiedere la sospensione o la revoca del certificato;

b) Il Titolare al quale è assegnato il certificato di firma digitale. Con successivo provvedimento verranno indicate le categorie che, in ragione della funzione che svolgono all’interno dell'Ente, potranno essere titolari di firma digitale e i soggetti che potranno autorizzarne il rilascio;

c) Incaricati del servizio di firma digitale, nominati dal Presidente e responsabili, su delega del Certificatore, dell'identificazione dei richiedenti, dell'attivazione delle procedure di emissione, revoca o sospensione dei certificati;

d) Certificatore, soggetto che si occupa della gestione del servizio di firma qualificata nel rispetto di quanto disposto dall'art. 32, comma 3 del Codice dell'amministrazione digitale.

Art. 44 - Tipo di utilizzo

1. La firma digitale è utilizzata per la sottoscrizione di documenti informatici nell'ambito delle attività istituzionali dei soggetti abilitati e nel rispetto dei poteri di firma derivanti dalla legge o dai regolamenti interni dell'Amministrazione Provinciale.

Art. 45 - Presentazione telematica di istanze e dichiarazioni

1. Sono valide tutte le istanze e le dichiarazioni pervenute all'Amministrazione per via telematica, firmate digitalmente da parte di privati, da altre Amministrazioni Pubbliche o da altri Servizi dell'Ente.

Art. 46 - Compiti e responsabilità degli incaricati di firma

1. Gli incaricati di firma provvedono a:

a) verificare con certezza l'identità del richiedente;

b) rilasciare i certificati qualificati attraverso l'utilizzo dell'apposito sistema informatico fornito dal Certificatore seguendo le istruzioni operative previste dal Manuale Operativo del Certificatore;

c) informare il richiedente riguardo agli obblighi assunti in merito alla protezione della segretezza delle chiavi private e al trattamento dei dati personali;

d) supportare il titolare nelle ipotesi di revoca, sospensione o annullamento della sospensione delle firme attivate;

e) raccogliere le comunicazioni di rilascio/rinnovo, sospensione e/o revoca e conservarle con modalità sicure;

f) individuare mensilmente i certificati la cui data di scadenza è compresa entro i trenta giorni solari successivi e, verificata la non sussistenza di condizioni per la loro sospensione o revoca, richiedere l'autorizzazione formale per il rinnovo degli stessi secondo quanto indicato dall'art. 39, lett. b);

g) rispettare le misure minime di sicurezza previste per il trattamento dei dati personali dal D.Lgs. 196/2003;

h) rispettare le necessarie procedure di sicurezza nell'esercizio delle proprie funzioni;

i) compilare l'elenco dei Titolari di certificato per l'identificazione;

j) fornire istruzioni ai Titolari sul corretto utilizzo del servizio di firma digitale;

k) conservare le buste - fornite dal Certificatore - contenti i PIN in luogo sicuro e protetto, avendone accesso esclusivo.

Art. 47 - Obblighi del titolare

1. Il titolare del certificato di firma digitale è tenuto:

- ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri e ad assicurare la custodia del dispositivo di firma, che utilizzerà personalmente e per ragioni istituzionali;
- a conservare con la massima diligenza e riservatezza i propri codici personali al fine di evitarne l'uso fraudolento da parte di terzi;
- a comunicare informazioni esatte e veritiere rispetto ai propri dati personali nell'ambito delle iniziali procedure di registrazione al responsabile del registro delle firme digitali e ad informare anticipatamente gli incaricati di firma dell'eventuale variazione del rapporto contrattuale con l'Ente e di tutti i dati richiesti per l'emissione del certificato;
- ad informare anticipatamente gli incaricati di firma di ogni circostanza che renda necessaria o, comunque, opportuna la revoca o la sospensione del certificato e del dispositivo di firma a lui assegnato; deve altresì informare tempestivamente l'incaricato di firma di eventuali richieste di revoca o di sospensione che egli, per necessità o urgenza, abbia inoltrato direttamente al Certificatore.

Art. 48 - Procedure di attribuzione / identificazione

1. Il soggetto al quale spetta dare l'autorizzazione al rilascio del certificato digitale ai sensi dell'art. 43 lett. b) del presente Regolamento invia all'Incaricato l'allegato modulo B,che costituisce parte integrante del presente Regolamento, in originale e debitamente sottoscritto, nel quale indica le persone autorizzate al possesso del certificato;
2. L'incaricato, ricevuta la richiesta di attivazione, verifica la regolarità delle autorizzazioni richieste dall'art. 43 lettera b) e, in caso positivo, convoca il richiedente per lo svolgimento delle operazioni di registrazione;
3. Il richiedente deve presentarsi dall'Incaricato, nel giorno comunicatogli, munito di un valido documento di identità, del codice fiscale;
4. L'incaricato, ferma restando la responsabilità del richiedente per omesse o false dichiarazioni, provvede all'identificazione del richiedente;
5. L'incaricato provvede a fotocopiare il codice fiscale e il documento di identità presentato e provvede affinché la copia sia firmata dal richiedente;
6. L'incaricato consegna al richiedente la busta contente i codici personali necessari per la procedura di registrazione e il dispositivo di firma da utilizzare per l'apposizione delle firme;

7. L'incaricato provvede alla registrazione dei dati anagrafici del titolare e all'invio informatico della richiesta al Certificatore seguendo le istruzioni del Manuale Operativo;
8. Al termine delle predette operazioni l'incaricato archivia tutta la documentazione raccolta (modulo B, fotocopia del documento di identità e codice fiscale) in contenitori debitamente protetti;
9. La stessa procedura viene utilizzata per il rinnovo quinquennale del certificato digitale.

Art. 49 - Causa di revoca e di sospensione

1. La revoca di un certificato determina la cessazione anticipata della sua validità. La revoca ha luogo su iniziativa del Certificatore, del Titolare, di colui che ne ha autorizzato il rilascio o del Primo Incaricato nelle ipotesi previste dall'art. 46, punto 3, del presente Regolamento;

2. La revoca ha luogo nelle seguenti circostanze:

a) Cessazione del rapporto di lavoro del dipendente per qualsiasi causa (es. pensionamento, dimissioni);
b) Perdita del ruolo, qualifica o funzione istituzionale che motivano l'assegnazione del certificato;
c) Smarrimento, furto o cambio del dispositivo di firma;
d) Smarrimento o furto dei codici di sicurezza;
e) Sospetta falsificazione o abusi;
f) Riscontro da parte del Certificatore o dell'Ateneo di una violazione, commessa dell'utente, delle regole di utilizzo.

3. La sospensione di un certificato determina l'interruzione temporanea della sua validità. La sospensione ha luogo su iniziativa del Certificatore, del titolare o di colui che ne ha autorizzato il rilascio.

4. La sospensione ha luogo nelle seguenti circostanze:

- Possibile, ma non certa, perdita dei codici di sicurezza;
- Venir meno di uno o più requisiti che ne motivano l'assegnazione.

5. Ai sensi dell'art. 36, comma 3, del Codice dell'amministrazione digitale la revoca o la sospensione del certificato, qualunque ne sia la causa, hanno effetto dal momento della pubblicazione, a cura del Certificatore, della lista che lo contiene. Il momento della pubblicazione deve essere attestato mediante adeguato riferimento temporale.

Art. 50 - Procedura di revoca e di sospensione

1. Sospensione su richiesta del Titolare.
Nel caso si verifichi una delle circostanze che rendono necessaria la sospensione del certificato il Titolare deve contattare telefonicamente il numero verde del Certificatore

e comunicare per iscritto l'avvenuta sospensione all'Incaricato; venuta meno la causa di sospensione, il Titolare ne può richiedere l'annullamento presentandosi dall'Incaricato munito di valido documento di identità previa compilazione del modulo 2, allegato del presente Regolamento e di cui costituisce parte integrante. Con l'annullamento della sospensione viene ripristinata la validità del certificato, che viene rimosso dalla lista di sospensione.

2. Revoca su richiesta del Titolare.
Nel caso si verifichi una delle cause che rendono necessaria la revoca del certificato il Titolare deve provvedere alla immediata sospensione del certificato seguendo le modalità di cui al precedente comma 1 ed, entro breve, deve inoltrare, tramite raccomandata A.R., la richiesta di revoca del certificato al Certificatore; nel caso in cui la richiesta di revoca sia motivata dallo smarrimento o dal furto del dispositivo di firma utilizzato per il rilascio del certificato occorre allegare alla domanda di revoca inoltrata al Certificatore la denuncia di smarrimento e/o di furto effettuata presso le autorità competenti; successivamente il Titolare dovrà dare comunicazione scritta dell'avvenuta revoca all'Incaricato.

3. Revoca o Sospensione su richiesta di colui che ha autorizzato l'emissione del certificato.
Qualora si verifichi una delle ipotesi previste dall'art. 45 lettere a), b), e), f), e h) del presente Regolamento su richiesta motivata di colui che ha autorizzato il rilascio del certificato di firma digitale, previa compilazione del modulo 3, allegato del presente Regolamento, l'incaricato provvede ad effettuare le operazioni di revoca e sospensione necessarie ad evitare abusi ed usi impropri del certificato, seguendo le modalità di comunicazione al Certificatore sopra indicate e informando il titolare dell'avvenuta revoca o sospensione.

Capo VII
Intranet ed internet

Art. 51 - Orario di accesso alla rete

1. L'Accesso a internet attraverso la rete della Provincia è normalmente consentito durante l'orario di lavoro, salvo esigenze contigenti da parte dei diversi servizi, esigenze che impongono l'utilizzo degli strumenti informatici e di rete al di fuori dell'orario tradizionale.

Art. 52 - Risorse condivise

1. L'Archivio di Rete cosi come definito nell'art. 2 let. o) è un'area strettamente professionale e non può in alcun modo essere utilizzato per scopi diversi da quelli lavorativi. Qualunque file che non sia legato all'attività lavorativa non può essere memorizzato, nemmeno per brevi periodi, in questo archivio.

2. Il Responsabile del sistema informatico svolge sulle unità di rete attività di controllo, amministrazione e può in qualunque momento procedere alla rimozione dei files che riterrà pericolosi per la Sicurezza del sistema informatico.

Art. 53 - Collegamento alla Rete

1. Non è consentito collegare alcun dispositivo alla rete provinciale senza la preventiva autorizzazione scritta del Responsabile del sistema informatico.

Art. 54 - Internet

1. Gli Operatori utilizzano il collegamento ad Internet per motivi legati ai propri doveri di ufficio.

2. Dato che ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza, gli Operatori sono tenuti ad evitare l'accesso ad Internet per motivi privati non inerenti al lavoro d'ufficio fatte salve le operazioni consentite nel presente regolamento e con i limiti ivi indicati.

3. L'accesso alla rete Internet dalla rete LAN della Provincia è fornito gratuitamente.

4. Si rammenta che i sistemi di accesso ad Internet della Provincia tengono traccia della navigazione dei singoli Operatori, più precisamente il Sistema informatico della Provincia memorizzano i seguenti dati:

a) IP;

b) username;

c) indirizzo della connessione;

d) data ed ora della connessione;

e) servizi;

f) protocolli.

Art. 55 - Chat

1. Il contenuto delle Chat è memorizzato per un periodo di 3 mesi ed è soggetto a backup periodico.

Art. 56 - Responsabilità nella navigazione web

1. L'operatore è considerato l'unico responsabile dell'attività espletata nella rete Intranet della Provincia e nella Internet mediante le proprie credenziali di accesso e di autorizzazione (username e password) di cui all'art. 7 del presente Regolamento.

Art. 57 - Filtri web

1. L'accesso a determinati siti web o categorie di siti web è limitata o impedita mediante appositi filtri web predisposti dal Responsabile del sistema informatico.

2. I filtri web a tal fine memorizzano alcune informazioni di navigazione, quali:

a) IP;

b) username;

c) indirizzo della connessione;

d) data ed ora della connessione;

e) servizi;

f) protocolli.

3. E' possibile chiedere l'accesso a siti o categorie di siti filtrati mediante l'apposito modulo presente nel sistema di filtraggio.

Art. 58 - E-Learning

1. Al fine di agevolare la formazione degli operatori, la Provincia di Teramo eroga corsi di formazione in modalità e-learning e incentiva , previa autorizzazione da parte del Dirigente di riferimento, l'accesso a corsi di formazione on-line erogati da soggetti esterni, per accrescere le competenze collegate alla funzione svolta.

2. Gli operatori possono accedere alla piattaforma e-learning della Provincia mediante le credenziali di autenticazione e autorizzazione attribuite loro dell'Amministratore del sistema, credenziali che devono essere gestite in base alle norme previste nel capo II del presente Regolamento.

3. L'accesso ai singoli corsi programmati è riservato esclusivamente agli operatori individuati mediante provvedimento dell'ente, i quali sono obbligati a frequentare personalmente i corsi secondo le modalità e nei tempi previsti dal provvedimento.

4. L'accesso ai corsi liberi al contrario è consentito a tutti gli operatori.

5. Durante le sessioni di collegamento alla piattaforma di e-learning della Provincia di Teramo sono memorizzate le seguenti informazioni:

a) IP;

b) username;

c) data ed ora della connessione;

d) data ed ora di disconnessione;

e) pagine e contenuti visualizzati;

f) risultati delle prove di valutazione.

6. Tali informazioni sono necessarie per accertare l'effettiva frequenza del corso da parte dei soggetti obbligati e lo svolgimento delle prove di valutazione.

Art. 59 - Divieti di navigazione

1. Ogni utente è obbligato ad utilizzare il servizio di accesso al web, ponendo la massima attenzione alla sicurezza del sistema informatico e telematico della Provincia, a tal fine sono posti i seguenti divieti:

- divieto di utilizzare il servizio per scopi illegali, per inviare o ricevere materiale pornografico, diffamatorio, discriminatorio, pericoloso per il sistema informatico;
- divieto di utilizzare il servizio per inviare o ricevere messaggi o materiali che incoraggino terzi a mettere in atto una condotta illecita e/o criminosa passibile di responsabilità penale o civile;

- divieto di utilizzare il servizio per inviare catene di lettere, comunicazioni commerciali e per svolgere attività di propaganda politica;
- divieto di aprire, mediante servizi di web mail personale, messaggi di posta elettronica sospetti o contenenti particolari tipologie di allegati (es. files con estensione exe, bat, com e file audio, video o immagini).

2. E' fatto, comunque, divieto di comunicazioni personali per motivi privati non inerenti al lavoro d'ufficio aventi ad oggetto dati sensibili o giudiziari ex D.lgs. n. 196 del 2003.

3. Il Responsabile del sistema informatico provvede ad inibire la consultazione dei siti web non utili alla produttività dell'Ente e, soprattutto, potenzialmente lesivi per l'infrastruttura.

4. Durante la navigazione web è vietato inoltre, il carico e lo scarico (upload/dowload) di file del tipo MP3, AVI, MPG, Quicktime, e/o altri tipi di files o programmi per la fruizione di contenuto audio/video non legati ad un uso d'ufficio;

5. Gli Operatori sono tenuti a ridurre al minimo:

- le transazioni finanziarie on-line, ivi comprese le operazioni di remote banking, acquisti on-line e simili;
- la registrazione a siti i cui contenuti non siano legati all'attività lavorativa;

6. Il Responsabile del sistema informatico si riserva di applicare per singoli e gruppi di Operatori politiche di navigazione personalizzate in base alle mansioni ed eventuali disposizioni concordate con la Direzione e con i Dirigenti, al fine di ottimizzare l'uso delle risorse, gli investimenti e le prestazioni delle connessioni esistenti.

7. Non è consentito inoltre visitare siti e memorizzare documenti informatici dai contenuti di natura oltraggiosa e/o discriminatoria per sesso/etnia/religione/opinione e/o appartenenza sindacale e/o politica.

Art. 60 - Utilizzo dei SNS per fini istituzionali

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 che 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. Sarà cura dei Dirigenti 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.

3. La Provincia di Teramo, quindi, consente di utilizzare i SNS per finalità istituzionali, ed in particolare per:

- diffondere informazioni inerenti le attività dell'Ente al fine di garantire la trasparenza;
- informare i cittadini sui servizi offerti e le relative modalità di fruizione;
- promuovere la condivisione di eventi ed iniziative organizzate dall'Ente, pubblicare sondaggi;
- creare nuovi spazi di dialogo con i cittadini e nuovi canali per raccogliere le loro opinioni e valutare le soddisfazione degli utenti su servizi ed attività istituzionali.
- Confrontarsi con le altre amministrazioni dello Stato
- attività di customer services sui servizi erogati

Art. 61 - Comunicazione istituzionale mediante i SNS

1. La comunicazione istituzionale mediante i SNS è consentita previa valutazione dell'effettiva utilità ed efficacia dell'utilizzo di tale strumento attraverso:

- il target individuato;
- i contenuti da diffondere;
- l'obiettivo da raggiungere;
- le risorse a disposizione.

Art. 62 - Attivazione di nuovi profili SNS dell'Ente

1. La Provincia ha un proprio profilo pubblico identificabile come “Provincia di Teramo”. Il Presidente, su proposta del Dirigente competente, autorizza l'eventuale attivazione attivazione di nuovi profili pubblici riferiti a specifici servizi previo parere dell'Ufficio “Ufficio Stampa – Comunicazione – Redazione web” che valuta la richiesta sulla base degli elementi di cui all'articolo precedente.

2. Il Dirigente richiedente incarica almeno due operatori (art. 1 let. d) 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).

3. Nel caso di un unico profilo pubblico di SNS gli operatori sono responsabili in solido della custodia delle credenziali di accesso.

4. L'Ufficio “Ufficio Stampa – Comunicazione – Redazione web” effettua il monitoraggio dei contenuti pubblicati sui profili di SNS pubblici ed è autorizzato ad intervenire in caso di contenuti non congruenti.

Capo VIII
Altri strumenti stampanti, fax e fotocopiatrici

Art. 63 - Utilizzo Stampanti

1. È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni.

2. È buona regola evitare di stampare documenti o file molto lunghi o di contenuto grafico su stampanti comuni.

3. Non è consentito stampare documenti personali su qualsivoglia stampante.

4. E' obbligatorio effettuare le stampe in modalità fronte-retro, fatta salva documentata impossibilità tecnica o amministrativa.

Art. 64 - Telefoni fissi

1. 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.

2. Le dette informazioni sono utilizzabili nei limiti dello Statuto dei lavoratori (L. 300 del 1970) e del codice privacy (D.lgs 196 del 2003) memorizzate per 3 mesi.

Capo IX
Monitoraggi e controlli

Art. 65 - Principi generali

1. La Provincia di Teramo adotterà ogni accorgimento tecnico necessario a tutelare l'Ente da eventuali comportamenti non consentiti, salvaguardando il rispetto della libertà e della dignità dei lavoratori; gli eventuali trattamenti effettuati saranno ispirati a canoni di trasparenza e rispetteranno il principio di pertinenza e non eccedenza.

Art. 66 - Monitoraggi

1. Il Responsabile del Sistema Informatico, effettua monitoraggi periodici su dati anonimi allo scopo di verificare l'attuazione del presente Regolamento, i possibili rischi alla sicurezza informatica e le possibili problematiche inerenti l'utilizzo degli strumenti informatici. Questi monitoraggi si possono classificare in:

- analisi del traffico di rete: effettuati attraverso specifici log dei dispositivi di rete;

- analisi del traffico Internet: effettuati attraverso specifici log dei dispositivi di connessione ad Internet; nel dettaglio i dati personali conservati nei modi e nei tempi previsti dalla normativa vigente sono:
    - data e ora di inizio sessione;
    - IP sorgente;
    - IP destinazione;
    - servizio;
    - nome utente;
    - dominio;
    - indirizzo web della pagina visitata;
    - durata complessiva sessione.
- Inventario Hardware e Software: effettuati attraverso procedure prevalentemente automatiche per le apparecchiature collegate in rete e in maniera semiautomatica per le macchine non appartenenti al dominio.

2. Il monitoraggio delle risorse hardware e software non coinvolge in alcun modo i dati personali e i documenti presenti sulle singole postazioni di lavoro e viene effettuato per finalità organizzative e gestionali.

3. I dati del traffico telematico verranno gestiti secondo le modalità e le tempistiche previste dalla normativa vigente in materia di sicurezza dei dati del traffico telefonico e telematico. La Provincia si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà pericolosa per la sicurezza del sistema informatico ovvero acquisita o installata in violazione del presente Regolamento.

Art. 67 - Controlli

1. La Provincia di Teramo si riserva di effettuare controlli per verificare il rispetto del Regolamento. Riguardo a tali controlli il presente Regolamento costituisce preventiva e completa informazione nei confronti dei dipendenti. I controlli devono essere ispirati ai principi generali di cui all'art. 3 del presente Regolamento. In base al principio di correttezza , l'eventuale trattamento deve essere ispirato ad un canone di trasparenza, come prevede anche la disciplina di settore (Statuto dei lavoratori).

2. I dati devono essere gestiti soltanto dai soggetti preventivamente designati quali responsabili e incaricati del trattamento, come precisa l'art. 30 del Codice in materia di protezione dei dati personali. Nel caso in cui emerga un evento dannoso, una situazione di pericolo o utilizzi non aderenti al presente Regolamento, che non siano stati impediti con preventivi accorgimenti tecnici o rilevati durante i monitoraggi o da attività di gestione degli strumenti informatici, la Struttura Informatica e Innovazione Tecnologica, segnala gli episodi alla Segreteria Generale che potrà adottare le eventuali misure che consentano la verifica di tali comportamenti preferendo, per quanto possibile, un controllo preliminare su dati aggregati riferiti all'intera Struttura organizzativa o a sue articolazioni. Il controllo su dati anonimi si concluderà con una comunicazione al

Responsabile della Struttura analizzata che si preoccuperà di inviare un avviso generalizzato relativo a un utilizzo non corretto degli strumenti aziendali, invitando i destinatari ad attenersi scrupolosamente al presente Regolamento.

3. Qualora le anomalie e irregolarità dovessero persistere, si procederà circoscrivendo l'invito al personale afferente alla Struttura in cui è stata rilevata l'anomalia. In caso di reiterate anomalie o irregolarità, saranno effettuati controlli su base individuale. In nessun caso, a eccezione di specifica richiesta da parte dell'Autorità Giudiziaria, verranno poste in essere azioni sistematiche quali: la lettura e la registrazione dei messaggi di posta elettronica (al di là di quanto tecnicamente necessario per lo svolgimento del servizio di gestione e manutenzione della posta elettronica); la riproduzione ed eventuale memorizzazione delle pagine web visualizzate dal lavoratore; la memorizzazione di quanto visualizzato sul monitor. Oltre a ciò l''Ente si riserva di effettuare specifici controlli sui software caricati sui personal computer utilizzati dai dipendenti al fine di verificarne la regolarità sotto il profilo delle autorizzazioni e delle licenze, nonché, in generale, la conformità degli stessi alla normativa vigente e, in particolare, alle disposizioni in materia di proprietà intellettuale.

4. Oltre a tali controlli di carattere generale, la Provincia di Teramo si riserva comunque le facoltà previste dalla normativa vigente di effettuare specifici controlli ad hoc nel caso di segnalazioni di attività che hanno causato danno all'amministrazione, che ledono diritti di terzi o che, comunque, sono illegittime.

Capo X
Sanzioni

Art. 68 - Sanzioni

1. Gli operatori sono responsabili per qualsiasi utilizzo degli strumenti elettronici e informatici della Provincia di Teramo non conforme alle disposizioni del presente Regolamento e/o alle leggi vigenti.

2. La Provincia di Teramo monitorizza l'utilizzo della rete e verifica, nel pieno rispetto della normativa vigente in tema di privacy, l'attuazione delle disposizioni del presente regolamento.

3. Tutte le informazioni raccolte sono utilizzabili nei limiti dello Statuto dei lavoratori (L. 300 del 1970) e del Codice privacy (D.lgs 196 del 2003) e memorizzate per i periodi di tempo indispensabili al raggiungimento delle varie finalità perseguite.

4. Nei casi di accertata violazione di tali norme, è demandata ai rispettivi dirigenti l'applicazione dei necessari provvedimenti disciplinari, fermo restando l'obbligo di segnalare alla competente Autorità Giudiziaria eventuali violazioni costituente reato.

5. L'Ente ha il dovere di segnalare alle autorità competenti, per gli opportuni accertamenti ed i provvedimenti del caso, gli eventuali usi illeciti dei servizi informatici e telematici.

Capo XI
Disposizioni finali

Art. 69 - Aggiornamento e revisione

1. Tutti gli Operatori possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento.

2. Le proposte verranno esaminate dalle strutture competenti congiuntamente al Responsabile del Servizio Informatico.

3. Il presente Regolamento è soggetto a revisione con frequenza annuale.