PROVINCIA
DI VENEZIA

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

REDATTO AI SENSI E PER GLI EFFETTI DELL'ARTICOLO 34, COMMA 1, LETTERA G) DEL Decreto Legislativo 196/2003, E DEL DISCIPLINARE TECNICO ALLEGATO AL MEDESIMO DECRETO SUB B)

PROVINCIA
DI VENEZIA

INDICE

1. Premessa....3
2. Elenco dei trattamenti dei dati personali....3
2.1 Tipologie di dati trattati e categorie di soggetti cui si riferiscono....4
2.2 Locali in cui si effettuano i trattamenti in formato elettronico....4
2.3 Strumenti per il trattamento dei dati personali in formato elettronico....4
2.3.1 Server e SAN (Storage Area Network)....4
2.3.2 Personal computer....4
3. Trattamento dei dati all'esterno della Provincia....5
4. Ruoli....5
4.1 Responsabile della sicurezza....5
4.2 Incaricati....6
4.3 Amministratori di sistema informatico....7
4.4 Interventi formativi....8
5. Analisi dei rischi che incombono sui dati....9
6. Misure atte a garantire l'integrità e la disponibilità dei dati....11
6.1 La protezione di aree e locali....12
6.2 La custodia e l'archiviazione di atti, documenti e supporti....12
6.3 Accesso alle sale macchine e sicurezza dei locali tecnici....13
6.4 Le misure logiche di sicurezza adottate....13
6.4.1 Sistema di autenticazione....13
6.4.2 Sistema di autorizzazione....14
6.4.3 Sistema antivirus e antispam....15
6.4.4 Sistema distribuzione aggiornamenti....15
6.4.5 Sistema di controllo dei flussi di navigazione internet....15
6.4.6 Sistema di monitoraggio dei server....16
6.4.7 Sistema di backup dei dati....16
6.4.8 Sistema di protezione perimetrale....16
6.4.9 Video sorveglianza....16
7. Dismissione di Pc e Server....17
8. Controllo generale sullo stato della sicurezza....17
9. Dichiarazioni d'impegno e firma....18
10. Nuovo Sistema di Backup....18
11. Misure di scurezza da adottare....18
12. Schedari ed altri supporti cartacei....18
13. Storico dei principali aggiornamenti....19
14. Schema di lettera di nomina degli incaricati....20
15. Schema di lettera di nomina degli amministratori di sistema....24
Allegato sub A) - Elenco dei trattamenti
Allegato sub B) - Elenco degli archivi logici e fisici
Allegato sub C) - Procedure di salvataggio e ripristino dei dati

1. Premessa

Scopo di questo documento è di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, da adottare per il trattamento dei dati personali, sensibili e giudiziari effettuato dalla Provincia di Venezia.
Conformemente a quanto prescrive il punto 19. del Disciplinare tecnico, allegato sub b) al D.lgs. 196/2003, nel presente documento si forniscono idonee informazioni riguardanti:

1. l'elenco dei trattamenti di dati personali (*punto 19.1 del disciplinare*), mediante:
   - la individuazione dei tipi di dati personali trattati,
   - la descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti,
   - la elaborazione della mappa dei trattamenti effettuati
2. la distribuzione dei compiti e delle responsabilità, nell'ambito delle strutture preposte al trattamento dei dati e previsione di interventi formativi degli incaricati del trattamento *(punto 19.6 del disciplinare*);
3. l'analisi dei rischi che incombono sui dati (*punto 19.3 del disciplinare*);
4. le misure, già adottate e da adottare, per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità (*punto 19.4 del disciplinare*);
5. i criteri e le modalità di ripristino dei dati, in seguito a distruzione o danneggiamento (*punto 19.5 del disciplinare*);
6. le procedure da seguire per il controllo sullo stato della sicurezza;
7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati affidati, in conformità al Codice della Privacy (D.Lgs.196/03) all'esterno della struttura del titolare (*punto 19.7 del disciplinare*);
8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la separazione di tali dati dagli altri dati personali dell'interessato (*punto 19.8 del disciplinare)*;
9. dichiarazioni d'impegno e firma.

2. Elenco dei trattamenti dei dati personali

Al fine di elaborare l'elenco dei trattamenti dei dati, posti in essere dal Titolare, la Provincia di Venezia ha individuato un software applicativo che consente di censire i trattamenti dei dati effettuati dai servizi dell'ente: il software è denominato "Intranet-DPS". La raccolta delle informazioni relative ai trattamenti viene condotta in autonomia da ogni singolo Responsabile (dirigente) che utilizzando le proprie credenziali ed il sistema procede operando secondo le seguenti macro fasi:

- Individua i trattamenti di dati effettuati all'interno del proprio servizio e li definisce nell'applicativo .
- Individua gli incaricati di ogni trattamento e li assegna al trattamento stesso.
- Individua per ogni trattamento gli archivi/sistemi utilizzati per il trattamento distinguendo se cartaceo o informatizzato.

L'elenco dei dati trattati effettuati presso gli uffici dell'Ente è contenuto nell'allegato "Allegato sub A) - Elenco dei Trattamenti" nel quale vengono indicati i singoli trattamenti corredati dalle seguenti informazioni: tipo di dato

(personale, sensibile,giudiziario), cartaceo o informatizzato, servizio/settore di pertinenza, finalità di trattamento, modalità di trattamento, natura del dato, interessati dal trattamento, misure di sicurezza adottate.

L'elenco degli archivi logici e fisici nei quali vengono conservati i documenti è riportato nell'allegato "Allegato sub B) - Elenco Archivi logici e fisici".

2.1 Tipologie di dati trattati e categorie di soggetti cui si riferiscono

La Provincia di Venezia tratta i dati personali che appartengono a soggetti interessati in quanto autori, destinatari o partecipi di atti, contratti, elaborati, missive e documenti analoghi formati dall'Ente o indirizzati o, comunque detenuti da nell'ambito dello svolgimento delle sue attività istituzionali.

Il trattamento dei dati personali consiste nelle operazioni o complessi di operazioni di cui all'art. 4, lett. a) del D.Lgs. n.196/2003, nell'ambito delle attività istituzionali svolte dalla Provincia di Venezia.

Il trattamento dei dati sensibili e giudiziari è effettuato soltanto ove consentito da norme di legge o di regolamento che identifichino le finalità di interesse pubblico, i tipi di dati e le operazioni su di essi eseguibili.

2.2 Locali in cui si effettuano i trattamenti in formato elettronico

Il trattamento informatizzato dei dati personali avviene in ogni sede della Provincia di Venezia nella quale siano presenti dei personal computer. L'elenco delle sedi aggiornato è riportato all'interno della sezione "Servizi online" del portale Web della Provincia di Venezia.

2.3 Strumenti per il trattamento dei dati personali in formato elettronico

2.3.1 Server e SAN (Storage Area Network)

Per server e SAN si intendono i dispositivi dedicati al trattamento e all'archiviazione dei dati elettronici di qualsiasi natura. Tali dispositivi sono collegati fra loro tramite rete locale e geografica protetta da apparati anti intrusione meglio descritti nel seguito. Più specificatamente una **Storage Area Network** (**SAN**) è un'area rete ad alta velocità costituita esclusivamente da dispositivi di memorizzazione di massa. Il suo scopo è quello di rendere tali risorse di immagazzinamento (storage) disponibili per qualsiasi computer connesso ad essa.

I server possono ospitare applicativi ai quali gli utenti accedono con opportune credenziali e che consentono loro di svolgere le mansioni per le quali sono stati incaricati.

2.3.2 Personal computer

Quasi tutti i dipendenti sono dotati di un personal computer collegato alla rete provinciale. Alcuni dipendenti condividono un unico personal computer al quale accedono mediante login e password personali. In ogni pc sono predisposte delle aree di rete nelle quali l'utente assegnatario ha la possibilità di inserire cancellare o modificare dati, ma dei quali non è garantito il ripristino in corrispondenza di eventi che ne causino la perdita o il danneggiamento.

3. Trattamento dei dati all'esterno della Provincia

Trattamento dei dati affidato a terzi: nei casi in cui la Provincia di Venezia affida a terzi attività in outsourcing che comportino il trattamento di dati di cui sia titolare la Provincia, nel contratto di affidamento oltre a prevedere la nomina del contraente quale "responsabile esterno" del trattamento, devono essere indicate le seguenti modalità cui attenersi nel trattamento stesso:

- Impegno a comunicare per iscritto alla Provincia nella persona del dirigente responsabile del contratto, gli incaricati al trattamento dei dati.
- Quali sono i trattamenti che verranno effettuati dagli incaricati.
- Le finalità del trattamento sono esclusive all'espletamento dell'incarico ricevuto.
- Adempimento degli obblighi previsti dal Codice per la protezione dei dati personali.

Trattamento dei dati in quanto amministratori dei sistemi: secondo quanto prescritto dal provvedimento del Garante per la protezione dei dati personali "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008, in G.U. n. 300 del 24 dicembre 2008, verrà richiesta ai "titolari" del trattamento dei dati delle società terze, a cui sono affidati in outsourcing i trattamenti di dati, la lista degli amministratori di sistema che gestiscono tali trattamenti e l'attestazione (per iscritto) che tali amministratori possiedono le caratteristiche previste dalla legge.

4. Ruoli

La Provincia di Venezia individua, coerentemente con le definizioni di cui all'art. 4 del Codice in materia di protezione dei dati personali, Il Titolare del trattamento, i Responsabili del trattamento e gli Incaricati del trattamento rispettivamente ai sensi degli artt. 28,29,30 del nominato codice. Pertanto il Titolare del trattamento dei dati della Provincia di Venezia è individuato nella persona del suo Legale Rappresentante il Presidente.
I Responsabili del trattamento sono i Dirigenti ognuno per la propria competenza.
Sono incaricati del trattamento dei dati personali tutti i dipendenti dell'Ente, nonchè tutte le persone fisiche dipendenti delle ditte operanti a qualsiasi titolo per la Provincia che hanno accesso ai dati o in maniera diretta o in outsourcing sia in via telematica che cartacea per servizi erogati dalla Provincia di Venezia che abbiano ricevuto un formale incarico dai Responsabili del Trattamento. L'elenco aggiornato dei trattamenti e degli incaricati agli stessi, è registrato e aggiornato costantemente aggiornato all'interno del sistema Intranet-DPS.

4.1 Responsabile della sicurezza

E' **responsabile per la sicurezza** il dirigente del settore Informatica.

4.2 Incaricati

Il trattamento dei dati personali sensibili e giudiziari viene effettuato solo da **soggetti che hanno ricevuto un formale incarico**, da parte del Responsabile (il Dirigente), mediante designazione per iscritto di ogni singolo incaricato, con il quale si individua puntualmente l'ambito del trattamento consentito.

Si riporta al paragrafo 13 del presente documento lo schema di lettera di nomina degli incaricati, da inserire, debitamente compilata, nel dossier del Settore.

Il codice, ed il relativo disciplinare tecnico, impongono ai soggetti che trattano dati personali di essere incaricati formalmente del trattamento mediante una lettera di incarico, che andrà raccolta, assieme a tutte le lettere di incarico di ogni Settore, in un dossier da conservare all'interno di ciascun Settore interessato.

Ogni dossier dovrà essere aggiornato annualmente.

La lettera di incarico costituirà e conterrà il profilo di autorizzazione del soggetto al trattamento dei dati personali, sensibili e giudiziari ed individuerà puntualmente l'ambito di trattamento consentito.

Il dossier, tenuto a cura del Dirigente responsabile del Settore del trattamento dei dati, conterrà tutte le nomine dei dipendenti quali incaricati nel proprio Settore, per ordine di mansioni e di attività svolte in ordine ai dati personali, sensibili e giudiziari.

E' possibile, per comodità, creare dei profili di autorizzazione in relazione a classi omogenee di incarichi che riguardino tutti i soggetti addetti allo stesso tipo di attività concernenti il trattamento di dati personali, sensibili e giudiziari, pur nella diversità delle diverse mansioni espletate.

I soggetti che svolgeranno attività ricomprese in classi omogenee di incarico otterranno il profilo di autorizzazione di classe di incarico.

Per i trattamenti effettuati con strumenti elettronici, si deve provvedere all'autorizzazione al trattamento dei dati di coloro che gestiscono o effettuano la manutenzione di tali strumenti mediante apposite lettere di incarico che individuino l'ambito del trattamento consentito.

L'individuazione agli addetti alla gestione o alla manutenzione di tali strumenti dovrà essere aggiornata periodicamente, almeno ogni anno.

Il dossier, dunque, conterrà:

- le singole nomine degli incaricati e le attività che sono loro consentite in relazione ai tipi di dati;
- i profili di autorizzazione per classi omogenee di incaricati accomunati dal trattamento dei medesimi tipi di dati;
- l'ambito del trattamento consentito agli addetti alla gestione o alla manutenzione di tali strumenti, con l'individuazione specifica dei medesimi.

Il dossier dovrà essere aggiornato annualmente sotto tutti e tre i profili ora descritti.

La copia informatizzata del dossier risiede nel sistema "Intranet-DPS" nel quale vengono riportati per ogni servizio il Responsabile individuato (dirigente) e gli incaricati. Il sistema tiene traccia degli aggiornamenti e delle modifiche ai profili degli incaricati operate dai responsabili dei servizi.

Qualora si rilevassero dati diversi da quelli sensibili o giudiziari che, a giudizio dei responsabili dei Settori operanti, presentino dei rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato,

in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che esso potrebbe determinare, il trattamento è consentito nel rispetto delle medesime misure e accorgimenti prescritti per quello dei dati sensibili e giudiziari.

4.3 Amministratori di sistema informatico

In base al provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, pubblicato nella Gazzetta Ufficiale n.300 del 24 dicembre 2008, l' attribuzione di amministratore di sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità. Verificate le suddette caratteristiche, il soggetto viene incaricato dal Responsabile della sicurezza tramite lettera di designazione individuale recante l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato tramite la lettera di nomina il cui schema è riportato al paragrafo 14 del presente DPS.

A tal proposito sono stati individuati tre profili di amministratore di sistema che vengono descritti nella sottostante tabella:

PROFILO RETE	Abilitato al trattamento (come definito dal codice) dei dati personali nell'ambito della gestione delle risorse della rete aziendale e dei DB: profili di rete, posta elettronica, fax informatici, file sharing, back-up di dati, monitoraggio traffico di rete, gestione accesso alle aree di rete, monitoraggio dei sistemi in genere.
PROFILO APPLICATIVI	Abilitato al trattamento (come definito dal codice) dei dati personali nell'ambito della gestione degli applicativi e dei DB: protocollo, contabilità, personale (cedolini stipendi, presenze), atti dell'Ente (delibere, determinazioni, firma digitale) e tutti gli altri applicativi di gestione settoriale.
PROFILO WEB	Abilitato al trattamento (come definito dal codice) dei dati personali e dei DB nell'ambito della gestione del web: intranet aziendale, sito della provincia e dei vari settori, posta elettronica utenti esterni (comuni), portali web dei Comuni, gestione DNS, gestione della DMZ in genere.

Gli estremi idenitificativi delle persone fisiche "amministratori di sistema", con l'elenco delle funzioni ad esse attribuite, è riportato sul portale intranet dell'Ente.

Gli **amministratori di Sistema** sovraintendono alle risorse del sistema informatico dell'Ente.

L'Amministratore di Sistema opera personalmente e dà direttive in relazione alle operazioni di trattamento dei dati personali cercando di evitare i rischi di distruzione o perdita, anche accidentale dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta, come previsto dal d. lgs. 196/03.

L'Amministratore di Sistema con profilo Rete avrà tra i suoi compiti quelli di:

- Disattivare i codici identificativi in caso di perdita della qualità degli stessi o di mancato utilizzo per un periodo superiore a sei mesi;
- Proteggere gli elaboratori contro i rischi di intrusione, mediante l'utilizzo di appositi programmi;
- Verificare l'efficacia e l'aggiornamento del software antivirus;
- Collaborare con i responsabili del trattamento dei dati personali alla stesura e all'aggiornamento del presente documento;
- Distruggere i supporti di memorizzazione nel caso non siano più riutilizzabili;
- Vigilare sul buon utilizzo dell'hardware e del software dato in dotazione agli utenti.
- Regolare le policy di accesso alle risorse della rete in base ai profili assegnati.

L'amministratore di Sistema con profilo Applicativi avrà tra i suoi compiti quelli di:

- individuare eventuali malfunzionamenti nelle procedure ed attuare le adeguate misure preservando l'integrità dei dati.
- Regolare le policy di accesso alle procedure del sistema in base ai profili assegnati.
- Gestire i profili di accesso agli applicativi
- Supervisionare i sistemi in modo da garantirne la funzionalità operativa.
- Implementazione e integrazione dei flussi informativi

L'amministratore di Sistema con profilo Web avrà tra i suoi compiti quelli di:

- Agire con profilo di superutente sui server nei quali sono installati i portali web ospitati dall'ente con la finalità di monitorarne lo stato per l'individuazione di eventuali tentativi di accesso fraudolenti.
- Supportare gli utenti nella gestione dei portali.
- Gestire il sistema di posta elettronica degli enti e delle amministrazioni ospitati nei sistemi della Provincia di Venezia.

Secondo quanto prescritto dal provvedimento del Garante per la protezione dei dati personali, verrà richiesta ai "titolari" del trattamento dei dati delle società terze, a cui sono affidati in outsourcing i trattamenti di dati, la lista degli amministratori di sistema che gestiscono tali trattamenti e l'attestazione (per iscritto) che tali amministratori possiedono le caratteristiche previste dalla legge.
Gli accessi effettuati dagli amministratori di sistema verranno registrati da un sistema di log predisposto in otemperanza a quanto previsto del provvedimento del Garante.

4.4 Interventi formativi

La Provincia di Venezia tramite il servizio Personale, nell'ambito del piano triennale di formazione a disposizione presso gli uffici, organizza interventi formativi in materia di sicurezza e di privacy.

5. Analisi dei rischi che incombono sui dati

E' necessario individuare i principali eventi potenzialmente dannosi per la sicurezza dei dati valutandone le possibili conseguenze e la gravità ponendoli in correlazione con le misure previste.

Si individua nella tabella che denominiamo 'Tabella di rischio', l'elenco degli eventi che possono essere causa di danni e che comportano quindi rischi per la sicurezza ed integrità dei dati personali.

In relazione a ciascun evento viene individuata una contromisura da adottare in relazione alla valutazione della gravità dell'evento stesso e alla probabilità stimata che esso si verifichi.

Le componenti di rischio possono essere idealmente suddivise in:

1. rischio legato ad atti di sabotaggio e ad errori umani, da parte del personale appartenente all'organizzazione del Titolare, o di persone che con essa hanno stretti contatti.

2. rischio di guasti tecnici delle apparecchiature, che interessa in particolare gli strumenti elettronici (risorse hardware, software e supporti) e rischio di penetrazione logica nelle reti di comunicazione

3. rischio di area, che dipende dal luogo dove gli strumenti sono ubicati. Tale rischio è legato sostanzialmente:

- al verificarsi di eventi distruttivi o alla perdita di dati (incendi, allagamenti, corti circuiti, smarrimento documenti)
- alla possibilità che terzi malintenzionati accedano nei locali dove si svolge il trattamento (rapine, furti, danneggiamenti da atti vandalici)

TABELLA DI RISCHIO

Evento		**Gravità stimata**	**Proba-bilità stimata**	**Coeff. di rischio**	**Misure d'azione per sventurare il rischio e per garantire l'integrità e la disponibilità dei dati**
Comporta-menti degli operatori	carenza di consapevolezza, disattenzione o incuria	8	8	64	Formazione specifica sulle conseguenze di atteggiamenti sbagliati rispetto alle norme di tutela dei dati personali contenute nel codice e rispetto alla corretta custodia dei dati trattati e delle credenziali di autenticazione assegnate.
	comportamenti sleali o fraudolenti	8	1	8	Sottoscrizione del "regolamento sull'utilizzo delle risorse informatiche".(Rif.4.4)
	errore materiale	8	6	48	Verifica e controllo da parte dei responsabili dei trattamenti sui comportamenti degli incaricati interni ed esterni. Formazione specifica sull'utilizzo delle risorse informatiche.
Eventi relativi agli strumenti	azione di virus informatici o di codici malefici	8	8	64	Aggiornamento giornaliero dell'antivirus (Rif.6.4.3,6.4.5)

TABELLA DI RISCHIO

Evento		**Gravità stimata**	**Proba-bilità stimata**	**Coeff. di rischio**	**Misure d'azione per sventurare il rischio e per garantire l'integrità e la disponibilità dei dati**
	spamming o altre tecniche di sabotaggio	8	10	80	Corretta gestione dei firewall e adeguato sistema di autenticazione e autorizzazione all'accesso da parte degli incaricati e dei responsabili del trattamento ai dati presenti nella rete interna (Rif. 6.4.1,6.4.2).
	malfunzionamento, indisponibilità o degrado degli strumenti	6	8	48	Adeguato sistema antispam e antivirus su server dedicati di posta elettronica (Rif. 6.4.3)
	accessi esterni non autorizzati	10	2	20	Periodica verifica dello stato di obsolescenza delle attrezzature informatiche assegnate agli incaricati e conseguente rinnovo o implementazione delle stesse.(Rif.7)
	intercettazione di informazioni in rete	5	2	10	Aggiornamento mensile dei sistemi operativi dei server e dei PC.(Rif.6.4.4)
					Esecuzione di opportuni back-up periodici (giornalieri, settimanali e annuali) dei server (Rif.6.4.7)
Eventi relativi al contesto	accessi non autorizzati a locali/reparti ad accesso ristretto	10	5	50	Formazione specifica sui comportamenti di tutela dei dati quali: chiusura a chiave degli armadi contenenti dati personali, chiusura dei cassetti,
	asportazione e furto di strumenti contenenti dati	8	1	8	chiusura delle porte degli uffici al di fuori del normale orario di lavoro.(Rif 4.4)
	eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	8	1	8	Sistemi di video sorveglianza.(Rif. 6.3) Installazione di opportuna cassaforte a norma per la custodia dei nastri di back-up.(Rif.6.4.7)
	guasto ai sistemi complementari (impianto elettrico, climatizzazione, ...)	2	7	14	Verifica del corretto funzionamento dei gruppi di continuità a supporto dei server.(Rif. 6.3)
	errori umani nella gestione della sicurezza fisica	3	3	9	Periodiche verifiche delle procedure di ripristino dei dati come descritto dal documento "Procedure di Salvataggio e Ripristino dei dati.docx"(Rif.6.4.7) Verifica del corretto funzionamento dei condizionatori delle sale macchine con la predisposizione di opportune segnalazioni di controllo in caso di avaria (SMS)(Rif.6.3)

- La gravità dell'evento viene stimata in ordine di gravità crescente da 1 a 10 punti.
- La probabilità che l'evento si verifichi viene stimata in ordine di probabilità crescente da 1 a 10 punti.
- Il coefficiente di rischio di ciascun evento si ottiene moltiplicando fra loro i due indici di gravità e probabilità. La scala del coefficiente di rischio va da 1 a 100.

Il grado di rischio più alto, o addirittura elevatissimo, è collegato al trattamento dei dati, sensibili e giudiziari, alla tutela dei quali devono quindi essere dedicate particolari attenzioni, come ad esempio la stesura degli atti utilizzando codici.
Come evidenziato dall'elenco dei dati trattati, esistono delle aree di rete e dei sistemi nei quali sono ubicati dati sensibili o giudiziari: nel primo caso l'accesso può essere effettuato esclusivamente da utenti dotati di opportuni codici identificativi di accesso e di particolari autorizzazioni e i dati sono ubicati in aree di rete separate dalle altre, mentre nel secondo caso i dati sono contenuti in database accessibili solamente tramite sistemi proprietari che possono essere utilizzati dagli utenti muniti di particolari credenziali di accesso di cui dispongono in maniera esclusiva .

6. Misure atte a garantire l'integrità e la disponibilità dei dati

Tutti i posti di lavoro della Provincia di Venezia sono collegati in rete locale e/o geografica e l'accesso agli stessi è consentito previa sottoscrizione da parte degli utilizzatori di apposito regolamento che contiene le modalità di corretto utilizzo delle attrezzature assegnate e dei programmi installati. Tramite la sottoscrizione del regolamento, il soggetto utilizzatore si assume contestualmente la responsabilità civile e penale sull'utilizzo di hardware, software e dati.
In relazione al proprio sistema informatico, l'Ente si dota delle misure minime di sicurezza, così come prescritto all'art. 33, nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31 del d. lgs 196/2003.

Nel presente paragrafo vengono descritte nel dettaglio e ad integrazione con le misure d'azione idonee descritte nella precedente tabella (paragrafo 3.) le misure atte a garantire:

- la protezione delle aree e dei locali (Misure Minime Fisiche), nei quali si svolge il trattamento dei dati personali,
- la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali, sensibili e giudiziari,
- la sicurezza logica, nell'ambito dell'utilizzo degli strumenti elettronici.

Si procede ora alla descrizione delle misure che risultano già adottate dal Titolare, nel momento in cui viene redatto il presente documento

6.1 La protezione di aree e locali

Per quanto concerne il rischio d'area, legato ad eventi di carattere distruttivo, gli edifici ed i locali nei quali si svolge il trattamento sono protetti come risulta dalle seguenti tabelle:

Descrizione misura	Note ed indicazioni per la corretta applicazione
Custodia degli archivi cartacei in armadi chiusi a chiave	Tutti i documenti cartacei contenenti dati personali di tipo sensibile e giudiziario sono conservati in armadi dotati di serratura e, per quelli attinenti allo stato di salute o alla vita sessuale dei soggetti interessati, in maniera separata dai dati personali trattati per finalità che non ne richiede il loro utilizzo. Sarà compito dell'incaricato che preleva i documenti garantire che i documenti siano riposti, sotto chiave al termine delle operazioni di trattamento.
Dispositivi antincendio	Tutti gli uffici, sono dotati di estintori regolarmente revisionati.
Controllo dell'operatore esterno addetto alla manutenzione	Gli addetti alla manutenzione sono sempre accompagnati dal personale dipendente della Provincia di Venezia con la finalità di controllarne l'operato
Cassaforte	La Provincia di Venezia. dispone di una cassaforte idonea a trattenere le copie di Back-Up e le parole chiave.
Portineria	L'Ente Pubblico effettua servizio di portineria in quasi tutti gli edifici. Solo in particolari casi l'accesso avviene previo controllo dei dipendenti. Nel caso di archivi contenenti dati sensibili o giudiziari, possono accedervi soltanto persone autorizzate ed i dipendenti, dopo l'orario di chiusura al pubblico, provvedono ad identificare chi accede.
Allarme antifurto	In tutti gli edifici provinciali è stato istallato un allarme di tipo volumetrico e sensoriale

6.2 La custodia e l'archiviazione di atti, documenti e supporti

Per quanto concerne il reperimento, la custodia e l'archiviazione di atti, documenti e supporti diversi (ad esempio, CD, fotografie, filmati ecc.), si è provveduto ad istruire gli incaricati, affinché adottino precise procedure atte a salvaguardare la riservatezza dei dati contenuti.

6.3 Accesso alle sale macchine e sicurezza dei locali tecnici

La Provincia di Venezia è dotata di 5 locali definiti Sala Macchine o CED. I locali sono ubicati presso:

- Centro Servizi, Via Forte Marghera 191 Mestre – Sede Principale
- Cà Corner, S. Marco 2662 Venezia – Sede Storica
- Via Catene 95 Marghera – Sede Vigili

Tutti i locali sono chiusi a chiave e dotati di impianto di condizionatore e gruppi di continuità opportunamente dimensionati rispetto ai carichi elettrici necessari. I locali sono costantemente sorvegliati da personale dell'ente e l'accesso agli stessi è autorizzato al solo personale del settore informatica dotato di badge di accesso opportunamente configurato. I gruppi di continuità delle sale macchine vengono verificati annualmente con dei test eseguiti da personale tecnico specializzato.

Considerato che i locali CED del Centro Servizi e di Cà Corner sono quelli che contengono la gran parte dei sistemi e degli storage sono stati dotati di un sistema di monitoraggio con videocamera che segnala accessi ai locali tramite email: la funzione del sistema è quella di evidenziare eventuali accessi non autorizzati. Le sale macchine sono dotate di sistemi di rilevazione incendio e di un sistema di rilevazione della temperatura che segnala al personale responsabile tramite SMS ed email, l'aumento di temperatura dei locali consentendo un tempestivo intervento.
I locali sala macchine di Cà Corner del Centro Servizi e di via Corso del Popolo sono dotati di un sistema di accesso e monitoraggio comandato remotamente che consente l'apertura dei varchi qualora per interventi tecnici si renda necessario l'accesso ai locali: le credenziali di accesso ai sistemi sono in possesso degli "Amministratori di rete" così come definiti nel paragrafo" 4.3 Amministratori di sistema informatico".

6.4 Le misure logiche di sicurezza adottate

6.4.1 Sistema di autenticazione

Il **sistema di autenticazione informatica** viene adottato per disciplinare gli accessi a tutti gli strumenti elettronici, presenti nell'organizzazione del Titolare.

E' impostata e gestita una **procedura di autenticazione**, che permette di verificare l'identità della persona, e quindi di accertare che la stessa sia in possesso delle credenziali di autenticazione per accedere ad un determinato strumento elettronico.

Per realizzare le credenziali di autenticazione si utilizza il seguente metodo: si associa un codice per l'identificazione dell'incaricato (*username)*, ad una parola chiave riservata (*password*), conosciuta solamente dall'incaricato, che provvederà ad elaborarla, mantenerla riservata e modificarla trimestralmente.
Per l'attribuzione e la gestione delle credenziali per l'autenticazione si utilizzano i seguenti criteri:

- ad ogni incaricato esse vengono assegnate e associate individualmente, per cui non è ammesso che due o più incaricati possano accedere agli strumenti elettronici utilizzando la medesima credenziale;
- è invece ammesso, qualora sia necessario o comunque opportuno, che ad una persona venga assegnata più di una credenziale di autenticazione.

Agli incaricati vengono impartite precise istruzioni in merito ai seguenti punti:

- dovere di custodire i dispositivi, attribuiti agli incaricati a titolo di possesso ed uso esclusivo, con i quali si può accedere agli strumenti informatici (ad esempio la smart card): la custodia deve avvenire in modo diligente, sia nell'ipotesi in cui tali dispositivi siano riposti negli uffici (viene prescritto l'obbligo di utilizzare cassetti con serratura), che in quella in cui l'incaricato provveda a portare il dispositivo con sé (viene prescritto l'obbligo di custodirlo come se fosse una carta di credito). In ipotesi di smarrimento, l'incaricato deve provvedere immediatamente a segnalare la circostanza all'amministratore di sistema, o alle altre persone che sono state a tale fine indicate, al momento dell'attribuzione del dispositivo;
- obbligo di non lasciare incustodito e accessibile lo strumento elettronico, durante una sessione di trattamento, neppure in ipotesi di breve assenza;
- dovere di elaborare in modo appropriato la password, e di conservare la segretezza sulla stessa. Agli incaricati è imposto l'obbligo di provvedere a modificare la password, con la seguente tempistica:
  - immediatamente, non appena viene consegnata loro da chi amministra il sistema
  - successivamente trimestralmente. Il cambio della password di accesso alla rete e di tutte le applicazioni integrate è imposto ogni tre mesi dal sistema di autenticazione tramite policy. L'utente viene avvisato all'avvicinarsi della scadenza attraverso messaggi di posta elettronica.

  Le password sono composte da almeno otto caratteri numerici e alfanumerici oppure, nel caso in cui lo strumento elettronico non permetta una tale lunghezza, da un numero di caratteri pari al massimo consentito dallo strumento stesso.

  - Le password, per maggiore sicurezza, non devono contenere riferimenti agevolmente riconducibili all'interessato, quali date di nascita o nomi dei figli.

La password non deve essere comunicata a nessuno. Nei casi di prolungata assenza o impedimento dell'incaricato, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, potrebbe però rendersi necessario disporre della password dell'incaricato, per accedere agli strumenti ed ai dati. A tale fine i responsabili chiedono all'amministratore di sistema di sostituire la password dell'incaricato assente, assumendo l'obbligo di comunicare tempestivamente al medesimo l'operazione effettuata e gli accessi avvenuti. L'incaricato, rientrando in servizio, provvederà tempestivamente alla modifica della propria password.

6.4.2 Sistema di autorizzazione

Per quanto concerne le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, si osserva che: si è impostato un **sistema di autorizzazione**, al fine di circoscrivere le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, a quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative. L'unica eccezione si ha nei casi in cui il trattamento riguardi

solo dati personali destinati alla diffusione: in questo caso non è necessario predisporre alcun sistema di autorizzazione, poiché i dati trattati sono, per definizione, conoscibili da chiunque.
Le autorizzazioni all'accesso vengono rilasciate e revocate dal responsabile della sicurezza dei sistemi, ovvero da soggetti da questi appositamente incaricati (amministratore di sistema). Il profilo di autorizzazione può essere studiato per ogni singolo incaricato ovvero per classi omogenee di incaricati.

Periodicamente, e comunque almeno annualmente, viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione: ciò per quanto riguarda l'ambito di trattamento consentito sia ai singoli incaricati, che agli addetti alla manutenzione e gestione degli strumenti elettronici.

6.4.3 Sistema antivirus e antispam

Per quanto riguarda la protezione, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus), vengono adottate le misure sotto descritte.
Il primo aspetto riguarda la protezione dei dati personali dal rischio di intrusione e dall'azione di programmi di cui all'articolo 615-quinquies del codice penale, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento (comunemente conosciuti come virus).
A tale fine, l'Ente si è dotato di idonei strumenti elettronici e programmi, che il Dlgs 196/2003 imporrebbe di aggiornare con cadenza almeno semestrale, ma che, in relazione al continuo evolversi dei virus, si è ritenuto opportuno di sottoporre ad aggiornamento, di regola giornalmente. Il sistema antivirus è centralizzato: gli aggiornamenti e lo stato dei pc vengono controllati da un console residente su un server. Ulteriore accorgimento di difesa perimetrale è la presenza di un agente antispam, ospitato esternamente alla rete provinciale, che filtra tutta la posta in entrata e in uscita.
Tutti gli incaricati sono stati istruiti, in merito all'utilizzo dei programmi antivirus e, più in generale, sulle norme di comportamento da tenere, per minimizzare il rischio di essere contagiati: a tale fine, è stato loro distribuito un regolamento dei comportamenti da tenere, e di quelli da evitare ed è stata pretesa la sottoscrizione dello stesso.

6.4.4 Sistema distribuzione aggiornamenti

Dato che la vulnerabilità dei pc è inversamente proporzionale al loro grado di aggiornamento in termini di sistema operativo e programmi, ci si è dotati di un apposito programma la cui funzione è la verifica di eventuali inconsistenze e inesattezze nella configurazione dei sistemi operativi e dei servizi di rete, e di correggere di conseguenza i difetti insiti negli strumenti stessi.

6.4.5 Sistema di controllo dei flussi di navigazione internet

Nel rispetto della delibera del Garante n. 13 del 1 marzo 2007 recante le linea guida per posta elettronica e internet,gli accessi degli utenti ad internet sono filtrati da un sistema di controllo centralizzato che consente di inibire l'accesso a determinati siti web che possono essere bloccati singolarmente oppure per categoria di appartenenza. Il sistema permette di attribuire autorizzazioni diverse ad ogni singolo utente delle rete o a gruppi di utenti.

6.4.6 Sistema di monitoraggio dei server

È in fase di implementazione un sistema di monitoraggio dello stato dei server che attraverso l'analisi di messaggi di allerta permetterà un intervento tempestivo dei tecnici specialisti in caso di malfunzionamento o rottura di un server o di un suo componente.

In caso di guasto di un server o di un suo componente, l'intervento di manutenzione viene garantito entro 8 ore lavorative successive alla segnalazione.

In caso di guasto di un personal computer o di un suo componente l'intervento di manutenzione viene garantito entro il giorno lavorativo successivo alla segnalazione.

6.4.7 Sistema di backup dei dati

La rete della Provincia di Venezia è dotata di un sistema che esegue il salvataggio di tutti i dati presenti nei dischi di rete e nei server dell'ente con cadenza giornaliera. I backup vengono conservati sia su unità disco appositamente predisposte che su unità nastro.

Per fronteggiare le ipotesi in cui i dati siano colpiti da eventi che possano danneggiarli, o addirittura distruggerli, vengono previsti criteri e modalità tali, da garantire il loro ripristino in termini ragionevoli, e comunque entro una settimana per i dati sensibili e giudiziari.

I sistemi e le modalità con la quale vengono realizzati i salvataggi sono meglio descritti nel documento "Allegato 3 - Procedure di Salvataggio e Ripristino dei dati" agli atti presso l'ufficio informatica.

In sintesi, per i dati trattati con strumenti elettronici, sono previste procedure di back up, attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema, su dispositivi opportuni.

Il salvataggio dei dati trattati avviene come segue:

settimanale il sabato;

- incrementale giornaliero ogni giorno lavorativo della settimana;
- ad ogni salvataggio si utilizza un supporto differente da quello in cui sono contenuti i dati dei salvataggi eseguiti la volta precedente. Il ciclo si conclude ogni 15 giorni;
- ogni mese viene eseguito un salvataggio completo.
- le copie mensili vengono custodite in una cassaforte ignifuga dislocata nell'area ad accesso controllato durante l'orario di lavoro;

6.4.8 Sistema di protezione perimetrale

La **protezione degli elaboratori in rete dall'accesso abusivo, di cui all'articolo 615-ter del codice penale**, ai sensi del quale compie tale reato chi si introduce abusivamente in un sistema informatico o telematico, è garantita da misure di sicurezza, che impediscono tali accessi avviene l'impiego di idonei strumenti elettronici, comunemente ricompresi tra i **firewall** e i sistemi di autenticazione.

6.4.9 Video sorveglianza

Tra le misure di sicurezza previste sono stati implementati dei sistemi di video sorveglianza di alcuni ambienti delle sedi provinciali, nella fattispecie sono state installate telecamere presso:

- l'area parcheggio (piano -1 e piano -2) del Centro Servizi a Mestre,
- la sala server del Centro Servizi a Mestre
- la sala server
- Portineria di Ca' Corner a Venezia.

Nei siti nei quali tali servizi sono operativi, sono presenti delle targhe segnaletiche che indicano la presenza di telecamere. Il monitoraggio viene effettuato al solo scopo di individuare accesi non autorizzati.

7. Dismissione di Pc e Server

In otemperanza a quanto previsto dal provvedimento del Garante sullaa Privacy "**Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali " del 13 ottobre 2008** *G.U. n. 287 del 9 Dicembre 2008,* e a seguito dei piani di svecchiamento delle Postazioni di Lavoro previsti nei contratti di manutenzione Global Service, la Provincia di Venezia ha adottato misure idonee a garantire la corretta distruzione dei dati presenti nei dischi dei PC e dei Server non più utilizzabili, secondo la seguente modalità:

- Qualora i PC/Server vengano reutilizzati donandoli ad associazioni o ad enti che ne facciano richiesta, prima di procedere con la consegna dei dispositivi si procede alla cancellazione sicura dei dati contenuti nei dischi utilizzando un opportuno software che riscrive sequenze di bit annullando di fatto la possibilità di recuperare il contenuto precedentemente memorizzato.
- Nel caso in cui il PC/Server venga dismesso in quanto non più efficacemente reutilizzabile, si utilizzano delle procedure hardware di degaussing dei dischi che li rendono inutilizzabili.

8. Controllo generale sullo stato della sicurezza

Al responsabile per la sicurezza, ovvero al Dirigente del Settore Informatica, è affidato il compito di aggiornare le misure di sicurezza, al fine di adottare gli strumenti e le conoscenze, resi disponibili dal progresso tecnico, che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito.

Al fine di verificare l'efficacia delle misure di sicurezza adottate, i responsabili e le persone da questi appositamente incaricati provvedono, anche con controlli a campione, ad effettuare una o più delle seguenti attività:

- verificare l'accesso fisico ai locali dove si svolge il trattamento;
- verificare la correttezza delle procedure di archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- monitorare l'efficacia ed il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici, mediante l'analisi dei log file, nei quali i software di sicurezza installati, i sistemi operativi e le applicazioni o le operazioni svolte dagli incaricati per il loro tramite. Attraverso questa analisi, che viene effettuata adottando strumenti automatici di reportistica e di sintesi, è possibile individuare i tentativi, riusciti o meno, di accesso al sistema e l'esecuzione di operazioni non corrette, o sospette;
- verificare l'integrità dei dati e delle loro copie di back up;

- verificare la sicurezza delle trasmissioni in rete;
- verificare che i supporti magnetici, che non possono più essere riutilizzati, vengano distrutti;
- verificare il livello di formazione degli incaricati.

Almeno ogni tre mesi, si procede ad una sistematica verifica del corretto utilizzo delle parole chiave e dei profili di autorizzazione che consentono l'accesso agli strumenti elettronici da parte degli incaricati, anche al fine di disabilitare quelli che non sono stati mai utilizzati in sei mesi.

9. Dichiarazioni d'impegno e firma

L'originale del presente documento viene custodito presso la sede dell'ente, per essere esibito in caso di controlli; inoltre sarà pubblicato nel portale della Provincia di Venezia.

Una sua copia verrà consegnata a chiunque ne faccia richiesta, in relazione all'instaurarsi di un rapporto che implichi un trattamento congiunto di dati personali.

10.Nuovo Sistema di Backup

Nel corso del 2010 l'Ente ha adottato un nuovo sistema di salvataggio dei dati su disco, ridondando i dati presenti presso le due sedi principali: i dati della sede Ca' Corner vengono salvati su di uno storage presente presso la sala macchine della medesima sede e quindi vengono replicati presso la sala macchine della sede Centro servizi; lo stesso avviene per i dati salvati presso la sala macchine del centro servizi che vengono duplicati presso la sala Macchine di Ca' corner. Questo consente di ridurre il fattore di rischio di perdita dei dati dovuti a disastri naturali o da furti.

11. Misure di scurezza da adottare

Per migliorare ulteriormente il livello di protezione dei dati, la Provincia di Venezia ha messo allo studio per il 2011 compatibilmente con le risorse disponibili, l'installazione di un sistema di protezione anti incendio presso il locale sala macchine del Centro Servizi di via Forte Marghera 191 con caratteristiche adeguate a preservare lo stato dei sistemi in caso di incendio; è previsto inoltre il perfezionamento delle modalità di protezione dei trattamenti informatizzati di dati sensibili e giudiziari.

12. Schedari ed altri supporti cartacei

I supporti cartacei, ivi quelli contenenti immagini, vengono ordinatamente raccolti in schedari, ovvero nella pratica cui si riferiscono, per essere archiviati, una volta terminato il ciclo lavorativo, come segue:

- gli archivi contenenti dati relativi allo stato di salute e dati sensibili in generale e giudiziari sono localizzati in tutte le aree, in cui si raccolgono le pratiche e gli schedari, ma sono conservati in armadi o cassetti chiusi a chiave in maniera separata dagli altri dati trattati per finalità che non ne richiedano il loro utilizzo;
- gli archivi contenente dati personali in generale sono collocati presso tutti gli uffici. Sono adottate idonee cautele atte a garantire la riservatezza degli interessati, quali custodia dei documenti all'interno di fascicoli

privi di indicazioni anagrafiche, anche se non necessariamente i fascicoli sono chiusi in contenitori muniti di chiave.

- Nell'" Allegato 2 -Elenco degli archivi logici e fisici", vengono riportati tutti gli archivi nei quali i diversi servizi /settori dell'ente archiviano i trattamenti cartacei.

13. Storico dei principali aggiornamenti

Nel **2010** il documento programmatico sulla sicurezza è stato adeguato secondo quanto previsto da:

- la delibera nr. 13 del garante del marzo 2007
- il provvedimento del Garante per la protezione dei dati personali dal titolo "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008, in G.U. n. 300 del 24 dicembre 2008
- il provvedimento del Garante per la protezione dei dati personali dal titolo "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali" del 13 ottobre 2008, in G.U. n. 287 del 9 dicembre 2008

Attualmente la Provincia di Venezia ha adottato un sistema informatizzato di raccolta dei trattamente effettuati nei diversi settori dell'ente eleaborando un archivio elettronico sui trattamenti stessi.

Venezia, li …….

14. Schema di lettera di nomina degli incaricati

Venezia .....
Al Signor/ Alla Signora .....

Oggetto: Lettera di incarico per il trattamento dei dati personali

D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"; "Allegato B": "Disciplinare tecnico in materia di misure.
Il/La sottoscritto/a ..... , in qualità di Responsabile del trattamento dei dati personali ex art.29 del D.Lgs. 196/2003, per il Servizio .....
• visto il Decreto Legislativo 30 giugno 2003, n. 196. "Codice in materia di protezione dei dati personali", di seguito definito "Codice";
• premesso che Il Titolare del Trattamento è Titolare del trattamento dei dati personali, ai sensi dell'art 28 del D.Lgs. 196/2003;
• preso atto che l'art. 4, comma 1, lettera h) del suddetto Decreto definisce "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
• atteso che l'art.30 del D.Lgs. 30 giugno 2003, n. 196, dispone che:
Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.
La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad un'unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.
Ciò premesso, in applicazione del "Codice in materia di protezione dei dati personali" (D.Lgs. 196/2003), con la presente La nomino Incaricato del trattamento dei dati personalità relativamente a quanto di seguito dettagliata:

Nello specifico Le sono stati assegnati per quanto concerne questa unità in uso e custodia i seguenti trattamenti informatizzati:

Tabella con elenco dei trattamenti

Inoltre Le sono stati assegnati per quanto concerne questa unità in uso e custodia i seguenti trattamenti cartacei:

Tabella con elenco dei trattamenti

Per le banche dati non informatizzate Le è affidato uso e custodia dei seguenti archivi:

Tabella con elenco degli archivi assegnati

L'incaricato del trattamento dei dati dovrà, nello svolgimento dei compiti ad esso assegnati quale dipendente/collaboratore/consulente della Provincia di Venezia:

1. adottare ogni accorgimento necessario ad assicurare l'integrità e riservatezza dei dati dei quali comunque venga a conoscenza;
2. curare che il trattamento avvenga in modo lecito e secondo correttezza, riguardi dati esatti, pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati, provvedendo, se necessario, al loro aggiornamento e che la loro raccolta e registrazione avvenga per scopi determinati, espliciti e legittimi;
3. trattare i soli dati sensibili e giudiziari la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati, conservarli fino alla loro restituzione in contenitori muniti di serratura, adottare misure di sicurezza a protezione delle aree e dei locali ove i dati in oggetto vengono trattati e controllare l'accesso delle persone ai locali medesimi dopo l'orario di chiusura degli archivi, provvedendo alla loro identificazione e registrazione;

4. curare l'adozione di accorgimenti necessari alla tutela della riservatezza di dati diversi da quelli sensibili e giudiziari che presentino rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato.

5. svolgere le attività previste dai trattamenti di cui al punto 1 secondo le prescrizioni contenute nel Documento Programmatico della Sicurezza ed in conformità ai sistemi di autenticazione e di autorizzazione assegnati.

In ordine alla richieste di accesso agli atti e documenti contenenti dati sensibili, nell'osservanza dei principi, delle misure, modalità e accorgimenti sovra indicati, si rammenta la necessità di procedere alla previa la verifica dei requisiti di cui alla L.241/90.

Si ricordano, di seguito, alcune cautele che necessariamente dovranno seguire gli operatori comunque a contatto con il pubblico.

1) nei rapporti di front-office:

- rispetto della **distanza di sicurezza:** per quanto riguarda gli operatori di sportello deve essere prestata attenzione al rispetto dello spazio di cortesia e, se del caso, invitare gli utenti a sostare dietro la linea tracciata sul pavimento ovvero dietro le barriere delimitanti lo spazio di riservatezza;

- **identificazione dell'interessato**: in alcuni casi può essere necessario dover identificare il soggetto interessato per esigenze di garanzia di correttezza del dato da raccogliere (si pensi a soggetti stranieri ovvero a dati identificativi che possono generare dubbi sulla correttezza della registrazione) ovvero con riferimento alla personalità della prestazione richiesta: può essere necessario richiedere ed ottenere un documento di identità o di riconoscimento ove si abbia un dubbio sulle modalità di scrittura del nome e cognome dell'interessato o si voglia avere garanzia dell'effettiva identità del soggetto interessato;

- **controllo dell'esattezza del dato:** fare attenzione alla digitazione ed all'inserimento dei dati identificativi dell'interessato, al fine di evitare errori di battitura, che potrebbero creare problemi nella gestione dell'anagrafica e nel prosieguo del processo;

- **obbligo di riservatezza e segretezza:** l'incaricato del trattamento deve mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni del trattamento e deve evitare qualunque diffusione delle informazioni stesse. Si ricorda che l'eventuale violazione dell'obbligo ivi considerato può comportare l'applicazione di sanzioni di natura disciplinare ed una responsabilità civile e penale, secondo quanto previsto dal codice della privacy;

2) cautele da seguire per la corretta comunicazione di dati a soggetti terzi o comunque con strumenti impersonali o che non consentono un controllo effettivo dell'identità del chiamante:

- **controllo dell'identità del richiedente:** nel caso di richieste di comunicazione di dati propri personali (presentate per telefono o per fax) occorre verificare l'identità del soggetto richiedente, attraverso la richiesta di invio, anche via fax, della fotocopia del suo documento di identità; successivamente alla verifica può essere utile comunicare all'interessato un codice personale identificativo, da comunicare al personale per ogni comunicazione impersonale (ad esempio a mezzo telefonico);

- **verifica dell'esattezza dei dati comunicati:** nell'accogliere una richiesta di comunicazione di dati personali, da parte dell'interessato ovvero di un terzo a ciò delegato, occorre fare attenzione che il dato comunicato sia esatto, pertinente, completo e non eccedente rispetto all'attività che si deve espletare, in particolare quando la richiesta viene soddisfatta telefonicamente o attraverso trascrizione da parte dell'operatore, di quanto visualizzato sul monitor; qualora si riscontri che i dati già in proprio possesso non sono aggiornati rispetto ad i dati comunicati dall'interessato, è necessario procedere all'aggiornamento dei

medesimi, previo espletamento delle formalità (richiesta, anche via fax, della fotocopia di un documento di identità) di cui al punto precedente.

3) istruzioni per l'uso degli strumenti del trattamento

- **telefono**: nel caso di richieste di informazioni da parte di organi di amministrazioni pubbliche, o di autorità giudiziarie, può essere necessario, a seconda della natura dei dati richiesti, procedere nel seguente modo:
    - chiedere l'identità del chiamante e la motivazione della richiesta;
    - richiedere il numero di telefono da cui l'interlocutore sta effettuando la chiamata;
    - verificare che il numero di telefono dichiarato corrisponda effettivamente a quello del chiamante (ad esempio caserma dei carabinieri, servizi pubblici e di PS, …);
    - procedere immediatamente a richiamare la persona che ha richiesto le informazioni, con ciò accertandosi della identità dichiarata in precedenza;
- **fax**: nell'utilizzare questo strumento occorre prestare attenzione a:
    - digitare correttamente il numero di telefono, cui inviare la comunicazione;
    - controllare l'esattezza del numero digitato prima di inviare il documento;
    - attendere la stampa del rapporto di trasmissione, verificando la corrispondenza tra il numero di pagine da inviare e quelle effettivamente inviate;
    - qualora vengano trasmessi dati idonei a rivelare lo stato di salute, è necessario inviarli mediante raccomandata A/R al destinatario della comunicazione al fine di assicurarsi che il ricevimento avverrà nelle mani del medesimo, evitando che soggetti estranei o non autorizzati, possano conoscere il contenuto della documentazione inviata;
    - in alcuni casi, può essere opportuno richiedere una telefonata che confermi da parte del destinatario la circostanza della corretta ricezione e leggibilità del contenuto del fax;
- **scanner**: i soggetti che provvedano all'acquisizione in formato digitale della documentazione cartacea (utilizzando ad esempio uno scanner) devono verificare che l'operazione avvenga correttamente e che il contenuto del documento oggetto di scansione sia correttamente leggibile; qualora vi siano errori di acquisizione ovvero si verifichino anomalie di processo, occorrerà procedere alla ripetizione delle operazioni;
- **distruzione delle copie cartacee**: coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero alla sostituzione della documentazione cartacea con registrazione ottica devono procedere alla distruzione controllata dei supporti cartacei non più occorrenti ovvero che presentino una forma non corretta. Occorre evitare di gettare la documentazione nel cestino della carta straccia senza aver previamente provveduto a rendere inintelligibile il contenuto: si potranno utilizzare apparati distruggi documenti o altri sistemi atti a ciò;
- **riutilizzo dei supporti di memorizzazione contenenti dati sensibili o giudiziari:** i supporti rimovibili (ad esempio floppy-disk, cd-rom, dvd) che contengano dati sensibili o giudiziari possono essere

riutilizzati solo se i dati precedentemente memorizzati non siano più visionabili da parte di terzi che procedano al riutilizzo del supporto medesimo; in caso contrario, occorrerà distruggere il supporto

4) istruzioni in tema di sicurezza

a) password o componente riservata d'accesso alla rete:
- la password non deve contenere riferimenti agevolmente riconducibile all'incaricato e dovrebbe essere generata preferibilmente senza un significato compiuto;
- deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi;
- l'incaricato è responsabile di ogni utilizzo indebito o non consentito della password di cui sia titolare;

b) back-up:
salvo che non sia previsto un sistema di salvataggio di dati personali automatico ovvero centralizzato, occorre procedere con cadenza almeno settimanale alla effettuazione di copie di sicurezza dei dati personali oggetto di trattamento, utilizzando gli apparati che siano messi a disposizione dell'incaricato e riporre le copie in un contenitore al quale possano accedere solamente soggetti autorizzati;

c) antivirus:
a meno che non siano adottati sistemi automatici di aggiornamento dei sistemi di protezione da programmi antivirus, gli incaricati del trattamento devono procedere all'effettuazione delle operazioni di aggiornamento dei programmi ivi considerati, almeno con cadenza settimanale o quando venga segnalata dal sistema tale esigenza, secondo le istruzioni visualizzate sullo schermo; una volta scaricato l'aggiornamento occorre procedere alla scansione dell'intero sistema per verificare la presenza sull'elaboratore in dotazione di virus;

d) stampanti:
Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento. La stampa di documenti contenenti dati sensibili deve essere effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.

e) protezione degli strumenti di lavoro:
in caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure atte a escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni o accedere alle banche dati. A tal proposito, a titolo meramente esemplificativo, si consiglia di adottare un sistema di oscuramento (cd. screen-saver) dotato di password, ovvero, in alternativa, occorrerà porre la machina in posizione di stand-by o spegnere l'elaboratore che si sta utilizzando.

Distinti saluti.

IL DIRIGENTE
Settore……
Dott…….

Per accettazione
L'INCARICATO

.....

PROVINCIA DI VENEZIA

15.Schema di lettera di nomina degli amministratori di sistema

Responsabile del procedimento:

Venezia, li

Oggetto: DESIGNAZIONE RUOLO DI AMMINISTRATORE DI SISTEMA

Il dirigente del settore Informatica
Visto il Decreto Legislativo 196/2003 denominato Codice in materia di protezione dei dati personali;
Visto il Disciplinare Tecnico in Materia di Misure Minime di Sicurezza allegato al D. Lgs. 196/2003 allegato B;
Vista la deliberazione n.2005/220 del 26/7/2005 che adotta il Documento Programmatico sulla Sicurezza della Provincia di Venezia e s.m.i. annuali;
Visto il vigente DPS;
Visto il Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, recepito nella Gazzetta Ufficiale n.300 del 24 dicembre 2008, denominato "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" che prevede espressamente l'individuazione dei soggetti preposti a svolgere le attività di amministratore di sistema;
Vista la definizione dei profili di amministratore di sistema secondo le macroaree individuate dalla tabella pubblicata in intranet;
Vista l'organizzazione del servizio Informatica, la suddivisione interna in gruppi di lavoro e considerato il personale assegnato al settore;
Valutate la qualifica, le caratteristiche di esperienza e competenza professionale, capacità e affidabilità da Lei dimostrate;
Valutato che le prestazioni da Lei effettuate in via ordinaria forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo relativo alla sicurezza;

DESIGNA

il sig./dott./ing. _____, nato a_____ il_____ impiegato presso IL SETTORE INFORMATICA DELLA PROVINCIA DI VENEZIA con qualifica _____, amministratore di sistema per il trattamento (così come definito all'articolo 4 comma 1 lettera a del Codice 196/2003) dei dati, le cui specifiche sono allegate e richiamate nella versione corrente del Documento Programmatico sulla Sicurezza, nell'ambito di operatività definito dal profilo di _____

Il dirigente del Settore Informatica
Dott.

_____